



Securing IT Data Centres

The Choices available

"Risk Protector"
Safeguarding the availability of your IT systems

Revision 1
6th February 2006

Contents

	Page
The new challenge for physical IT infrastructures:	3
Managing the risks	5
Identify the risks	5
Identify measures to reduce risk	6
Review your security measures & rehearse and review security plans	7
Security Planning	7
Creating your Security Plan	8
Business Continuity	9
Identifying and reducing vulnerabilities	12
Flexible Solutions for Data Centres	13

The new challenge for physical IT infrastructures:

Whether a small business or a major enterprise - the demands placed on IT performance are incessantly growing. Highly complex applications, ever-faster processors, round-the-clock information and communication call for more than just an intact physical infrastructure. This gives rise to a number of elementary questions:

- Does the building fabric have suitable levels of protection?
- Can physical security measures be deployed quickly?
- Are the climate control provisions for individual racks, server room or even whole data centres able to handle generation of greater heat and IT scalability?
- Is the IT program in new technology deployment scalable to existing M&E services?
- Are power supply and back up designed for high availability?
- How can optimum use be made of the existing space when IT facilities are expanded?
- Are the applications and servers protected in case of hardware failures?
- Can all functions be managed efficiently via a perfect monitoring and remote control system?
- Can expansion be integrated later without interrupting current operations?
- Has clean build partition system v traditional construction build been considered? Thus protecting your IT investment with a reusable modular construction system.
- Are all the costs under control in the longer term - from investment through to operation and maintenance?
- How secure is the building and surrounding environment that houses the above?
- Do the facilities reside within a flood plane?
- Will there be power outages due to the construction program for the pending Olympic developments?

With a complete solution servers will at last deliver the performance paid for and at the same time minimise costs.

- Ultimate flexibility reduces initial investment outlay and safeguards the future value of investments.

- Reduced operating costs through remote maintenance, administration and high availability.
- Modular scalable components simplify planning.,
- Minimised installation costs through plug-&-play technology and space-saving rack-based configuration.
- Is there an IT Compliance Charter in operation?

Whether server room or data centre, whether high or highest availability the ability to adapt with changing needs at any time can grow with your demands.

A scalable service package means it is possible to obtain a complete solution from a single partner - from software-based configuration to installation and intelligent escalation management strategies, through which failure risks can be quickly recognised in day-to-day operation-adding up to operational reliability which a company demands.

Taking every aspect of the above for granted, every once in a while the unthinkable becomes horrific reality.

At Hemel Hempstead early in December 2005, fate delivered a hammer blow to the unsuspecting inhabitants of the area and its surroundings - a raging inferno which will take years to come to terms with.

Out of this disaster there are lessons to be learnt for any organisation reliant on highly vulnerable IT infrastructures.

Accidents do happen, but before they do, IT equipment and data needs to be protected - no matter what is thrown at it: explosions, fire, corrosive gases, floods or vandalism.

Everything from data security issues to ECBS certified rooms (SEAP approved) are now available to protect a business. It's like insurance, it may never be needed, but rest assured, if the worst comes to the worst, vital business data should be in safe hands. ECBS offer single protection cover and endorsements of an insurance policy that protect IT claims up to €50,000 and in some cases up to €50m in the event of a single claim against risks and outages.

Room in Room technology is becoming common practice and growth within IT sectors is vertical as the element with risks grows beyond our imaginations.

Managing the risks

The best way to manage the risks to an organisation is to start by identifying the threats and vulnerabilities, eliminate risks by introducing correct levels of protection, suitable for the continuance of all business plans and infrastructures.

Proactive measures are better than reactive decisions to restore, rebuild IT facilities. Cost model upfront will be smaller than a total rebuild after any disaster.

For most businesses, there will be nothing of particular concern, and simple good practice - coupled with vigilance and some consideration of contingency arrangements, will be all that is required.

If, however, assessment shows vulnerability in some way, a variety of protective security measures should be taken.

