COMMON CYBER-SECURITY MEASURES IMPLEMENTED BY UK ORGANISATIONS

Every year, the 2022 Cyber Security Breaches Survey, commissioned by the Department for Digital, Culture, Media & Sport as part of the National Cyber Security Programme, provides valuable insights into cyber-security and data breach trends reported by UK employers.

This infographic provides information on the actions organisations have taken to bolster their cyber-security efforts in the last 12 months.

CYBER-SECURITY CONTROLS AND POLICIES

The most common controls organisations have implemented to bolster their cyber-security include:

Having up-to-date malware protection

Using firewalls that cover the entire IT network, as well as individual devices

Restricting IT admin and access rights to specific users

Enforcing a password policy that ensures that users select strong passwords

Backing up data securely using a cloud service

36% of businesses and **35%** of charities have a formal policy or policies covering cyber-security risks. Common concerns cyber-security policies address include:

- **The process by which data is supposed to be stored**
- **The staff who are permitted to do on their organisation's IT devices**
- **The ways in which remote or mobile working affects cyber-security**
- **The items that can be stored on removable devices, such as USB sticks**
- **Use of cloud computing**
- **Use of network-connected devices**
- **Use of personally owned devices for business activities**

Of the organisations that have formal policies covering cyber-security:

44% of businesses and **47%** of charities have not reviewed their cyber-security policies within the last six months.

22% of businesses and **17%** of charities have not reviewed their policies in the last year.

RECOGNISING SUPPLIER RISKS

Only **13%** of businesses and **9%** of charities have formally reviewed the potential cyber-security risks presented by their **immediate** supply chains.

Only **7%** of businesses and **5%** of charities have included their wider supply chains in such a review.

UNDERSTANDING GOVERNMENT INITIATIVES

49% of businesses and **40%** of charities have implemented at least five of the government's '10 Steps to Cyber-security.' This represents a **1%** drop for businesses and a **5%** drop for charities compared with last year's responses, but a total decrease of **20%** for businesses and **23%** for charities since the 2020 survey. It's worth noting that these steps were updated by the National Cyber Security Centre between the 2021 and 2022 surveys.

Only a combined **4%** of businesses and charities have implemented all 10 steps. This is identical to 2021 findings but down from **12%** and **14%**, respectively, in the 2020 survey.

riskhub
the business resilience people