Admincontrol

Handbook: How to manage the impact of hybrid working on cybersecurity

admincontrol.com

Quick overview

Hybrid working is one of the buzz terms of the moment – offering organisations the opportunity to reduce costs, boost productivity and increase employee satisfaction. But what are the implications for security? How can organisations adapt, achieve all the positives, but also make sure they don't expose themselves to unnecessary and potentially catastrophic risk?

This guide will help you answer those questions. We look at:

- Why threat levels are increasing because of hybrid working
- The security measures needed across all levels of organisations
- Specific measures needed to keep board-level working secure
- The changes needed in corporate governance to drive a cybersecurity aware culture

The current level of threat

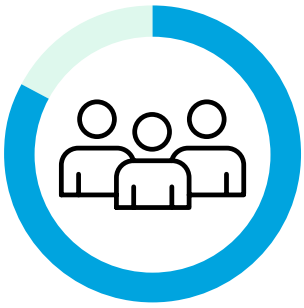
The growth of hybrid working

The concept of hybrid working is simple: it allows people to split their time between the workplace and home to help them operate more productively and efficiently.

According to many research reports, there are strong reasons to suggest that this ambition is an achievable reality. One recent survey by the analyst group Omdia confirmed that 68% of enterprises believe employee output has improved since the mass move to remote working. Another 35% said they have the metrics to prove it[1].

There is also significant evidence that employees are on board with the idea. In 2021, Accenture revealed that 63% of high-growth companies have already adopted a hybrid model and 83% of workers prefer it that way[2]. Other experts, including Gartner, have urged all organisations to tap into this sentiment and get ready for managing hybrid workforces[3].

63% of high-growth companies have already adopted a hybrid model



83% of workers prefer hybrid working

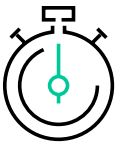
Associated threats

This is all positive. However, it is also clear that hybrid working exposes organisations to increased risk of security breaches. Problems arise from users toggling between secure and insecure networks, not following IT security policies when at home, weak passwords, using unauthorised personal devices and bringing malware into the office when they log back in the corporate network.

A recent survey by HP Wolf Security found that 83% of global IT teams believe this has created a 'ticking time bomb' for corporate network breaches[4]. The biggest threats are coming from:

- Ransomware
- Email based attacks
- Attacks against publicly exposed systems
- Exploited vulnerabilities in unpatched devices
- Data leakage
- Leaked credentials

Ransomware has surged in particular because cyber criminals and government-backed spying agencies are exploiting the fact that many people are working from home – one report found that incidences on corporate networks had increased by 72% in the first half of 2020 alone[5]. Another report by cyber security firm Ivanti states that attackers are also exploiting new vulnerabilities associated with older unpatched devices, bringing the total number of vulnerabilities associated with ransomware to 278[6].



83% of global IT teams believe hybrid working has created a 'ticking time bomb' for corporate network breaches

The average cost of a data breach reached $4.24 million per incident in 2021

The question is – how can organisations address the vulnerabilities to reduce threats, while still delivering on their hybrid working ambitions?

Email based threats are also increasing – ranging from phishing attempts where employees could be tricked into opening a malicious attachment or link, to business email compromise (BEC), where attackers impersonate managers and other credible individuals to incite fraudulent financial transfers. A report by Mimecast said that this kind of impersonation fraud surged by almost a third during the first 100 days of the pandemic[7].

There has also been a recent increase in incidences of 'client-side' attacks on the scripts behind publicly exposed websites and applications – with cyber criminals using them as a vector to gain entry to corporate networks.

Overall, these factors combined have contributed to a huge upsurge in data breaches and leaked credentials that are being sold online. One survey estimates that by 2020 the number of stolen and exposed credentials had risen 300% in just two years[8].

There is no doubt that hybrid working, for all its benefits, creates significant headaches for organisations. It seems that Europe is affected in particular. A report by Check Point found that the highest growth in attacks this year has occurred in the Europe Middle East and Africa (EMEA) region (36%)[9].