Anyone seeking to enhance security should conduct a risk assessment audit to determine which measures are appropriate (exactly what protection is needed, from what, how, from whom, where might it come from, how likely is it?).

FSA require their members to be Basel II compliant within their business architecture and structure.

Identify the risks

Fact 1: Concrete, brickwork and gypsum walls with 30/60/90/120 fire protection do not help IT hardware against humidity, moisture (Source: Debus).

Fact 2: 75% of cable / pipe work entry points are overlooked and can be the main source of entry for killer gases (Source: Debus).

Fact 3: At least 65% of all decision makers are ignorant of the vital differences in testing standards. Traditional fire tests according to British Standards primary objectives are saving life and fire containment not maintaining the correct environment for IT Hardware (Source: Debus)

Fact 4: 85% of building engineers, architects and fire fighting experts have no idea of the critical values specified for protecting magnetic media and related computer hardware (Source: Debus).

Fact 5: 80% of all major computer room disasters start outside of the protected area (Source: Debus).

Fact 6: Most IT areas will be affected by acrid gases and from fire extinguishing water in the event of a disaster (Source: Debus).

Fact 7: 1Kg of plastic releases gases and could destroy 5800 cubic metres of IT floor area. Most computer rooms will include plastic items in the shape of chairs/carpets/laptops/servers etc. New plastic items have a higher concentration and are 10 times more dangerous (Source: Edinburgh University).

Fact 8: 10 Litres of heating oil can contaminate 23,000 cubic metres of air (Source: Edinburgh University).

Fact 9: 10 Kgs of Polymethane plastic contaminates 25,000 cubic metres of air (Source: Edinburgh University).

Ask the following questions:

Is there anything about the building, business activities or staff that could be affected?

Establish what should be protected and what are the vulnerabilities.

Priorities for protection will probably be under the following categories:

- People (staff, contractors, customers, visitors);
- Physical assets (the fabric of the building and its contents);
- Information (electronic and non-electronic data); and
- Processes (supply chains, critical procedures etc).

Of these, people will normally be the top priority. The importance of the other assets will depend on the nature of the business. It may be something tangible - for example, the data suite where all transactions are recorded, the IT system or a piece of equipment that is essential to keep a business running.

Plans may already be in place to safeguard the most important assets from other threats.

For example:

- Plans to deal with fire, flooding and crime;
- Procedures for assessing the reliability and integrity of those to employed;
- Steps to protect the IT systems from viruses and hackers;
- Measures in place to limit individuals' access to some information or parts of the premises.

If there are reasons to believe that there are greater risks because of the nature of the business, anticipate and research where the vulnerabilities lie.

Identify measures to reduce risk

Since it is impossible to eliminate risk altogether, identify the most appropriate measures to reduce the risk to an acceptable level. An integrated approach to security is essential.

This involves:

Physical security, building fabric suitability;

Information security, firewalls, verification;

Managing staff securely (i.e. good personnel practices), education, ongoing risks assessment and protection protocols.

Before investment in additional security measures, review the current situation. Existing measures are often adequate if properly used and maintained, but attention to them may have become lax. Staff may be unaware of them or may have developed habits to circumvent them. Simply reinstating good basic security practices and a regular review will bring benefits at negligible cost.

Careful planning can help make security measures more cost-effective. For instance, it may be possible to introduce new equipment or procedures in conjunction with new building works or refurbishments. Or, in multi-occupancy buildings, shopping centres, high streets and business parks, it is usually possible to agree communal measures.

Review security measures & rehearse and review security plans

Conduct regular reviews and rehearsals of plans to ensure that they remain accurate and workable, and to take account of any temporary or permanent changes (e.g. new building work, changes to personnel or information and communication systems, revised health and safety issues).

Make sure staff understand and accept the need for security measures and that security is seen as part of every bodies responsibilities, not merely something for security experts or professionals. Make it easy for people to raise concerns or report observations.

Security Planning

The formulation of a security policy and the appointment of a Security Co-ordinator to oversee the policy should ensure that a response to a potential threat is well planned and executed.

