



[Home](#) [Services](#) [About us](#) [Contact us](#)

January 2008
0121 506 9230

Prevention or survival? The choice is yours when it comes to information security

With the year-end data disasters involving child benefit data lost by HM Revenue and Customs and driving test details mislaid in the States it seems that many large organisations are having to think as much about surviving an information security breach, as preventing one.

Luckily most small businesses don't face the same kind of threat to security - they don't tend to have layers of faceless personnel spread around the country, split sites using apparently insecure internal postal systems and very few choose to have masses of data processed off-shore. That's the good news.

However information security threats are still a fact of life for any business and it's very much the Bronte Business Networks mantra that prevention is always better than cure. As [quoted in our last newsletter](#) DTI figures indicate that 44 per cent of businesses have suffered a malicious breach of security. For smaller businesses the attacks are most likely to come from viruses, worms, spyware, adware, email and web based application threats, although some of the threat will come from staff misuse or misunderstanding too. So if you make only one New Year's resolution for your business make it to follow the Bronte A B C guide to enhancing your computer and network security to safeguard your business information.

A B C Guide to Information Security

This Bronte A B C guide to preventing an information security breach highlights the most important areas all business owners and data managers should focus on.

A - Access

The first and perhaps most important aspect of security is all about access, who has it, how you prevent those who shouldn't have it getting it and how to manage access simply and efficiently so that giving or preventing access doesn't become a strain on your business.

Thinking firstly about internal threats to data security we recommend that you operate a **policy** of least access, providing access to data, systems or files on a need to know basis. This may sound a little draconian but it's one of the best ways to prevent security breaches or inadvertent data corruption within your organisation. Password protection on files, file permissions and encryption can all be used here.

Passwords for access to all PCs and servers are essential to offer first line protection for your data in case of theft. It is a good idea to provide guidance to your staff on the format of passwords to make sure they are as secure as possible. (Read the [Bronte Guide for Secure Passwords](#)).

The set up of your computer network and individual PCs can also offer increased security. A properly configured **firewall** makes it harder for hackers to access your data but also prevents potentially harmful programmes being downloaded inadvertently from the Internet.

Bronte User Tips for January

Each month we'll bring you tips for getting the most out of everyday IT applications.

This month: [Creating documents in Office 2007 you can share.](#)

Understand Security Threats

Spyware is software that is installed on a PC to intercept or take partial control over the user's interaction with the computer, without the users consent

Spyware programs can collect various types of personal information but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting Web browser activity, accessing websites blindly that will cause more harmful viruses, or diverting advertising revenue to a third party. Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of internet or other programmes.

Email **spam filters** will not only ease the frustration of your staff but also provide protection from harmful viruses which can all too easily be spread.

If your business uses wireless technology, either in the office or to provide access for staff working remotely then it is very important to make sure that full **wireless network encryption** is enabled. It's very easy to hack into a wireless network and although you are perhaps unlikely to be targeted by dangerous criminal hackers students have been known to hack networks just for the fun of it.

If you need advice or guidance on how to make your computer network safe from external threats contact Bronte Business Networks.

B - Back-up

Implementing a regular backup procedure is essential to safeguard critical business information. All too many smaller businesses fail to follow a robust back-up procedure sometimes with serious consequences. A client recently spent days pulling their hair out trying to retrace their steps when they lost all the emails for the last year and discovered their back-up (which had never been tested) was corrupt.

The first thing to decide is the most appropriate type of back-up for your business. On-line back up is becoming more common as broadband connection speeds increase and firms look for a simple automated process. Many traditional businesses prefer tape back-up, which has served them well over many years whilst others opt for continuous protection with data being backed up immediately. Whichever method you choose there are a few simple rules to follow:

- Be clear on whether you will use a full back-up or incremental back-up and fully understand the consequences of these options in terms of storage space and restore processes.
- Ensure all relevant data is set to back up - don't forget to back up email, contacts and calendar details for example.
- Test your backups frequently by restoring data to a test location.
- Allocate responsibility within your organisation for back-up and make sure the job is given an appropriate level of importance.
- Ensure your backed-up data is held in a secure location – if you back-up on-line where is the data being held and what their disaster recovery procedures are if they are hit by fire, theft etc? If using a hard copy back-up is this stored securely off-site?
- Back-up data at least on a daily basis and test your back-up weekly, without fail

For information and advice on implementing an effective back-up procedure to safe-guard your data call Bronte Business Networks on 0121 506 9230.

C - Catch-up

There are unfortunately in life some unscrupulous people who like to take advantage of other's misfortune. It's a fact of life that software contains bugs. As a new bug or security loophole is discovered the criminals work as fast as they can to exploit it before the problems can be fixed and updates issued. That's why it's so important to work on the most up to date version of any software and install updates as soon as they become available.

When Microsoft or any other software company discovers vulnerability in its software, it typically releases an update that can be downloaded over the Internet. The update "patches" the loophole or bug to keep hackers from causing trouble. Setting your computers to automatically download the latest patches and updates will help.

If you are in any doubt about whether your software is fully secure you can check by visiting the relevant software supplier's website or alternatively call [Bronte Business Networks](#) to arrange a review of your systems.

To check your knowledge and understanding if IT security issues take the [Bronte IT Security Knowledge Test](#).

Download: Information Security Guide

Because we believe that information security is so important we are making available a copy of a detailed [Microsoft Guide to Security for Small Business](#). You can download a pdf copy of the guide from the [Bronte Business Networks website](#).

Security Audit

A review of operational procedures, software and physical security will highlight potential loopholes in your systems and procedures. Bronte Business Networks offer a full security audit looking at everything from disaster recovery and server configuration to back up procedures and system administration policies.

To discuss your information security concerns contact Bronte Business Networks on 0121 506 9230 or [email Bronte here](#).

About Bronte

Bronte Business Networks offer a full range of outsourced IT services, tailored to your business. Whether you are looking to install a new network, update your software, add to your hardware, need help maintaining an existing system or require an emergency response, you can be sure of a personal, professional and prompt service. To find out more how you can make the most of your IT visit www.brontebusinessnetworks.co.uk.

Subscription Details

Bronte News is emailed to subscribers monthly. Feel free to pass on to friends and colleagues. To subscribe [email us here](#).

If it has been sent to you in error we apologise, if you wish to unsubscribe [email us here](#).

©Bronte Business Networks. All Rights Reserved.

Blythe Valley Innovation Centre, Central Boulevard, Blythe Valley Park, Solihull, B90 8AJ