

Top Tips

Prevent and cure IT disasters



1. Get to know suppliers, let them get to know you

The gap between your expectations and your supplier's ability (or willingness) to meet them is where disaster can strike.

You need to be clear about requirements and expectations on both sides of the table, identifying grey areas for attention. For example, commissioning a website design without properly discussing hosting or maintenance could lead to unexpected fees or animosity later on.

Formalising requirements through contracts or service level agreements can identify gaps, but fostering honest and mutually beneficial relationships is equally important when working with suppliers.

2. Think of backup as a strategy, not a task

When considering backup strategy, a balance needs to be struck between accessibility, security and cost. Review your data use, consider the options available and find the right balance for you.

Your backup methods will depend on factors such as how much data you have, how frequently it changes, and its value to your business. If you backup at weekends, you should accept that any data created midweek might be lost. If you keep a backup disk in your desk drawer, you must accept the risk that sensitive data may be stolen.

Such considerations illustrate why successful backups are more about how you do it, than if you do it at all.

3. Don't be complacent about password security

Most businesses hold sensitive data on computers or networks, from client or prospect lists and customer data through to financial records or trade secrets.

Malicious users or hackers exploit weak password security to get into your networks (or stolen computers). If they get in, they can steal your information or abuse your systems.

Using longer passwords (8 characters or more) and mixing letters and numbers helps reduce the chances of being caught out. Changing passwords regularly is also recommended.

4. Plan software updates

The security of your system - not to mention its reliability - depends on robust software. Updating software regularly helps avoid security threats and keeps your systems running smoothly.

That said, it's important to understand how software updates may impact business processes - for example, if you use a web based content management system, has it been updated to work with the latest browser update? If it hasn't, updating software could render your services inoperable.

Updates are important, but ensure your update schedule is cohesive and contingencies (such as system restores or backups) are in place if things go wrong.

5. Have a continuity plan

How much time and energy you devote to developing your continuity plan will depend on the size of your company and its reliance on uninterrupted IT services. Regardless, if you use computers, you need a plan if things go wrong.

Imagine the kind of disasters that could affect your business - such as fire, flood or data loss - to identify how and where your operations will be most affected. Also, consider how quickly you need to be up and running if disaster does strike. Such questions will highlight key areas for attention.

If the answers flag up concerns, make your continuity plan a priority and invest time and resource to ensure you are ready for disaster.

More info - Visit www.businesslink.gov.uk/it for a comprehensive range of IT resources, including more information on the issues covered in this guide.

Have your say

Do you have a Top tip to add to the list? Do you think one particular tip should take top spot, or maybe knocked off the list altogether?

Business Link's online resources are extremely popular across the South West and beyond. With your contributions, we can make these resources even better, for you and thousands of other readers.

Visit www.businesslink.info/feedback to submit your Tips or comments.

Thank you! We really appreciate your time and feedback.



For more information or further resources:

Visit www.businesslinksw.co.uk or call
0845 600 9 006

© Crown copyright 2007, For terms and conditions of use please our website.