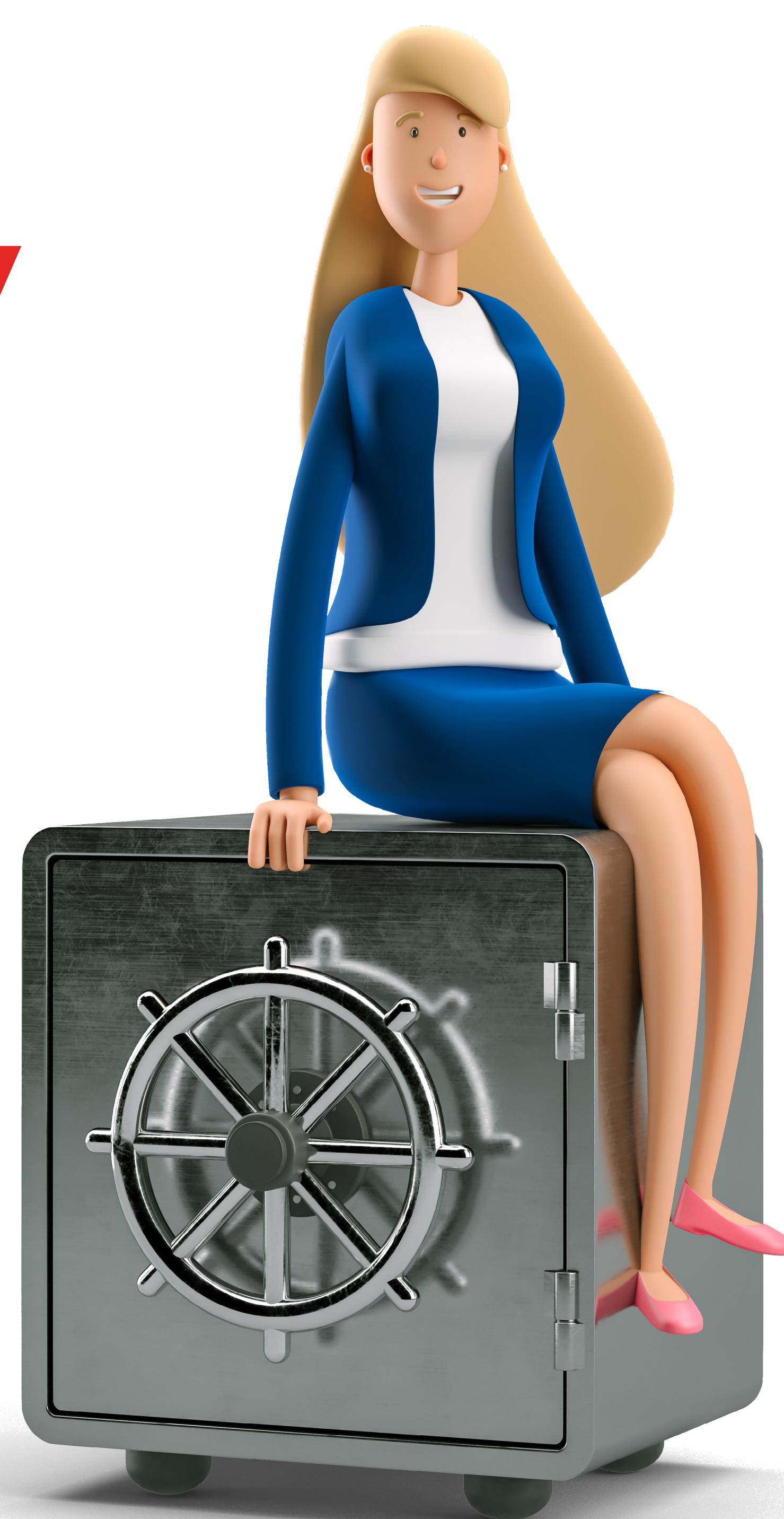# The importance of Cybersecurity for SMBs

Triggered by the global pandemic, the rapid transition to working from home forced businesses to scramble to support a larger remote workforce. The speed at which this was executed means that certain security measures and requirements inevitably fell by the wayside.

At the same time, cybercriminals found a new opportunity for attack with remote workers and improperly secured connections and technologies. Together, these trends created a more vulnerable environment affecting the cybersecurity defences of many organisations.

1/3
Around **1/3** companies transitioned **81-100%** of their employees to remote working

2/3
More than **2/3** companies moved **61%** or more of their workforce to a work from home environment

44%
44% admit they haven't provided cybersecurity training focused on the potential threats of working from home

68%
68% have not deployed a new antivirus solution for work-issued devices

45%
45% have not analysed the security or privacy features in the software tools considered necessary for remote working

However, IT leaders acknowledge the number of challenges of cybersecurity in the move to working from home.

55%
55% see the need to train employees on how to securely and compliantly work at home as a priority

53%
53% acknowledge that setting up work or personal devices with new software for employees to work remotely is a challenge

1/2
Over **1/2** cited the need to shift to a new, remote model of communication and/or collaboration among employees

47.5%
47.5% companies are struggling with limited IT resources to serve employees working from home

45%
More than **45%** see finding the right cybersecurity tools to support home workers as a key challenge

36.6
36.6% are concerned about how to enable their staff to achieve a work/life balance

Since the shift to remote working, businesses have encountered a range of security issues.

1/5
Around **1/5** companies have faced a security breach caused unintentionally by a remote worker

24%
24% have had to spend money unexpectedly to resolve a security breach or malware

1/3
Around **1/3** admitted to using personal devices rather than company devices leaving them more vulnerable to breaches

18%
18% admit that cybersecurity is not a priority for employees