The Co-ordinator must have sufficient authority to direct the action taken in response to a security threat and have direct access to the board of directors. He or she must be involved in the planning and design of the building's exterior security, access control etc, so that every aspect is taken into account

The Co-ordinator should have a number of responsibilities;

- Production of the risk assessment and subsequent security plan;
- Conducting regular reviews of the plans.

During the development of the plan it is also advisable to discuss them with other occupants of the premises and with neighbours, as well as to consult all the emergency services and the local authority.

Creating a Security Plan

The Co-ordinator should aim to produce a plan that has been checked and fully rehearsed and which is regularly audited to ensure that it is still current, workable and compatible with a business continuity plan. DR tests should be performed with your Telco and IT carrier at six monthly intervals to ensure BCP is working to the correct DR Plans, any amendment detail or instruction must be recorded and logged for the revised master plan.

Effective plans are simple, clear and flexible - although flexibility should not mean that they are open to varying interpretations during an incident, or offer a confusing range of options to follow. Personnel must be clear about what they need to do in a particular incident. Once made, precise plans must be followed.

The following measures provide a general reference point for businesses or organisations putting new security measures in place.

1. Take time to carry out a risk assessment. What kind of threats might one be facing? What is the likelihood of these happening? Where are the vulnerable points?
2. If building or acquiring new premises, try to plan security measures from the outset. This is likely to be more efficient (in both time and expense) than adding on security measures at a later date.
3. Make security awareness part of the organisation's culture. Put someone at Board level in charge. Arrange regular briefings for personnel on what they should be looking out for, and keep notices up-to-date. Take personnel seriously if they identify potential threats. Train for emergency and evacuation procedures, and rehearse them regularly
4. Ensure good basic housekeeping in and around the buildings
5. Look at how to protect information. Ensure that those who supply, operate and maintain IT systems are reputable and reliable. Possible security measures range from enhanced IT security to disposing carefully of any confidential waste.
6. Plan now for Business Continuity - how to continue to function if an incident occurs which could put premises or IT systems are out of action.

Business Continuity

Planning for continuance after a disaster or disruption is increasingly recognised, as an essential component in management of risk, your DA and BCP strategy must be tested fully to the agreed emergency plan.

Businesses are accustomed to planning against commercial risks, e.g. the sudden failure of a critical supplier, an unexpected bad debt, and industrial action or the discovery of a serious fault in a product or process.

Nearly one in five businesses suffer a major disruption each year.

Business continuity is the means of ensuring that the essential functions of a business survive a terrorist incident, natural disaster, public sector strikes, power outages or any other disruption.

It is important for any business or organisation to plan its own survival following the loss of, or denial of access to, buildings, a significant number of staff, IT systems, records and information. Plans for key home workers with software platforms and connectivity must be enabled and live in anticipation of such events.

What to do

Establish top-level ownership of business continuity planning within the organisation.

Base plans on an explicit and up-to-date analysis of:

- The risks the organisation faces, i.e. the sorts of major incidents to plan for. What credible disruptive events might happen?
- The impact that such an event would have on the organisation and its operating environment. What would the disruptive event do to the organisation's ability to continue functioning?
- The critical business functions of the organisation that must survive any disruptive event, together with time scales for their recovery.
- Which normal business activities are really essential and how quickly, and in what order is it necessary to restore them following a disruption?

Be clear about real priorities.

When analysing the risks, think in terms of the following four broad categories:

- Natural disasters (e.g. fire, flood, explosion, severe weather);
- IT or infrastructure failure (e.g. power failure);
- Terrorism (An organisation might be affected by a terrorist attack even if it is not the specific target of that attack);
- Theft, industrial unrest or other civil disorder.

