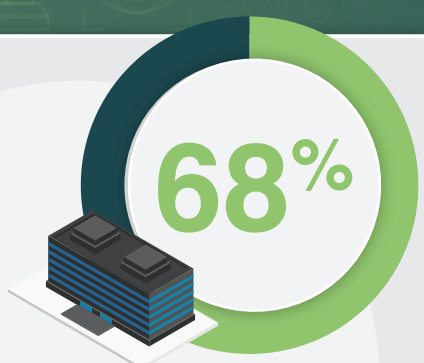
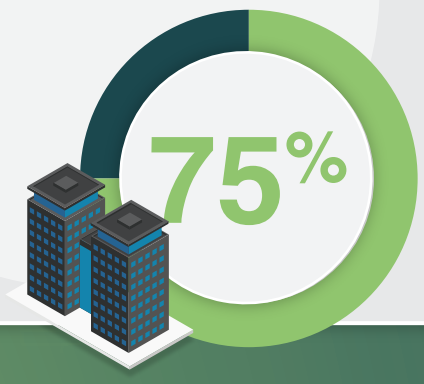
Are businesses more exposed to cyber-crime than ever before?

01 Frequency...

68% of mid-sized and **75%** of large-sized businesses have reported a breach/attack in the last 12 months.





02

32% of businesses experience security issues at least once a week in 2020 (vs. 22% in 2017).

04 Attack vectors

Most disruptive attacks or breaches identified...

Fraudulent emails or being directed to fraudulent websites:

67%

Impersonating organisations in emails and online:

11%

Virus, spyware and malware:

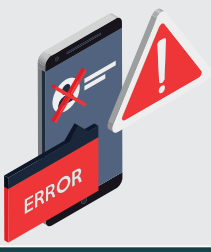
7%

Hacking or attempted hacking of bank accounts

4%

Unauthorised use of computers, networks or servers by outsiders

3%

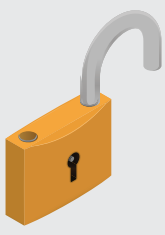


Ransomware:

2%

Unauthorised use of computers, networks or servers by staff:

1%



Other:

3%

05 Consequences of being attacked

65% do not carry out cyber security risk assessments.

36% do not monitor gaps in their security.

06 Pull on IT resources[1]

IT teams spend, on average, **39 hours** (5 working days per month) monitoring endpoints.

07 10 steps to mitigate cyber security risk[2]

01	02	03	04	05
Constantly evaluate your Network security	Defend your network perimeter	Increase user education and awareness	Malware prevention policies to establish defences	Control access to removable media controls

06	07	08	09	10
Apply security patches and ensure Secure configuration of all systems	Manage user privileges	Establish Incident report management processes	Continually monitor all systems and policies	Establish Home and mobile working policies, protect data in-transit and in-rest

All information provided from: DCMS Cyber Security Breaches Survey 2020 - unless otherwise stated.
[1]Alien Vault 2019 Endpoint Security Survey.
[2]www.ncsc.gov.uk.

exponential-
APPLIED INNOVATION