PayePass eGuide

PayePass

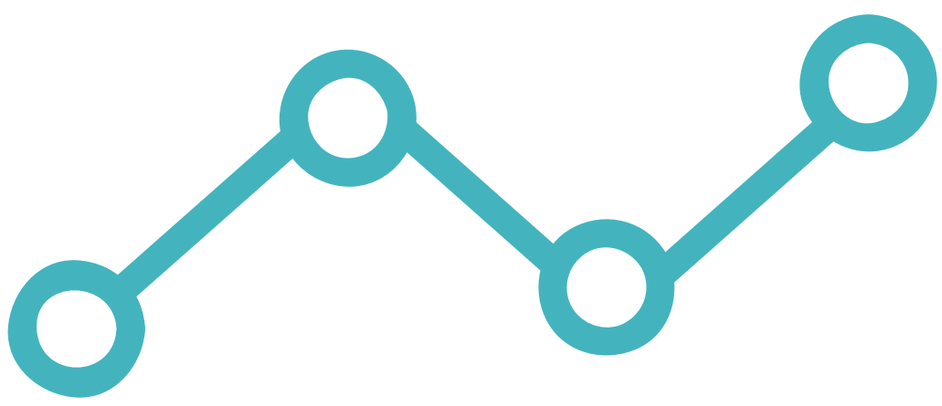
HOW TO REACT TO A DATA BREACH

KEY STEPS ON HOW TO REACT AND THE IMPORTANCE OF PREPARATION

Whether caused by one isolated incident, a series of incidents or a cyber-attack, data breaches result in considerable time and resources to resolve. The potential damage to a business can be extensive, from financial costs and operational downtime to considerable reputational harm.

With such wide-ranging consequences it pays to be prepared. However, according to recent research, only 19% of businesses strongly agreed that they are prepared to respond to a data breach caused by their remote working staff.

Even businesses that believe they are well prepared are likely to have some operational weaknesses. It is not uncommon for businesses to not truly appreciate the obstacles in overcoming a breach.



Things to consider to mitigate the obstacles:

- the complexity of notifying data subjects
- managing communications
- notifying regulators
- implementing a raft of operational processes and procedures
- bringing in specialist support

Organisations tend to focus on prevention of data breaches – investing in systems and software to minimise the risk of a breach. However few go further and prepare for the response required should a breach occur. Data breaches can happen at any time to any business of any size. Global news stories of attacks are constant and there are no indications that they will decrease. On the contrary, all indications are that they will increase.

Preparation is key

It's important that you're in a position to immediately respond the moment you become aware of a breach. The majority of decisions that need to be made in reaction to a data breach can be pre-determined and prepared in advance. Resulting in a less pressured situation should a stressful crisis occur. A pre-approved process will ensure that you know who to consult, including:

- Legal advisors
- Insurance experts
- Public Relations
- Response consultants
- Regulators

So, what can you do now?

- Understand and review the data you hold for all data subjects such as customers and employees.
- Remove duplicate records
- Split joint account names to individual data subjects
- Do you hold current and full contact details?
- Do you actually need to retain the data any longer?

How do you communicate a data breach to data subjects?

Most businesses will immediately resort to traditional methods of communication and send out letters or email notifications. However, more and more businesses are reviewing other and multiple communication channels they could use in the event of a data breach and how this affects wider communication plans to media, stakeholders and regulators.

Speedy and clear post-breach communications can mitigate the consequences of a breach, so businesses should consider using as many options as possible.

Email

For speed, email communication continues to be the most popular distribution channel. However, be mindful that people are now very cautious of phishing emails and are viewing any unexpected email with a high degree of suspicion. Also, do not ignore the possibility of a cyber-attack disabling your servers with the consequences that you may not be able to access the data for sending emails or receiving emails. Do you have a data back-up that you can access in worse case scenarios?

Post

Communication by post is increasing, as letters are viewed with a greater degree of consumer confidence, but post is slower than email and might not be opened or opened immediately. As with email, you will need to be able to access your data to send letters by post.

