HOW ORGANISATIONS RESPOND TO CYBER-ATTACKS

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 illustrates how prepared organisations are to respond to cyber-incidents. Specifically, this infographic visually represents what types of cyber-incident response procedures organisations have in place, how often their most disruptive breaches are reported and what additional cyber-security measures are implemented in response to an incident.

UNDERSTANDING AND RESPONDING TO THE CYBER-INCIDENT

93% of businesses and **89%** of charities have at least some degree of cyber-incident response procedures in place. The most common procedures include:

- **Informing directors/ trustees/governors of the incident**
- **Assessing the scale and impact of the incident**
- **Keeping an internal record of the incident**
- **Informing a regulator of the incident** (when required
- **Debriefing to record lessons learnt from the incident**
- **Attempting to identify the source of the incident**

Only **40%** of businesses and **25%** of charities reported their most disruptive breach outside their organisation, and even then, it's often only to their cyber-security providers. This indicates that cyber-threats may be underreported and more common than currently known.

In response to experiencing a breach, only **62%** of businesses and **57%** of charities have taken steps to protect their organisation from future attacks.

These efforts include:

- **Additional staff training or communications**
- **Installed, changed or updated antivirus or anti-malware software**
- **Changed or updated firewall or system configurations**