Consider how these different disruptive events might affect the organisation. For example, a major terrorist incident could have one or more of the following consequences (over and above any commercial impact):

- Damage to buildings, perhaps making them unavailable for a long period;
- Ensuring HV/LV power availability is correct to growing IT demands
- Ensuring A/C units can cope with the loads on heat generation from IT systems
- Ensuring you can operate a neutral heat gain policy in your server farms
- Increasing the fire rating of your IT Room past the minimum 30 minutes towards 120 minutes
- Eliminating the risk of water ingress from sprinkler systems to core IT equipment
- Eliminating the risk of smoke contamination and ingress
- Loss of IT systems, records, communications and other facilities;
- Unavailability of personnel through of disruptions to transport;
- Loss of personnel from death, injury, or unwillingness to travel;
- Adverse psychological effects on personnel, including stress and demoralisation;
- Disruption to other organisations or businesses depended upon;

Estimate what resources would be needed to maintain critical business functions following a disruptive event. These are likely to include some or all of the following:

- Sufficient people with the necessary expertise and motivation to lead and manage the organisation;
- Access to key records and IT systems;
- Reliable means of communication, especially with the personnel;
- Ability to carry on paying personnel, to ensure their safety, and to provide them with welfare and accommodation;
- The ability to procure goods and services;
- To be able to respond to demands from clients

Ensure the plan is:

- Simple (focussed on principles, with no unnecessary detail);
- Crisis-friendly (easy to understand under stressful conditions, offering clear default settings to guide decision-makers);

- Robust (able to cope with a wide range of contingencies);
- Clear about responsibilities and authority;
- Understood by everyone who is involved, including outsiders;
- Up-to-date;
- Proven to work;
- Regularly tested;
- Consistent with the plans of partner organisations and stakeholders.

In addition, think about:

- A communication strategy for raising awareness among personnel and others who need to be aware of the plan, e.g. other businesses, the emergency services, local authorities;
- Arrangements for dealing with people who may be affected but who are not employees of the organisation (e.g. customers, clients, contractors, visitors).

If there is no plan, consider what arrangements could be implemented now to make the organisation more resilient.

These might include:

- A designated crisis management team led by senior personnel;
- Succession planning for key personnel;
- A robust telephone and/or e-mail "cascade" system for contacting personnel outside working hours;
- Copies of essential data or records stored off site;
- Access to personal IT systems from other sites;
- Remote access to IT, enabling staff to work from home;
- Robust communications;
- Robust banking and financial arrangements to ensure, for example, that the continuation of payment to employees and suppliers is possible;
- Back-up accommodation;
- Procedures agreed in advance with the emergency services and/or local authorities.

Identifying and reducing vulnerabilities

As with other security measures, a risk assessment should be conducted to establish whether there might be a particular risk of an electronic attack. The extent of the risk will help to determine the extent of the measures needed to apply. If the necessary expertise to do this is not available systems security professionals should be approached for advice.

The following general countermeasures will considerably reduce the chances of a successful attack against information systems.

- Acquire systems from reputable manufacturers and suppliers. Cheaper options may be expensive in the long run.
- Ensure that software is as up-to-date as possible. Suppliers of software are constantly fixing security loopholes in their software. These fixes (or "patches") are available from their websites consider checking for patches and updates at least weekly.
- Ensure that Internet-connected computers are equipped with anti-virus software, as most viruses emanate from the Internet. Download "signature files" from the website of anti-virus software supplier regularly. Each of these files will cover and protect from a particular type of computer virus.
- Always ensure that information is regularly backed-up. Consider keeping a copy securely in another location.
- Try to ensure that those who maintain, operate and guard the systems are reliable and honest.
- Seek regular security advice from system and service providers and make sure to act upon it - pre-empt attacks rather than wait for them. If an attack is discovered, seek advice immediately.
- If there are particular categories of material to protect, consider encryption. Again, seek advice, depending upon what should be encrypted, but encryption packages such as PGP are readily available.
- Take basic security precautions in order to prevent software or other information falling into the wrong hands. Implement a programme of security awareness amongst personnel. Operate a clear desk policy (i.e. desks to be cleared of all work material at the end of each working session).
- Invest in security cabinets and fit locking doors.
- Ensure the proper destruction of confidential material.