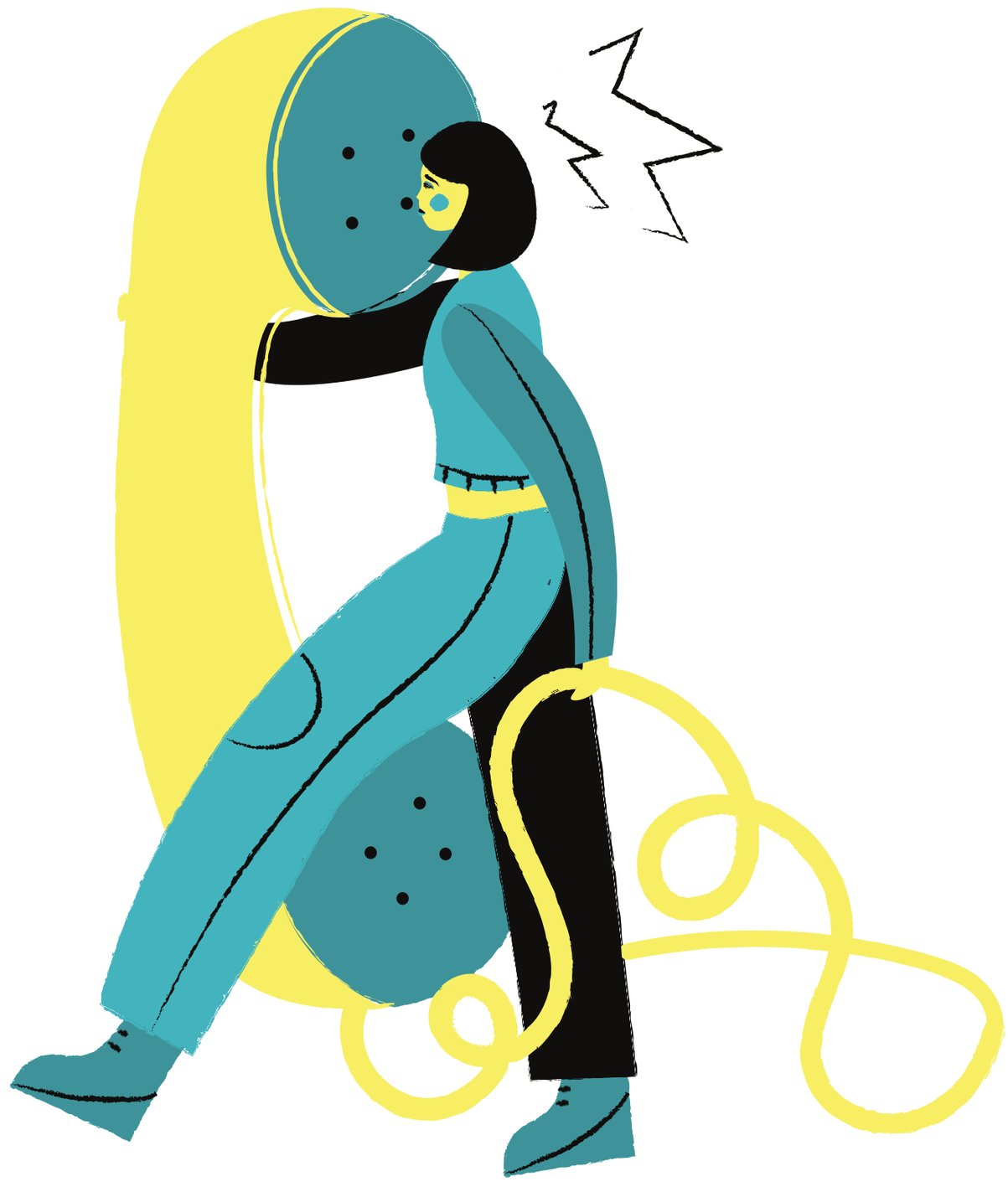
Website

What if your website goes down? Consider having a microsite ready to go live to provide important information. You could also consider a live chat or chatbot function to respond to any immediate queries.

Telephone

A data breach will inevitably result in a significant increase in the number of telephone calls to your business, but what if your telephone system is compromised? Having scalable call centre support could be invaluable as many people want to talk to someone to be able to ease their concerns.

All businesses should plan ahead to consider how they will deal with a huge increase in the need to deal with incoming and outgoing communications. Does your business have the internal resources, knowledge, and skills? If not, start to scope out what this might look like for your organisation. You may even want to consider briefing a specialist to support you through your response.



In conclusion

As we have identified, preparation is key! What is your current policy/process? Are your staff briefed? There is plenty that can be done now and as part of a strategic plan to minimise your risk should any form of data breach occur within your business.

Get in touch...

0151 440 2993

askus@payepass.com

www.payepass.com