HSB

A Munich Re company

Technical bulletin

Protecting small businesses from data breach

Today, virtually all businesses collect and store personal information about customers, employees and others. The frequency of data breaches - the theft, loss or mistaken release of private information - continue to make headline news.

Data breaches aren't just a big business problem; small and medium-sized businesses with fewer data security resources are particularly vulnerable.

In fact, 39% of small and 65% of medium-sized UK businesses experienced a cyber security breach or attack in 2020(1). As a result, it's important for businesses of every size to take steps to prevent a data breach. Here's how:

1. Only keep what you need: Inventory the type and quantity of information in your files and on your computers. Reduce the volume of information you collect and retain only what is necessary. Don't collect or keep information you don't absolutely need. Minimise the number of places you store personal private data. Know what you keep and where you keep it.

2. Safeguard data: Lock physical records containing private information in a secure location. Restrict access to that information to only those employees who must have access. Conduct employee background checks. Never give temporary employees or vendors access to personal information on employees or customers.

3. Manage use of portable media: Portable media, such as DVDs, CDs, USB hard drives and 'flash drives' are more susceptible to loss or theft. This can also include smartphones, MP3 players and other personal electronic devices with a hard drive that 'syncs' with a computer. Allow only encrypted data to be downloaded to portable storage devices.

4. Destroy before disposal: Cross-cut shred paper files with private information you no longer need before disposal. Destroy disks, CDs/DVDs and other portable media before disposal. Deleting files or reformatting hard drives does not completely erase your data. Instead, use software designed to permanently wipe the hard drive or physically destroy the drive itself. Also, be mindful of photocopiers, as many of these scan a document before copying. Change the settings to clear data after each use.

5. Update procedures: Do not use National Insurance numbers as employee ID numbers or client account numbers; develop another ID system. Make sure that your procedures comply with any applicable laws or legislation. Also, make sure that they align with any applicable industry required standards, such those that may be required by the Payment Card Industry (PCI) Data Security Standard.

6. Educate/train employees: Establish a written policy about privacy and data security, and communicate it to all employees. Require employees to put away files, log off their computers and lock their offices/filing cabinets at the end of the day. Educate employees about the different types of cyber-attacks, what types of information are sensitive or confidential and what their responsibilities are to protect that data.

7. Control computer usage: Restrict employee usage of computers to business use. Do not permit employees to use file sharing peer-to-peer websites or software applications, block access to inappropriate websites and prohibit use of unapproved software on company computers.

8. Secure computers: Implement password protection and 'time out' functions (requires re-login after period of inactivity) for all computers. Train employees to never leave computers unlocked or unattended. Restrict tele-commuting to company-owned computers. Require the use of strong passwords that must be changed on a regular basis. Don't store personal information on a computer connected to the Internet unless it is essential for conducting business.

9. Keep security software up-to-date: Keep security patches for your computers up-to-date. Use firewall, anti-virus and anti-spyware software; update virus/spyware definitions daily. Check your software vendors' websites for any updates concerning vulnerabilities and associated patches.

10. Stop unencrypted data transmission: Mandate encryption of all data. This includes data 'at rest' and 'in motion'. Also consider encrypting email within your company if personal information is transmitted. Avoid using Wi-Fi networks; they may permit interception of data.

HSB Cyber Insurance

Our all-in-one computer, data and cyber insurance policy provides comprehensive cover for small and medium-sized businesses. For more information, visit our website:

www.hsbeil.com

Why choose HSB?

- Leading specialist provider of engineering and technology insurance and inspection services in the UK and Ireland
- UK-based arm of Hartford Steam Boiler, the equipment breakdown insurance and inspection market leader since 1866
- Part of Munich Re, a world leader in risk solutions, consistent risk management and financial stability
- Financially strong and stable - rated A++ (superior) by A.M. Best Company
- A member of the Institute of Customer Service, demonstrating our commitment to continually improving customer service performance and professionalism

(1) Cyber Security Breaches Survey 2021 - Department for Digital, Culture, Media and Sport

HSB
A Munich Re company

HSB Engineering Insurance Limited, registered in England and Wales: 02396114, Chancery Place, 50 Brown Street, Manchester M2 2JT. Registered as a branch in Ireland: 906020, 28 Windsor Place, Lower Pembroke Street, Dublin 2. HSB Engineering Insurance Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority in the United Kingdom, and is authorised and regulated by the Central Bank of Ireland as a third country branch in the Republic of Ireland.

www.hsbeil.com HSBEI-1450-0622-3 Picture credits: Getty Images