STORKEY & CO

MANAGEMENT CONSULTANTS

USEFUL
BUSINESS CONTINUITY STATISTICS
AND OTHER INFORMATION

STORKEY & CO LIMITED
90 LARSEN CRESCENT ● P O BOX 51 096 ● TAWA ● WELLINGTON ● NEW ZEALAND
PHONE +64 4 232 4594 ● FAX +64 4 232 9465 ● MOBILE +64 21 414 510
EMAIL IAN@STORKEYANDCO.COM ● WEBSITE WWW.STORKEYANDCO.COM

PCs & Computing

The loss of a single PC has caused bankruptcy.

Initial cost of a PC is only 20% of the true cost of ownership – PC Pro, Oct 1997.

A 1992 DTI survey concluded that UK businesses lose £1.1b annually through computer security breaches and £580m through physical damage to IT systems.

A 1998 survey commissioned by Tertio showed that 21% of companies admit they cannot assess the business risk of network downtime.

Costs

Typically insurance only covers 60% of any actual loss.

Price Waterhouse/BSI survey showed that 15% of firms experiencing a disaster lose more than £1m and 20% lose between £250,000 to £1m.

Data/Back Ups

The effectiveness of back-up arrangements is often key to recovery (back-log management).

80% of firms who suffer a data loss which requires a restore from back-up go out of business within three months – source freelance IT journalist.

According to a University of Texas study, 94% of companies suffering a catastrophic data loss will not survive – 43% don't re-open and 51% close within two years.

According to HP, of the 13 million small businesses in Europe only around 50% back up regularly.

According to the Audit Commission only 9% of companies claim against loss of data.

Survival Chances

80% of businesses suffering a major disaster go out of business within 13 months according to the BCI.

According to a 1993 IBM/Cranfield Management College survey 43% of business suffering a disaster never re-open and a further 30% go bust later as a result.

According to a 1993 survey by the University of Minnesota the lost of a critical resource for more than 10 days can destroy a business.

Only 40% of organisations with BC plans have tested them and when plans are first tested 80% are shown to have major flaws – Andrew Hiles (Survive! Chairman).

Bombs

Manchester bomb (June 15, 1996) – according to David Howarth, senior emergency planning officer, Manchester City Council – resulted in £5 million loss of trade on first day alone.

According to NatWest Insurance Services:

- 452 businesses were severely disrupted by the 1996 Manchester bomb and 250 of them went bust within six months.
- nearly 75% of firms hit by a serious fire end up closing.

Of the 350 firms affected by the World Trade centre bomb, 180 have gone bust and not all of those had their HQs at the centre.

VIRUSES

A BBC report in February 1998 said that a virus infection can cost as much as £1,700 per computer to put right.

According to Sunday Times article in 1994 a new virus is written every 25 minutes.

BUSINESS CONTINUITY

According to the ABI:

- 1998 losses due to fire damage to UK businesses were over £1.6m a day or £600m for the year.
- weather-related claims were £255m.
- there were 134,000 claims for theft despite the significant growth in CCTV - according to the HO there are over one million CCTV cameras in operation in the UK.
- 66% of company car drivers are involved in an accident every year (40% higher than private motorists).

According to an 1993 IBM computer failure survey:

- 20% of firms had experienced a computer disaster with last year, 33% deliberately by malice, fraud or misuse of the system, 33% as a result of software or hardware failures, 20% due to fires, floods or Acts of God and remainder due to user error power failure.
- less than 25% of companies had a viable contingency plan.
- of the 57% of companies that had some kind of a plan, the majority were useless because had not been properly tested.
- 43% of companies had no recovery plan, the main reason for this being that managers believe insurance will cover their losses.
- 60% of companies are not covered for employee negligence or abuse of their computers.
- 75% not covered against software failure.
- 70% of firms experiencing a computer failure cease trading within 18 months.

According to 1996 Securit survey (computer service division of Securicor), poor internet security, frequent crashes and a lack of DR procedures leave mission-critical applications on the LAN facing disaster:

- many users have weaknesses in IT procedures even though nearly 80% of respondents run mission-critical business applications over the LAN.
- only 37% use virus checking procedures with their internet connections.
- nearly 10% had a serious network problem at least once a week and 19% at least one a month.
- only 55% had an IT DR plan, 33% claimed they would get one within next 12 months, and 12% believed had no need for one.
- data loss most commonly arose from back-up failure or finding data had not been backed up at all.

