Cyber attacks have become more frequent. Among the 46% of micro and small businesses identifying any breaches or attacks, more now experience them at least once a week (32%, vs. 22% in 2017).

The nature of cyber attacks has evolved. Among those identifying breaches or attacks, 86% had phishing attacks (vs. 71% in 2017), 24% were impersonated and 18% had malware (including ransomware).

Cyber security is increasingly important for smaller businesses. 79% of these businesses say that cyber security is a high priority for their management boards, up from 69% in 2016.

Almost all smaller businesses report having technical controls. This includes having up-to-date malware protection (87%), network firewalls (82%), restricting IT admin rights (80%) and password policies (80%).

Most smaller businesses are seeking information. 54% sought information in the last 12 months (vs. 43% in 2016). But just 16% have heard of the National Cyber Security Centre’s Small Business Guide.


For further cyber security guidance for your business, visit the National Cyber Security Centre website (www.ncsc.gov.uk) to find:

- the Small Business Guide drafted especially for smaller businesses (www.ncsc.gov.uk/smallbusiness)
- the government-endorsed Cyber Essentials scheme, which enables organisations to be certified independently for having met a good-practice standard in cyber security (www.cyberessentials.ncsc.gov.uk).
EXPERIENCE OF BREACHES OR ATTACKS

46% of micro and small businesses identified cyber security breaches or attacks in the last 12 months.

£3,110 is the average annual cost for micro and small businesses that lost data or assets after breaches.

Among these 46%:

32% were attacked at least once a week (up from 2017)
26% needed new measures for future attacks
20% lost staff time dealing with the breach

MANAGING RISKS

69% have cloud backups (up from 2018)
50% have applied technical controls in all five Cyber Essentials areas
41% have staff whose job role includes information security or governance (up from 2016)
37% have cyber security policies (up from 2016)