

## How to avoid a data disaster



03/02/10 17:03

Email | Print | SHARE

1. ▶ **Know the law** - The Data Protection Act, says CTO of Bcrypt Marc Hocking, demands you process data fairly and lawfully. It must be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed. And appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal data. You are, says CEO of Carbonite David Friend, "legally obligated to keep key financial and contractual data for a minimum of seven years".
2. ▶ **Don't be a recession 'victim'** - Since the beginning of the recession, with corners and IT departments cut accordingly, computer forensics [business](#) Kroll Ontrack has reported a 100% rise in critical application recoveries.
3. ▶ **Do the obvious** - Before you stifle a yawn, have you definitely got suitable virus and malware protection firewalls covering your entire workforce, including [mobile](#) and home workers, asks Robert Mackenzie, a partner in the business [technology](#) and consulting arm of accountants Scott-Moncrieff. And are password change requests automated?
4. ▶ **Carry out a risk assessment** - Know what you need to secure and who can access it, print it, send it, copy, paste or delete it. Consider customer databases, financial spreadsheets, designs, IT applications. Be led by what brings in revenue and keeps your business functioning, says Ian Masters, UK sales and marketing director at Double-Take Software.
5. ▶ **Don't box-tick your policy** - On the new data legislation, Dan Bowyer of The Engine Room, says he doesn't think it's top of his clients' minds or necessarily enforceable. That said, just box ticking is pointless, he says and a policy can be created for around £1,500 - £3,000, including consultancy, documentation, and education.
6. ▶ **Create restricted areas** - Where do you keep crucial data right now? Physical controls – lock and key – over access to office areas, says Mackenzie, is a box you should tick. Are laptops, servers, backups and paper files there for opportunistic thieves to get their grubby mitts on, asks Ann Dempster, managing director at Plum Software.
7. ▶ **Back up data** - Ok, this one's a biggie. A data loss or attack could leave staff twiddling thumbs for days – and clients reviewing their contract with you. Worse than that, your backups might not actually work – when did you last try to recover something from one? You need a system and a regular procedure to check staff are doing it properly and the kit is working. "On average," warns Plan B DR's Tim Dunger, "20% of backups usually fail." Online backups, he says, save moving tapes or disks around and are "more secure in encrypted form", says Dunger, but as it doesn't keep a local copy of the data how long will it take to download all of it? And what will happen if the provider were to go out of business, as some have, asks Andrew Dodd, EMEA product marketing and marcom manager for HP. He suggests network attached storage devices (NAS) as a solution, which automatically backup multiple PC, Mac or Linux systems. Finally, Networks First's non-exec Derek Dale warns that the new trend for virtualisation is a risk: "With a 'one box' solution, any failures are total."

8. ▶ **Backup mobile employees** - "Use tools such as hidden partitions on laptops to save images of the systems," says David Blackman, general manager of Northern Europe from Acronis. "That way, should a user be travelling when an emergency occurs or a virus hits, the remote user will be able to restore the data and programs on the laptops themselves."
9. ▶ **Formulate a disaster recovery plan** - This is your formal checklist of how to deal with a disaster. Reputation, productivity and sales could be hit. Compliance with data protection could be compromised. Dunger advises you prepare a list of kit you need to get up and running, and a step by step process for retrieval of operating systems and accessing backed up data.
10. ▶ **Protect employees from themselves** - The majority of data breaches, says Nick Lowe, regional director, Northern Europe Check Point, "occur not because of malicious behaviour, but because an employee was just trying to save a little time, to get their job done quicker, or because they simply forgot to apply security". Automate as many of your security measures as possible, such as mobile encryption. A private corporate network for mobile workers, is worth having, suggests senior product marketing manager at iPass Matt Cooke. And when staff leave, revoke user access promptly, says Richard Walters, co-founder and Product Director at Overtis Systems.
11. ▶ **Scan and secure important documents** - Go digital with paper, says Dempster. "It is essential that these are kept both secure and easily retrievable using proper client management software." Colin Gallick, CEO of Invu, which specialises in document management says: "Unlike standard off-site archives, electronic document management systems (eDMs) also collate everything centrally so that all of the information across the company is easy to search, access, and control."
12. ▶ **Dispose carefully** - "Are you disposing of data correctly?", asks Mackenzie. "The Data Protection Act stipulates that data should not be held longer than necessary. You need robust measures in place to ensure that data is removed from your systems, and that the devices which held it are also disposed of securely when they come to the end of their useful life."
13. ▶ **Beware social networking sites** - Your Twitter and Facebook policies permitting, social networks pose a threat, with third party applications integrated on such sites capable of carrying malware, says Simon Morris, R&D director at risk management service provider Pentura.
14. ▶ **Carry out testing** - Most companies scan for malware and have anti-virus software installed, but more proactive testing should be carried out, says group security manager of data centre provider TelecityGroup Geoff Donson, formerly with the Metropolitan Police's Serious and Organised Crime Agency (SOCA), and the National Hi-Tech Crime Unit. "Both penetration testing and vulnerability scans show how well a network can stand up to external attack and both should be employed regularly."