CANTERBURY EMPLOYERS' CHAMBER OF COMMERCE

WE KNOW BUSINESS

PROTECTING YOUR DIGITAL DATA

QUICK GUIDE

PROTECTING YOUR BUSINESS FROM LOSS OF DIGITAL DATA

Businesses these days rely very much on electronic data for general records, accounts, inventories, communications etc. We need to be careful about how we manage this data and take steps to maximise the security of the data held by organisations.

To minimise the risk of a data breach or loss requires action against specific security threats such as software viruses and malware, and hackers. It can also require action in the form of broader authentication and data security strategies, including back-up, business continuity planning and disaster recovery planning.

Focus on your most loyal customers and diversify your customer base while expanding your markets where possible

VIRUSES & MALWARE

There are many different types of threats to computers, generally named 'malware' (malicious software), and including worms, viruses, trojans and spyware.

Malware can take many different forms including allowing hackers to operate the computer remotely; stealing information directly from the computer; destroying information; and/or spreading malware to other computers in contact with the infected host.

Malware can be spread in many ways:

- Via attachments
- Via removable storage devices such as USB thumb drives
- From visiting infected sites

There is no guaranteed way of ensuring your computers are safe from malware but you can dramatically reduce the likelihood of damage by:

1. installing security software (incorporating anti-virus, firewall and anti-spyware programmes) and updating it regularly
2. ensuring that your computer operating system automatically checks for updates and installs any updates as soon as they are available
3. stopping and thinking before you click on links and attachment.

In larger companies, it is best practice to:

- document and enforce IT security software update and scanning procedures
- install IT security software on end point computers, all internet gateways and server points of access
- alert system administrators to the presence of malware

While IT security software can reduce threats, how computers are operated can also help reduce the risk. Try to:

- use secure passwords and change them frequently
- only click on links and attachments from people you know

- visit only credible websites
- limit the use of removable media from outside your organisation.

HACKERS

'Hackers' may gain unauthorised access to your computer programmes or systems and use the information for disreputable purposes. While your computer is connected to the internet hackers may try to directly exploit vulnerabilities they detect on your computer, leave malware in your website to infect visitors or use keystroke logging to eavesdrop on your communications.

Securing your computer
It is best practice that every office computer connected to the internet has a 'firewall' (a barrier designed to prevent unauthorised or unwanted communications between computer networks) in order to reduce the amount of unwanted access.

Securing your website
As well as securing your computer it is important that your website does not pass on threats to their visitors.

Ensure that your website developers are aware of your desire for website security.

Securing your wi-fi
Ensure that your wi-fi security is enabled (e.g. password protected) to reduce the likelihood of other people looking to use your connectivity for inappropriate purposes or to try and access your information transmitted via the network.

BACKUP

Businesses must have a regular and where possible, automated backup system in place for their servers and website, and could include:

- hourly/daily incremental backups – on and off site (tapes, discs, USB, over the internet)
- server image backups – on and off site

In a 'hosted environment' (e.g. where your servers/website are hosted outside you physical location), standard backups will often be part of the hosting service.

BUSINESS CONTINUITY PLANNING/DISASTOR RECOVERY PLANNING

Business continuity planning (BCP) and disaster recovery planning (DRP) are very similar. Businesses should develop a set of processes and procedures that are needed to ensure that the critical business functions of the organisation continue to operate in the event of a disaster, even if only at a minimal operational level.

It usually covers the following areas:

- risk assessment and management
- business impact analysis
- strategy planning and agreement
- plan development
- plan testing and maintenance