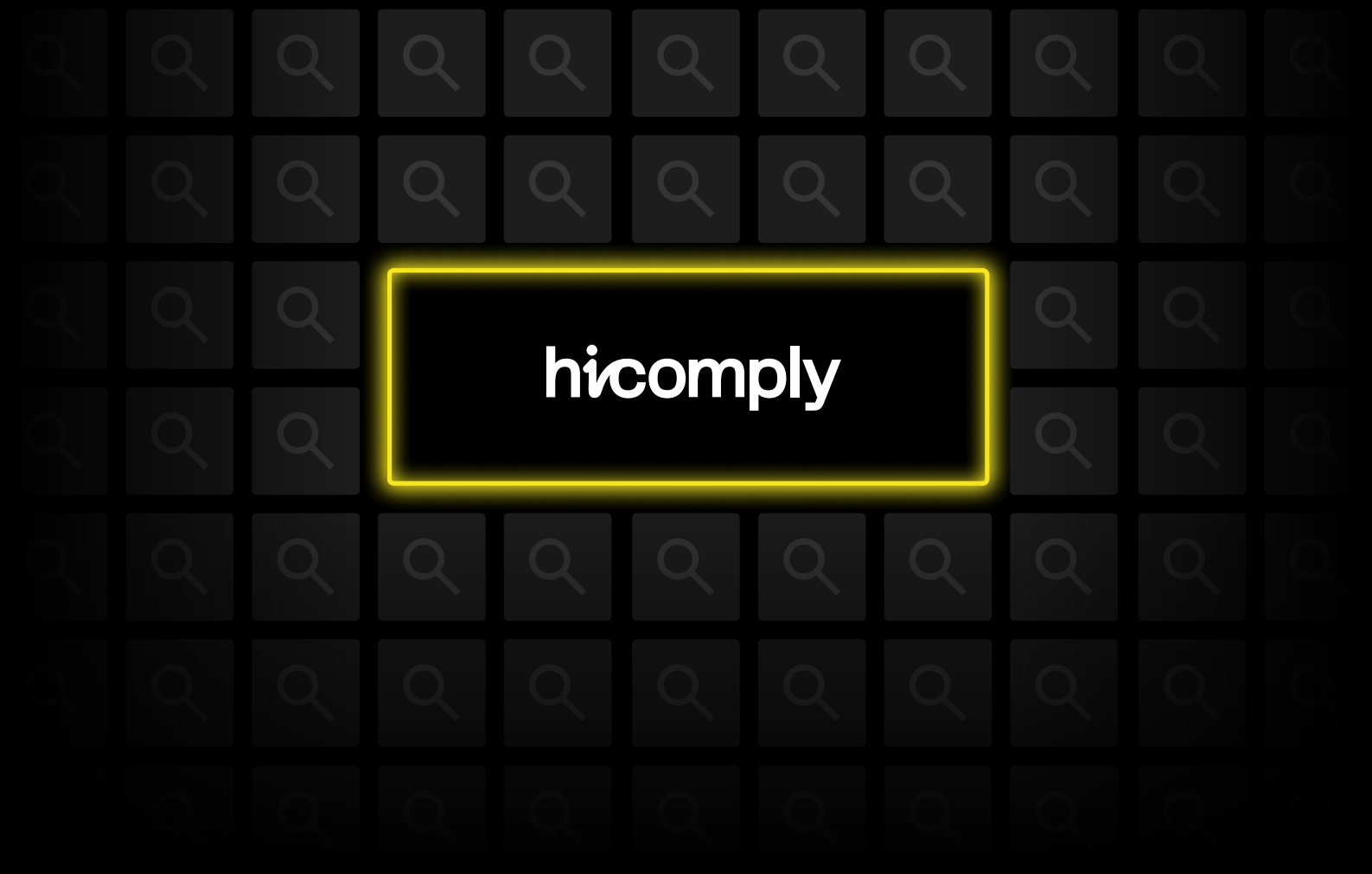
hicomply

A guide to preventing and handling data breaches

- Discover what constitutes a data breach and when a breach must be reported
- Learn how to set up your information security posture to prevent data breaches
- Find out how ISO 27001 certification can support your business security

Contents



Introduction

In 2021, a record number of users used Google to search for information around data breaches, the impact and what can be done to stop breaches occurring.