Flexible Solutions for Data Centres

Most Data Centres are now rapidly becoming obsolescent – with the introduction of increased density of equipment Blades, Storage et al such that the electrical and cooling loads cannot be provided for easily if at all. You can sterilise space and not use it to obtain part of the M&E required, the problem is that the cost of space sterilisation is such that it is cheaper to find new space. This is the reason that the majority of Companies – in particular the Finance sector are actively seeking new Data Centre space Tier 4 type. There is little if any of this type of space available in the UK or throughout Europe.

Future-oriented security systems are intelligently moulded to suit specific requirements and conditions. They can be extended and refitted with flexibility (can be relocated and reassembled at a different location). Scaleable IT security room solutions are configured to suit security requirements, from basic protection right up to high availability.

Modularity and ECB-S (European Certification Board-Security Systems) certification characterise these high-availability IT security room solutions, suitable for areas where the highest levels of security are required, e.g., in airports, security offices or banks which cannot tolerate any downtime whatsoever.

In addition to hardware systems, network components and telecommunications systems, complete IT system locations or archiving systems can also be housed in this "made-to-measure" shell, keeping them completely safe against elementary damage.

A secure room should provide protection against the following, while maintaining IT equipment in the best environmental practice of not exceeding a 50-degree heat rise or 85% relative humidity.

Fire:

- ECB-S certified and audited, backed by an insurance bond.
- Minimum requirement of F90 with accreditation of 30 minutes at BSEN1047-2 / Din 4102-2. Incorporating upgradeable systems to achieve F120 with 60 minutes at BSEN1047-2 / Din 4102-2.
- Certified hermetically sealed duct entry points.
- Certified AC/ Overpressure entry enclosures.

Water:

- Stagnant water (72 h, 40 cm 20 drops)
- Fire-extinguishing water (IP code, EN 60529)
- Humidity (the limit values stated in EN 1047-2) should be observed

Explosion:

- 200 kg TNT, at a 40-metre distance (accredited by UK Government)

EMC:

- Includes damping for electromagnetic fields. The damping ranges from 13db to 65db on a frequency band between 10khz and 1ghz.

Dust:

- Dust resistance to (IP-Code, EN 60529)

Combustion fumes:

- Resistant to combustion fumes in accordance with EN 18095 this classification describes the air exchange rate of the total room volume at defined pressure ratios and is below a value of 0.8.

Debris:

- Impact test according to EN 1047-2 (1 x 200 kg impact from a distance of 1.5 m)
- Impact tested according to EN 1363 (3x 200 kg impact from a distance of 1.5 m)
- Impact test according to DIN 4102 (15-20 kg from 20 cm)

Unauthorized Access:

- In accordance with EN 1627 WK 2
- In accordance with EN 1627 WK 3
- In accordance with EN 1627 WK 4

Additional equipment that should also be considered:

Air conditioning

UPS (uninterrupted power supply).

Early fire detection system.

Fire alarm and extinguishing systems.

Cable management and cable separation.

Access control.

Room surveillance.

Alarm procedure concepts.

Water warning system.

Remote surveillance.

Door systems.

Duct systems

Electronic controller system.

Video surveillance.

Raised access flooring.

Basic protection in line with current regulations for IT and communications systems, also for important infrastructures such as air conditioning, power supply, and alarm systems.

The networked world of information technology requires secure system functions and an appropriate infrastructure. Due to the complexity of modern IT concepts it takes expert skills to draw up the technical specifications for data processing systems, networks and data backup. When it comes to physical system design the premise is that sensitive systems are subject to special risks. The high availability requirements of data processing call for a range of structural and infrastructural measures.

Great importance should be placed on the issue of "structural fire protection" and "Explosion protection" following recent catastrophes around the world.

Risks to businesses are an unknown entity, it cannot be predicted, but businesses can plan ahead to eliminate known risks in our modern day to ensure business continuity with minimum loss and disruption of earnings and collateral damage.

Risk can also be translated to a level of business earning that a company is willing to forfeit against the investment of protecting one's infrastructure and IT services.

Absolute reliability should set the standard