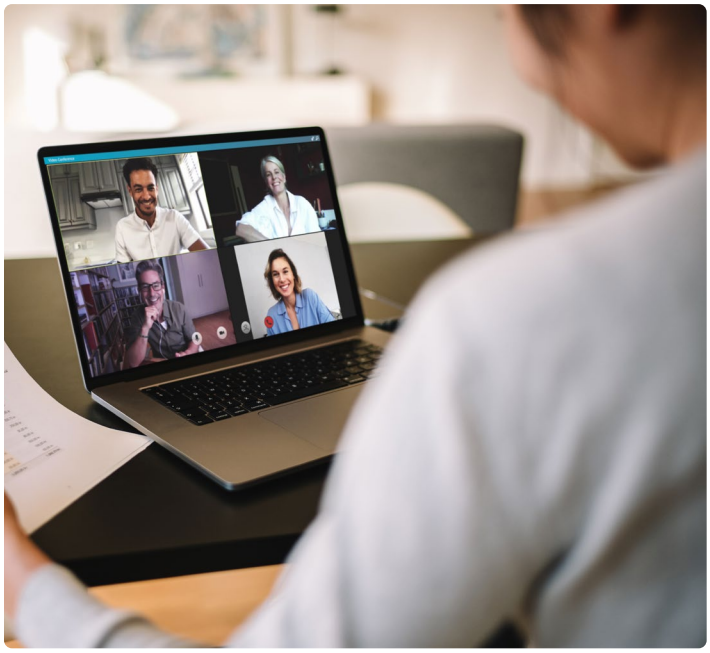
The Risks of Hybrid Working: A Cyber Security Battle

Hybrid working in some form seems set to be the norm for many businesses moving forwards. In fact, according to McKinsey, 90% of global organisations are looking to combine remote and on-site work permanently.

But the last few years of hybrid working were not without their hiccups.

Cyber crime has increased by 600% since the start of the pandemic, and many businesses admit that their plans to tackle this with hybrid working in mind are vague.

So, what are the cybersecurity challenges faced by the hybrid workforce and what can business owners and employees do to combat them?



Loss of oversight

One of the biggest cybersecurity risks continues to be human error.

In April 2020, Google said they were blocking more than 240 million COVID-themed spam messages every day, as well as 18 million malware and phishing emails.

Distractions at home, coupled with the lack of ability to easily ask for IT support as you would in the office, can mean that these (often very convincing) spam emails are opened.

It's easier to develop bad security habits when working from home, and a lack of oversight and accountability could mean that bad habits are brought back into the office.

Unsecured networks

When working solely in the office, organisations can have more control over their network security.

On the other hand, personal laptops and home networks may offer much less protection from malware, making employees possible targets for cyber attacks.

It's also possible that when working from home, employees use their phones as authentication devices or to use some work-related applications they might not otherwise have used in the office.

Upon the return to the office, employers should look out for this and make sure everyone is aligned on the appropriate software to use.

How do we combat these threats?

Employee Training

With many businesses committing to hybrid working for the foreseeable future, it makes sense as a business owner to evaluate current cybersecurity weaknesses in your working-from-home practices.

Start by developing a cybersecurity policy and training your employees to follow it.

Employees should have an in-depth awareness of the vulnerabilities, and how to mitigate risk by responding correctly to phishing emails and social engineering. Ensure that they know how to create strong passwords, use encryption and authentication appropriately, and physically protect their devices.

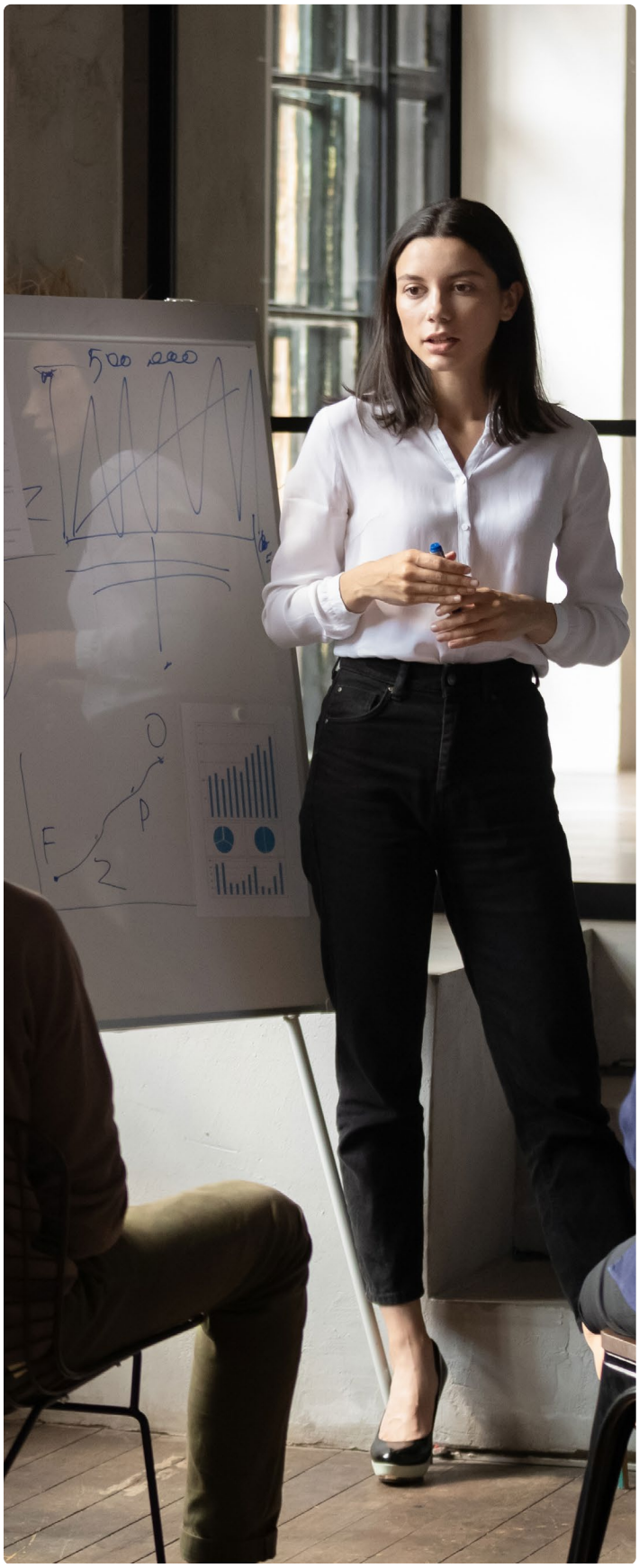
When it comes to incident response plans, businesses should not neglect to factor in home working. It's important to make sure channels of communication are open and that everyone is reachable in some way at all times – particularly the incident response team.

Zero Trust Policy

This model of security has become increasingly popular over the last year.

Its basic premise is that devices and users within the business network should not be trusted by default. Rather, they should be continuously authenticated – ideal when it comes to work-from-home security.

The Zero Trust Model requires micro-segmentation, first-class detection and response, multi-factor authentication, and end-to-end encryption. Done correctly, a move to the Zero Trust Model will be a transformation rather than a retrofit – with the way you manage security transformed from the ground up.



Securing your data

Data is one of the most important fundamental components of any business. Be it employee data or client data, it needs to be secure.

Here at Vinters, we offer a range of services that ultimately protect your data as the vital asset it is. Whether it's managed IT support you need, or a secure virtual server solution, we're here to help.

Check out our blog if you're struggling to choose between Cloud and Dedicated Servers.

Vinters