This could be a direct response to an increase in hackers trying to find flaws in the cyber defences of businesses and gain access to sensitive data. While scammers also regularly target individuals, for example by impersonating a family member to ask for money , it's often businesses that bear the brunt of a data leak.

In these scenarios, businesses that have been victims of a data breach commonly have to pay out substantial sums to both government and the victims.

To make sure that you have all the information you need about data breaches and the ISO 27001 certification designed to protect your business information, our Hicomply experts have answered nine key questions about data breaches.

What is a data breach?

A data breach is the release of private or sensitive information by an organisation. This can be released in either an intentional and unintentional means.

Many of the most damaging data breaches take place when an unauthorised party gains access to confidential information, often for personal gain. Most data breaches are caused by malicious software (known as malware), hacking attacks or insider leaks.

For example, a breach could occur if a member of staff clicks on an email attachment that is infected with malware. The malware, downloaded by accident, could go on to infect their computer and gain access to the business network or any information stored on the computer itself.

When must data breaches involving personal data be reported?

A breach must be reported to the Information Commissioner's Office (ICO) should it represent a significant threat to the right and freedoms of the individuals involved. This is defined as leading to potential discrimination, damage of reputation, financial loss or loss of confidentiality.

If the risk poses a significant threat to the individuals involved, for example the loss of confidential details that may lead to financial implications, the organisation must make every effort to make them aware of the situation without hesitation. In order to avoid this, implement our top tips to keep your data safe.

How much time do you have to report a data breach?

According to the ICO, it is the duty of all organisations that once they have become aware of a potential data breach, they must report it within 72 hours. You can report a data breach here if you have been impacted.

How much compensation are people entitled to if their data has been leaked in a breach?

The amount of compensation individuals are entitled to will differ greatly depending on the type of breach that has taken place. Factors which will influence this include:

- The potential risk that has been incurred due to the data leak
- The distress that is has caused the victim.

GDPR enables individuals to claim compensation of up to £2,000 if their personal data has been part of a breach, lost or mis-used, however claims can be much higher if there has been significant damage caused.

What are the consequences of a data breach?

A person's data being breached can lead to forgery of accounts using all personal details that have been stolen.

People stealing personal data can also have access to an individual's banking details and passwords, meaning more accounts being created in their name or money being stolen from their account.

For the business that have suffered a data breach, they may be faced with a heavy fine, major damage to their reputation and legal action.

What is ISO 27001?

The ISO 27001 is an internationally recognised standard of managing information security systems, having been standardised in 2005 and updated in2017.

Created by the International Organisation for Standardisation and the International Electrotechnical Commission, the standard uses a risk-based approach to secure organisations sensitive data and keep it safe.

What is ISO 27001 certification?

ISO 27001 certification is awarded to companies that provide quality data security to clients. This can benefit a business through greater customer satisfaction, legal compliance, and improved risk management.

An ISO 27001 certificate will provide customers with the feeling of trust that their data is safe with the company. ISO 27001 certification must be renewed every three years.

How much does ISO 27001 certification cost?