1996 Spikes Cavell Network survey found:

- 91% of UK companies have multiple network failures every year. Although many companies had contingency plans to deal with big failures, many of these never been tested.
- 52% of IT managers said their users expect 100% network availability.
- causes of LAN failure: 68% hardware failure, 38% large files, 24% software, 4% taken down & 3% new software.

1997 Spikes Cavell survey of IT mangers commissioned by Business Computer World:

- 80% of managers considered DR planning a top priority.
- 14% of managers had no form of DR plan.
- 68% of companies have had a disaster serious enough to disrupt their IT systems in the last 6mths.
- 44% of firms have had a power cut in last 6mths – most common cause of computer downtime.
- 85% of businesses have an agreed procedure for dealing with IT related disasters.
- 33% of organisations back up data to an off-site location (data vaulting).
- 66% of firms are insured for the replacement cost of recovering data.
- 66% of firms have contracts with outside DR specialists.

1996 Information Security Breaches Survey:

- 46% of companies hit by theft.
- average cost of theft had increased from £7,000 in 1994 to £25,000 in 1996.
- one third of companies took over a week to recover from a theft.
- reconstruction of data was one of the major recovery costs.
- only 18% of companies recovered all the costs of a theft.
- 41% were not covered or received no pay out from insurance.

- more than 50% of companies found a contingency plan highly effective in dealing with computer disasters.
- one third didn't have a contingency plan.
- data loss caused by failures in back-up or recovery procedures caused the most incidents with a serious impact on an organisation.
- only 10% aware of the BS7799 standard for information security management and had reviewed their security standards against it.
- 90% of organisations reported at least one serious information security breach in the past two years.

KPMG - Computer Security Review 1994:

- password security – 25% of mainframes not adequately protected, 35% of minis and 79% of PCs.
- 38% of organisations with mainframes or minis reported a loss of computer facilities in previous 12 months yet had no recovery plan – 58% rank these computers as business critical.
- only 64% of organisations had classified their data or programs according to sensitivity.
- 78% of organisations said loss of mainframe would be critical or very disruptive to business yet 25% didn't have a contingency plan for these facilities.
- 70% of organisations said loss of offices would be critical or very disruptive to business yet over 60% didn't have a contingency plan for these facilities.
- over 30% of organisations said loss of PCs would be critical or very disruptive to business yet over 55% didn't have a contingency plan for these facilities.
- 25% had never tested their mainframe contingency plan.
- 43% had never tested their mini contingency plan.
- 42% had never tested their PC contingency plan.
- although majority of organisations had insurance to cover loss of computer hardware, the cover dropped for software and the cost of recreation of data, indicating that management do not appreciate the true value of software and data assets held on their computers.

THE INTERNET

A 1999 global survey by Infosecurity 99, Secure Computing & NetPartners found that:

- employees spend 30 minutes/day non-business net surfing.
- an estimated 50% have accessed adult sites.
- non-business use of the net is costing employers £2,500 per employee annually - based on an average salary of £20,000 plus non-wage staff costs.
- 84% have unlimited access to the web.

- 76% of employees use web to search for new jobs.
- 83% for personal finance.
- 82% for sports.
- 85% for general entertainment.
- 56% visit chat rooms.
- 84% for travel.
- 35% of companies don't have formal policy on web control.
- 43% of firms didn't have a formal policy for controlling the use of external email.
- 63% of companies had a formal policy for preventing the download of offensive material but only 38% strictly enforced the policy and only 20% of respondees said they would report colleagues for downloading offensive material.
- 41% of firms reported an incident of improper net use but only 21% resulted in formal action.

Statistics and information were provided by Survive! The Business Continuity Group.

Survive!
1st Floor, Waterman House
101-107 Chertsey Road
Woking, Surrey GU21 5BW
UK
Tel: +44 1483 710600 Fax: +44 1483 710601
http://www.survive.com