THE DATA DANGER

A *RISKY* BUSINESS

Our personal data must be protected from criminals who want to defraud us out of money. Businesses are the custodians of customer data so are at the front line in the war against fraud.

The danger is not new – but the nature of it has changed due to the digital revolution. Companies have to protect their paperwork, ensuring it is securely stored and destroyed, and they also need to be aware of cyber threats. A study at the end of 2018 showed that four in ten firms suffered a cyber security breach in the previous 12 months. For businesses with 250 or more employees, that rises to 72%.

THE ALARMING NUMBERS

The alarming numbers come from the Cyber Security Breaches Survey, a research project put together by pollsters and academics for the UK Government.

About three-quarters of businesses say cyber security is a high priority for their senior management **BUT** only 27% have a formal cyber security policy.[1]

One-in-five businesses *NEVER* update senior managers on cyber security.[1]

in Made in InVision

The mean cost of breaches with a financial impact is £3,100 – but that's £22,300 for large businesses.[1]

The mean spend on cyber security for a business in the last year was £3,580 – but that ranges from £2,200 for small businesses to £149,000 for large companies.[1]

Many businesses don't handle or dispose of their paperwork properly either. Studies have shown that:

40%

of all data breaches are paper based, showing the importance of not just focussing on cyber attacks

19%
Paperwork sent to the wrong people

14%
Lost or stolen paperwork

4%
Data left in an unsafe place

3%
Insecure disposal of paper

Source: Information Commissioner's Office data (quoted by third parties such as IT Pro
https://www.itpro.co.uk/security/31386/gdpr-doesnt-just-apply-to-digital-data)

Only 27%

of companies say they have policies for the safe storage and disposal of confidential information.[2]

One in four

employees admit they don't shred confidential information – causing a substantial risk of a paper data issue.[3]

in Made in InVision

HIGH PROFILE BREACHES

In March 2018, Google discovered a bug in the API for Google+ that allowed third party app developers to get hold of the data of users and their friends. The breach wasn't revealed until October with potentially **500,000 accounts** affected and up to **438 third-party apps** able to access private information.[4]

The Information Commissioner's Office found that Wolverhampton City Council threw confidential waste – featuring names, dates of birth, employment records, medical records and bank details – into a skip on an industrial estate.[5]

A £250,000 fine was issued to Scottish Borders Council when employees' pension records were found in a supermarket's paper recycling bank.[6]

In the US, telecoms giant T-Mobile announced hackers had obtained the details of about **two million customers**. The data taken included customers' name, zip code, phone number, email address, account number, and account type.[7]

More than 850,000 pieces of paperwork were lost by the NHS in the UK. Some of the documents – including sensitive health data – were sent to an outsourcer by mistake.[8]

In September, hackers gained access to **30 million Facebook accounts**. In 14 million cases, users' basic contact information was taken. In another 15 million, gender, religion, location, device details and 15 most recent searches were taken.[9]

details and 10 most recent searches were taken.

In November, hotel chain Marriott revealed that its Starwood guest database had suffered from an issue that could have dated back to 2014. **500 million customers' data** was taken, including names, addresses and contact details.[10]

The UK Government admitted to **losing thousands of papers** after misplacing sensitive documents it had removed from the National Archives.[11]

THE DAMAGE CAUSED BY A DATA BREACH

REPUTATION

Negative headlines can leave you with some work to do to avoid your brand being associated with a breach. Marsh and Microsoft's Global Cyber Risk Perception Survey in 2018 found reputation loss was business' biggest concern from a cyber attack – 59% say this.[12]

TRUST

Will customers keep coming to you if they feel their data isn't safe? 64% of consumers say they are unlikely to do business with a company where financial or sensitive data was stolen.[13]

https://safenet.gemalto.com/resources/data-protection/customer-loyalty-data-breaches-infographic/

FINANCIAL

The mean cost of a breach is £3,100 – or £22,300 for large firms. The cost comes both in terms of directly addressing the breach and handling

PRODUCTIVITY

You will need to divert resources – whether it's from marketing or other activity – while you recover from a data breach. The drain on

LEGAL

Businesses who fail to handle data correctly could well find themselves in breach of the law.

the aftermath and strengthening security.

productivity is one reason why the cost of this sort of crime is set to be £5 billion by 2021.[14]

GDPR

The highest profile breach so far came from British Airways. **The airline was fined a record £183 million** after a breach of its security saw **information of about 500,000 customers taken.** The data included credit card details, names and addresses, login information and travel bookings.[15]

HOW TO PROTECT YOUR BUSINESS

The personal data of customers and clients is highly valuable to criminals and they're always looking for new ways to get their hands on their valuable resources. While businesses can never fully eradicate the risk – it is possible to reduce the chances of falling a victim to this sort of crime.

Train staff

It's estimated that more than 90% of breaches come from human error and you're only as safe as your workforce allows. Pay special attention to spotting common issues and best practice with password management.[16]

Have a plan/policy

Make it visible to everyone who needs it and regularly update and refine it.

Encrypt and backup key data

Restrict access to areas where key paperwork is stored.

Correct disposal

Invest in security software

Don't skimp on this. Your data is worth saving and investing here – online AND offline – could avoid a bigger issue down the line.
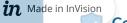
Update software

Ensure your software is regularly updated so that it's catching the latest issues.

Update passwords

Ensure all passwords are regularly updated.

Shred key paperwork

Destroy documents as soon as they aren't needed. Also keep a record of what needs to be destroyed and when.

Ensure that hard drives and physical storage items such as USBs are properly disposed of.

Be wary of BYOD

'Bring your own device' might make it difficult to control the equipment being used.

Open communication

Encourage open communication so staff know where and how to raise concerns.

Insurance

Take out insurance that covers you in case of data breaches.

Use privacy screens

Avoid people seeing confidential data on screens.

Protect your printer

Use a password for your printer and collect all printed material immediately.

Restricted access

Restrict access to store rooms to necessary personnel.

We protect what matters.

Shred-it®

SOURCES

1. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

2. https://www.kellysrm.co.uk/news/paper-data-breaches-40-of-all-data-breaches/

3. https://www.restore.co.uk/Datashred/Resources/News/secure-shredding-history-stats-and-facts

4. https://www.theguardian.com/technology/2018/oct/08/google-plus-security-breach-wall-street-journal

5. https://www.computerweekly.com/news/1280095449/Wolverhampton-City-Council-breaches-DPA-with-document-skip-dump

6. https://www.bbc.co.uk/news/uk-scotland-south-scotland-19561192

7. https://www.theverge.com/2018/8/24/17776836/tmobile-hack-data-breach-personal-information-two-million-customers

8. https://www.theguardian.com/society/2017/oct/16/nhs-data-loss-scandal-deepens-with-162000-more-files-missing

9. https://thenextweb.com/facebook/2018/10/12/facebook-data-breach-details/

10. https://techcrunch.com/2018/11/30/starwood-hotels-says-500-million-guest-records-stolen-in-massive-data-breach/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=UQqekQuKxka9SNMkNxdRSA

11. https://www.theguardian.com/uk-news/2017/dec/26/government-admits-losing-thousands-of-papers-from-national-archives

12. https://www.spamtitan.com/web-filtering/new-research-reveals-extent-of-reputation-loss-after-a-cyberattack/

13. https://safenet.gemalto.com/resources/data-protection/customer-loyalty-data-breaches-infographic/

14. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

15. https://www.theverge.com/2019/7/8/20685830/british-airways-data-breach-fine-information-commissioners-office-gdpr

16. https://blog.getusecure.com/post/the-role-of-human-error-in-successful-cyber-security-breaches

Made in InVision