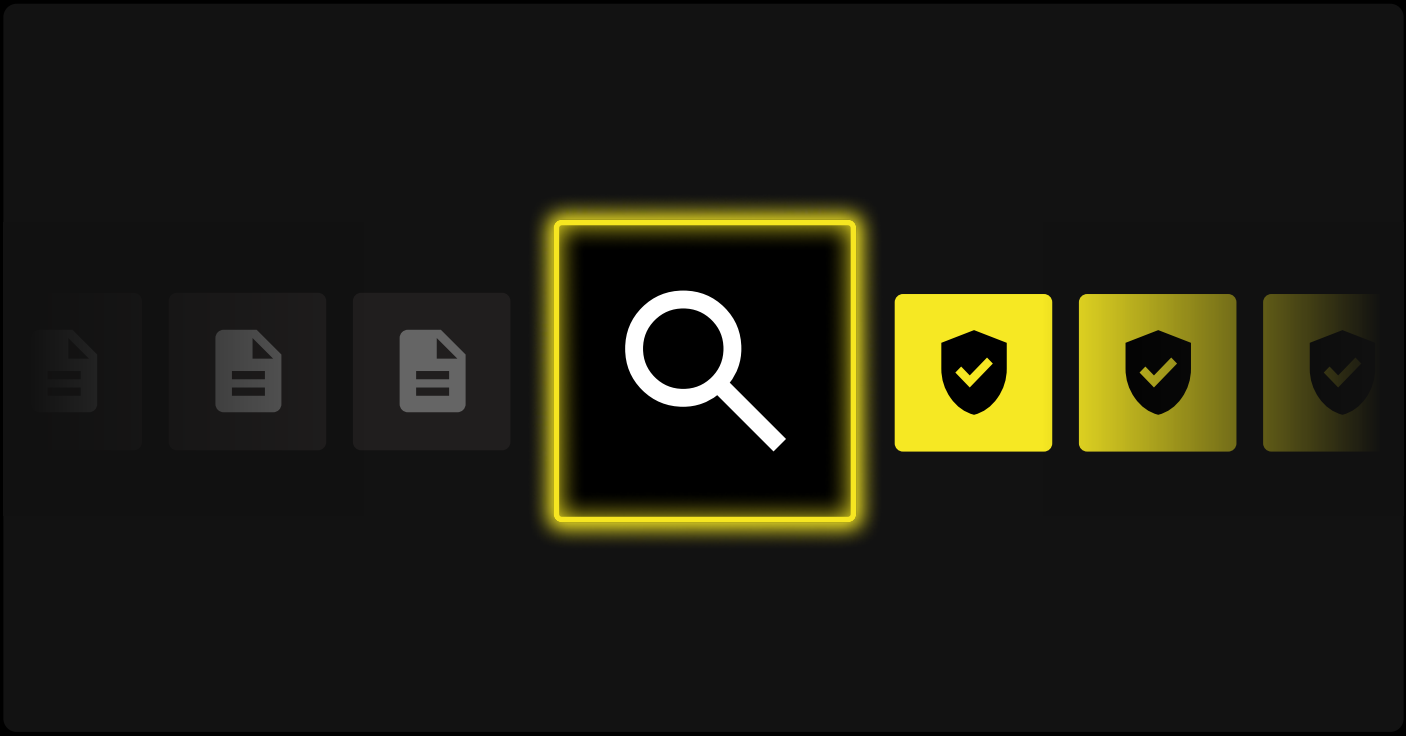
When calculating the cost of ISO 27001 certification, factors such as number of employees and audit time need to be taken into consideration.

In general, certification audits will start out at around £3,000 and will cover up to almost 50 employees. When employee numbers reach the mid to late 1000s then it can cost over £13,000. For a more accurate quotation for your business, contact Hicomply.

How is an ISO 27001 audit run?

There are both internal and external ISO 27001 audits that can be carried out. Internally, they are used monthly or annually to ensure that standards put in place, in order to achieve or maintain certification, are stringently adhered to.

An external audit is conducted by a certification body every three years in order to gain or maintain certification. Hicomply's software provides the tools to guide you through the internal auditing procedure.



Conclusion

Implementing ISO 27001 can enable you to protect your business, preventing data breaches and the consequences of those breaches. For more information about data breaches and the benefits of ISMS, visit the Hicomply blog or take some time to read our infographic on the benefits of ISO 27001.

To learn more about the process and how Hicomply's software can make ISO 27001 certification quick, simple and hassle-free, get in touch with the team.

www.hicomply.com