Top Seven Things You Must Do To Keep Your Business Data Secure

The exhaustive interconnectedness of tablets, mobile phones, desktop computers, printers, traffic control systems, and even cars, has created a world in which every connection is a potential security hazard. Data security has become the #1 priority for every business, yet recent reports show that many organisations have failed to implement appropriate measures.

It's worse than you think

In September 2015, security intelligence company LogRhythm released the details of a nationwide study that revealed the true scale of the problem. 33% of employees and 43% of managers admitted that confidential company information was vulnerable to theft or unauthorised access. 72% of workers said they believed the greatest threats are employee related, and 16% admitted accessing documents they should not be reading at work. LogRhythm concluded that the percentage of respondents who admitted unauthorised access to workplace documents 'potentially equates to 719,000 across Australia'—a staggering figure.

So what can you do?

Create and implement an exhaustive data security policy. Conduct six-monthly checks to ensure staff are familiar with security procedures. Review the policy every year, and improve where necessary. Use the following checklist to improve your protocols:

1 ***_ Password Management

Powerbits recommends the use of password managers, such as LastPass, which allows you to generate a different password for every site. Keep your passwords complex. Strong passwords typically consist of more than eight alphanumeric characters in a random sequence.

2 Email Hygiene

Spammers and hackers will try to bait you with fraudulent identities, dangerous urls, and viruses or malware disguised as innocent attachments. Unsolicited emails should be treated with extreme caution. Do not click on an embedded url, and do not open the attachment even if it has a harmless extension (e.g. .xls, .zip, .doc). If in doubt, check any contact details (e.g. phone number) but do not reply to the email.

3 Multifactor authentication

This is a form of layered security in which a user is required to present more than one form of verification. Examples include:

a. MyGov website: enter username and password, receive sms with verification code, enter verification code
b. Commbank website: log into account with username and password, request verification code for a specific operation (e.g. transferring money), receive sms with verification code, enter verification code

Adding multifactor authentication to your systems will greatly improve data security.

4 Security updates and patching

Operating systems update and patch themselves automatically, but the process is not infallible. Your IT specialist will know when and how to roll out security updates with maximum efficiency and minimum stress.

5 Antivirus and antimalware protection

It's not bulletproof, but it helps. Ask your IT specialist to recommend a package suitable for your business. One popular brand is Bitdefender, which offers a highly customisable suite ranging from anti-virus to firewall protection.

6 Network security

Your router is your gateway to the internet. It needs to be fit for purpose, and absolutely secure. Manufacturers regularly release firmware updates to improve security and performance. Your IT specialist will be happy to manage these for you.

7 Database, folder and file permissions

Often overlooked is the issue of internal access to sensitive data. Correct controls must be applied to ensure that employees only have access to data appropriate for their role and responsibilities. Ask your IT specialist to implement the correct permission set for every user on the system.

PowerbITs
Making Technology Work For You
1300 887 889
info@powerbits.com.au
powerbits.com.au