WHO MOVED MY MOAT?

The cyber security risks of home and hybrid working – what finance and law firms need to know

A special report commissioned by

dohertyassociates

Executive summary

After the UK went into lockdown due to COVID-19, Doherty Associates wanted to know more about the likely impact on its clients in the legal and financial sectors, especially their exposure to cyber attack and data breaches in this new era of home and hybrid working. The company therefore commissioned an external research consultancy to investigate how firms in these sectors had adapted and to see what they were doing to mitigate risk.

The research was undertaken in December 2020 and asked all participants about their experiences since the first nationwide lockdown was enforced on 23rd March 2020.

The cohort was made up of a panel of **IT decision makers** comprising 3,000 people with direct responsibility for IT and data security (e.g., chief technology officers, heads of IT and compliance officers) and 2,000 further employees from the **general workforce** (e.g., associates, directors and lawyers). All were working for private equity or investment and asset management firms, in insurance/underwriting, or in law firms specialising in mergers and acquisitions and commercial law.

> Given that one in five IT decision makers said that a cyber attack or data breach could cost their firm anything from £1m to £50m, the survey results make for eye-opening reading.

Key findings

Since the first UK-wide lockdown in March 2020:

- **85%** of the general workforce say they have worked on both personal and work devices
- **42%** of the general workforce say they have emailed confidential information
- **34%** of the general workforce say they have had no cyber awareness training while working from home
- **25%** of the general workforce say they have experienced or caused a data breach
- **38%** of IT decision makers say their firm has experienced at least one cyber attack or data breach

So why does this matter?

With over half (56%) of IT decision makers expressing a preference for a mix of home and office working, and over one third (34%) of the general workforce reporting that the process of winning new business is actually *easier* when working from home, it seems clear that the 'new normal' of hybrid working is here to stay.

It is therefore crucial that firms act now to mitigate the risk of attack and to keep their employees and clients as secure as possible.

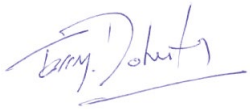
Introduction from Doherty Associates

The way we work has changed forever. More than ever before, technology must support people to do their best work, no matter their location. And it must also keep their information protected and secure, without being intrusive.

While it remains the case that most information leaks out by accident, the chances of this happening have increased during lockdown as the 'attack surface area' now extends out to every device being used, no matter who owns it. At the same time, cyber criminals are finding ever more sophisticated ways to target employees who are working from home.

Here at Doherty Associates, we have many clients in the legal and financial sectors, where security and trust are paramount. We wanted to understand more about the challenges they've been facing due to the rapid rise in home working, so we commissioned a study examining the cyber and data security practices of a 5,000-strong cohort working in private equity, asset management, insurance and underwriting, and corporate law.

In this report, we indicate where the greatest risks lie and the actions firms can take to keep their business, their people, and their data safe.



Terry Doherty
Founder and CEO
Doherty Associates

Unlock potential while remaining secure

To see how Doherty Associates can help you achieve your productivity goals while staying cyber secure in this new era of hybrid working, please call Alex Bransome, our Chief Information Security Officer, on 020 8987 1150 or email

enquiries@doherty.co.uk

'While many businesses appreciate that a 'castle and moat' perimeter defence approach is no longer fit for purpose, they are also struggling to keep up with the fast-moving challenges of hybrid working. We can help them understand those challenges and stay one step ahead.'

– Terry Doherty

It's not the tip of the iceberg you need to worry about It's the bit you can't see...

When the first lockdown was announced in March 2020, businesses were forced to move swiftly to adapt to home working. Many firms with robust cloud technology already in place found that it supported their need for flexibility and collaboration. They were quickly up and running and typically, they have remained strong and continued to grow their business during the pandemic.

By contrast, those who had remote working suddenly thrust upon them without the right technology in place may now have gaps in their security – and they might not know the true extent of the dangers they are facing.

While confidence levels and perceptions of risk vary, the truth remains that many firms are unaware of all the attacks and data breaches that are occurring remotely. For example:

> The data gathered highlights contradictions in the number of attacks that have been reported by the general workforce and those which are being detected. This suggests that many firms are still in need of a well-rounded cyber security programme that incorporates protective, detective and responsive solutions, if they are to keep their information, people and workforce safe.

This is especially true for law firms and companies in the financial sector, which are attractive targets for cyber criminals due to the high value of their transactions and the critical importance of client confidentiality. So, underestimating the risks and vulnerabilities that come with home and hybrid working could prove costly.

Anticipation beats mitigation

To see how Doherty Associates can help prevent cyber attacks or data breaches causing irreversible damage to your business and your professional reputation please call Alex Bransome, our Chief Information Security Officer, on 020 8987 1150 or email

enquiries@doherty.co.uk

Firms may be unaware of the sheer volume of attacks and data breaches that are happening remotely

Since the first UK-wide lockdown in March 2020:

42% of the general workforce say they have emailed confidential information

25% of the general workforce say they have experienced or caused a data breach

14% of the general workforce say they have experienced a phishing attack or similar

52% ...yet **of IT decision makers say they have not experienced a cyber attack or data breach**

These figures suggest that employees are not reporting all of the mistakes they make to IT decision makers, which means their firms may not be seeing the full picture with regard to the risks they are actually facing.