The impact of such attacks can be huge. Earlier this year, we got another reminder of how real the danger is when a major cyberattack exploited vulnerabilities in Microsoft Exchange. The attack affected many different enterprises, including Norway's Parliament, as well thousands of other organisations globally. This was all at an enormous cost. This year, IBM revealed that the average cost of a data breach reached $4.24 million per incident in 2021, the highest in 17 years[10]. Cybersecurity ventures estimates ransomware damages to reach $20 Billion by the end of 2021[11].

Keeping the whole organisation secure

Security policies

There are many practices that boards and management teams can put in place to reinforce security for hybrid working. This needs to start with developing a cybersecurity policy and ensuring all employees and stakeholders are fully engaged.

As part of this, it's essential to educate your employees on the importance of being aware of the threat, and how to counter it, including identifying and responding appropriately to phishing attempts, and physically protecting devices from theft. Continual training and reviews of employee cybersecurity awareness, tailored to the new reality of hybrid working, are key to making this happen.

Such policies should also focus on encouraging users to create stronger passwords that are more like 'passphrases' – for example 'I love the smell of coffee in the morning'.

Security advocates now recommend this approach because it is much more difficult for hackers to crack using computers: typically, a computer will take more than 10,000 centuries to guess a passphrase, compared to just four hours for a traditional password containing 8 characters, upper and lowercase letters, numbers and special characters.

Other practical considerations and tips

There are also technical measures, investments and strategies that leaders need to consider to support safe hybrid working. As a minimum, this should include:

IMPLEMENTING SECURE VPN ACCESS

A Virtual Private Network (VPN) is an encrypted private network that extends over a public network. It is a vital tool for protecting hybrid working, enabling you to control remote logins and introduce highly secure access to the enterprise network for any user, from any device, and from any location. According to research, business use of VPNs rocketed by 165% in the first month of Covid 19 lockdowns.

DEPLOYING MULTI-FACTOR AUTHENTICATION

As well as strengthening passwords, it is also advisable to introduce a stronger, multi-layered means of verifying the identity of all users. This means that you only grant access to a website or application after users successfully present two or more pieces of evidence, which can include a password, security token, memorable word or a biometric identifier (such as a fingerprint). Education and enforcement is again important though. Most people don't currently use two or multi-factor authentication in their personal and professional lives. Google recently revealed that less than 10% of Gmail account holders enable its 2FA option, prompting the firm to announce this year that it's going to auto-enrol 150 million users on the service[12].

INTRODUCING ENDPOINT MONITORING

Endpoint monitoring is important because it enables you to analyse live and historical footprints left by hackers on your systems to identify evidence of malicious cyber activity. For example, it will enable your organisation to identify where multiple login attempts by an automated system have been made. In 2020, Gartner identified this as one of the key security areas that enterprises should focus on during and beyond the pandemic[13].

LOOKING BEYOND THE OFFICE NETWORK

The increasing use of the Internet of Things in private households is also an area of new vulnerability. This means assessments of hybrid working security should also look at where devices connect business PCs to the home network and can lead to blind spots. An unsecured home router, smart speaker or even a 'smart' coffee machine with a standard password connected to the company's network can suddenly become the way in for those who want to do harm. Any security strategy needs to consider the full range of IoT devices connected to a network – home or otherwise.

APPLY A ZERO TRUST STRATEGY

In the modern Hybrid working place you can no longer solely rely on the traditional model of trusted networks and devices. Instead, organisations are increasingly turning to a 'zero trust' model whereby they do not automatically trust any device, system or user trying to access their resources. The advantage of applying this model is that it enables you to detect and stop attacks in their early stages – before the attacker is able to breach your entire network. To get started, you can follow the principles laid out by the UK **National Cyber Security Centre** or frameworks like **CIS Controls v8**.

APPLYING ANOTHER LAYER TO SPECIALIST AREAS

It's important to not just look at security in a general sense but to also investigate specialist areas of the business and where necessary add another layer to your security review specific to that solution or function. This is especially vital where the use of digital hybrid working tools has only recently become the new norm.

The Head of Security at Admincontrol, Ole Martin Refvik.

"In my opinion, everyone should have 2FA in place. The top management need to put security on the top of their agenda and make sure their employees use 2FA."

