BOARD-LEVEL BRIEFING

7 ways boards can promote secure hybrid working

Hybrid working is here to stay. What are the implications for security – and how can boards and leadership teams keep their organisations safe?

The positives of **hybrid working**

68% of enterprises say employee output has improved[1]

83% of workers prefer it that way[2]

35% of organisations say they have the metrics that prove the benefits[1]

63% of companies have adopted a hybrid model[2]

The level of threat to **cybersecurity**

83%
of global IT teams say hybrid working is a 'ticking time bomb'[3]

72%
Ransomware incidences on corporate networks increased by 72% in the first half of 2020[4]

278
The number of vulnerabilities in unpatched devices has risen to 278[5]

1/3
Email based threats surged by almost a third in the first 100 days of lockdowns[6]

36%
the highest growth in cyberattacks is in EMEA [7]

$4.24m
The average cost of a data breach reached $4.24 million per incident in 2021, the highest in 17 years[8]

Actions that boards should take now

1. Encourage an open dialogue
Encourage a working environment where all employees feel they can be open about potential breaches in hybrid scenarios – more transparency increases more continual learning.

2. Demand more frequent security briefings reviews with leaders
Insist on more regular briefings with management teams and security experts – at least monthly – to get a better handle on where and how new threats are emerging.

3. Ask employees what they think
Initiate an assessment of employees' perception of new security issues: establish how well they understand the threat related to hybrid working, risks associated with all the devices they use (including devices like smart speakers), and what their responsibilities are.

"Encourage a working environment where all employees feel they can be open about potential breaches"

4. Encourage new cybersecurity policies for hybrid working
Use findings from assessments and reviews to push for new or revised cybersecurity policies, tailored specifically to how employees are changing the way they work.

5. Back policies with training
Support leadership teams to invest in continual training, education and culture change programmes to make sure employees understand and engage with new security policies.

6. Back investment in fit-for-purpose technology
As a minimum, systems required to protect a hybrid workforce should include secure VPNs, multi-factor authentication and endpoint monitoring.

7. Adopt secure hybrid working at board-level
Lead by example and use a specialist board portal to keep work on sensitive and confidential information secure – wherever board directors choose to work from.

Hybrid working requires a new security-aware culture across organisations.

Download the full report on How to manage the impact of hybrid working on cybersecurity

Download now

admincontrol.com

Admincontrol

References: 1. Omdia, The Future of Work: The Business Imperatives Shaping the New Normal, 2021 **2.** Accenture, The Future of Work: A hybrid model, 2021 **3.**HP Wolf Security, 2021HP Wolf Security, Rebellions and rejections report, 2021 **4.** Skybox Security, 2020 Vulnerability and Threat Trends Report **5.** Ivanti, Ransomware Index Spotlight Report, 2021 **6.** Mimecast. The State of Email Security 2020 **7.** Check Point, Cyber Attack Trends 2021 Mid-Year Report 2021 **8.** IBM and Ponemon Institute, Cost of a Data Breach Report 2021.