Keeping board-level working secure

Another key area to review is board-level communication and collaboration within a hybrid working environment. Typically, board members are used to traditional, analogue ways of working and have only recently started getting used to digital tools and the security precautions that they require. By their nature, boards also routinely handle an organisations most confidential information – leaving them potentially more vulnerable to attack.

For these reasons, you also need to support boards in their transition to hybrid working by making sure they adopt secure working practices. The best way to do this it to move away from insecure email and collaboration channels and adopt modern, advanced board portal technology that has board-specific security measures built-in.

As ever, it is also important to introduce secure working policies to make sure all these functions are being used correctly by board directors and that that the policies are being enforced.

This will enable boards to take advantage of functionality that includes:

- Ringfenced communication via secure communication channels with the portal
- Secure storage for all current and historical documents
- Electronic signing for remote approval of board documents
- Two Factor Authentication to restrict access and ensure stringent user verification
- Compliance with GDPR

The need for new corporate governance and a culture change

Adopting the right technology for hybrid working is important if boards want to protect data and lead by example. The story shouldn't end there though. Boards don't just need to look at cybersecurity in terms of how they work – they also need to adopt a leadership position and help to drive and shape a new cybersecurity aware culture across hybrid-working organisations.

Leadership of this kind is crucial to helping make sure that security isn't just perceived as a technical policy that needs to be followed. Boards need to take measures to ensure that security is a key part of the organisations DNA, its corporate governance and its overall mission and performance measures.

As a first step towards achieving this goal, boards should actively pursue regular meetings with management teams and technical security experts within the organisation. This will help them get a clear understanding of the wider business context for security, the impact of breaches, and the potential competitive advantage of well-run security practices that protect systems and data.

Ultimately, this will help to improve decision-making on security at all levels and provide a more sound footing for the safe, secure, hybrid-working organisation of the future.

As a second step, they should also seek to establish a climate of trust and transparency around security. At the moment, most employees are reluctant to report a security threat for fear of reprisal. This is unsustainable and is likely to lead to more breaches going undetected. It could also result in a lack of learning from errors that prevents continual improvement in security management processes. To address this, boards should take on the responsibility of establishing a more open dialogue between employees and managers, encouraging transparency, and driving a more positive cybersecurity aware culture.

Finally, boards should also consider pushing towards making better use of data to improve decision-making on security. This could start by instigating an assessment of the current state of security awareness, attitudes and behaviours across different employee profiles, and comparing behaviours when people are working on or off-site. Boards should also insist on regular access to data on security performance and, where necessary, discuss ways with management teams to change those metrics to make them a better fit for a hybrid environment. Cybersecurity should be a frequent and regular part of the boardroom agenda. Having fit-for-performance metrics is critical to ensuring that those discussions are based on the right insight and are as productive as possible.

Next steps

With attacks increasing in the wake of increased hybrid working, getting security right and promoting a positive culture around the issue is more important than ever. Find out how you can protect your organisation and your critical board-level communications by visiting

admincontrol.com

Get in touch to discover how to keep your board documents safe

Admincontrol's mission is to provide the ultimate solution for decision-makers. The company offers a smart and secure collaboration platform for boards, management and other stakeholders, where they can access, share, discuss and process information efficiently. Admincontrol has over 115,000 active users worldwide.

The company is growing rapidly and is headquartered in Norway with local offices in the UK, Denmark, Sweden, Finland and the Netherlands. Admincontrol is part of the successful Visma Group, a leading European software company.

→ info@admincontrol.com

→ www.admincontrol.com

Sources:

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 Gartner survey, 2020
4 HP Wolf Security, Rebellions and rejections report, 2021
5 Skybox Security, 2020 Vulnerability and Threat Trends Report
6 Ivanti, Ransomware Index Spotlight Report, 2021
7 Mimecast. The State of Email Security 2020
8 Digital Shadows, From Exposure to Takeover, 2021
9 Check Point, Cyber Attack Trends 2021 Mid-Year Report 2021
10 IBM and Ponemon Institute, Cost of a Data Breach Report 2021
11 Cybersecurity Ventures, 2021
12 https://blog.google/technology/safety-security/making-sign-safer-and-more-convenient/
13 Gartner, 7 Security Areas to Focus on During Covid 19, 2020