Finding the fault doesn't fix the problem
You also need to find a remedy...

One third of all IT decision makers surveyed report feeling inadequately protected by existing working from home protocols, despite many months passing since the start of the pandemic.

For example, when asked to report confidence in their firm's threat visibility and detection systems, 23% say they are 'not confident' of being alerted to a cyber attack as it occurred, and 19% are 'very unconfident'. At the same time, the number of firms providing cyber security training is worryingly low.

> Over a third (34%) of the general workforce say they have not received any cyber security training since the start of the pandemic, despite the fact that they are now using different software and platforms to collaborate as well as a mix of personal and work devices.

Empowering employees with the knowledge to identify threats in real-time can become a firm's greatest security asset, which means cyber security training is a 'must' and not just a nice-to-have in this new era of home and hybrid working.

Firms know the risks are 'out there', but taking action closer to home has not been prioritised

Since the first UK-wide lockdown in March 2020:

42% of IT decision makers say they feel inadequately protected against the threats of home working and that they lack confidence in their existing threat visibility and detection systems

33% of IT decision makers say they feel more vulnerable to a cyber attack or data breach with the workforce operating outside of the office

25% of IT decision makers say they can't guarantee security on every device used out of the office

51% ...yet only half of IT decision makers say their firm has conducted a cyber risk assessment

66% ...and *only two thirds* of the general workforce say they have had any cyber awareness training since shifting to remote working

This indicates a disparity between risks perceived and actions taken. And this is precisely the type of gap that cyber criminals will exploit.

Home working may boost productivity
But it also adds miles to the security perimeter...

As little as a year ago, flexible or remote working was considered unviable by many businesses. Today, that notion is long-gone – along with any sense of being safe behind an office firewall.

While office working is unlikely to disappear altogether, traditional 9-5 conventions have been upended, with many home workers enjoying greater flexibility and a better work/life balance, without the time-consuming daily commute.

In fact, over half (56%) of IT decision makers say they'd rather not go back to the way things were. And it seems that people are working just as efficiently, even if it is from their kitchen tables.

> Over one third (34%) of the general workforce say they have found it easier to win new business and close deals while working from home. However, a more flexible, hybrid scenario is creating increasingly complex cyber security challenges as employees move between different set-ups, in different places, using different devices.

This requires a robust, holistic approach; one that's capable of applying suitable protective layers of security along with appropriate monitoring to detect such threats before they become a problem. Otherwise, the business gains many firms have achieved through lockdown are at risk of being undermined.

The move to home working may have started as a necessity, but it's becoming a choice

Since the first UK-wide lockdown in March 2020:

56% of IT decision makers say they want to continue with a mix of home and office working

34% of the general workforce say that the process of winning new business is easier and closing deals is faster when working from home

21% of the general workforce say they have seen an increase in the number of deals closed and clients acquired

There are proven benefits to hybrid working. But many firms still need to take action to ensure those benefits aren't outweighed by cyber threats and to mitigate the risks.

Making one mistake might cause a problem Making a habit of it certainly will...

All employees need to be aware of or trained in the 'cyber security fundamentals', so that they can anticipate, identify, and mitigate threats, wherever they are working from. This is vital for home workers who are often using multiple devices, including personal ones.

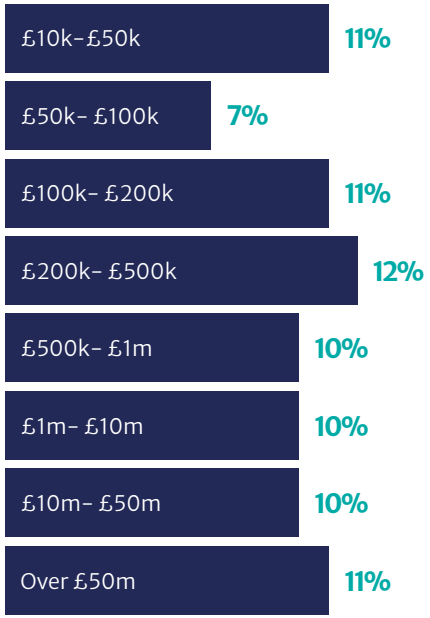
Instilling an ethos of meticulous cyber hygiene across the workforce is critical if teams are to continue to operate safely, securely and in full compliance with FCA regulations when working from home. This will also ensure that client contracts and other privacy obligations are better protected.

It's also worth stating that the cost of compromising a firm's critical data, including personal information that would lead to GDPR breaches and the risk of prosecution, is significant.

> Recovering lost or stolen data can be time consuming. Plus the data may be used by hackers to harass customers and threaten the firm, leading to a loss in client confidence.

The financial cost and reputational damage can be serious, and in the legal and financial sectors where trust is paramount, it may be difficult or even impossible to recover.

The financial impact of a successful cyber attack or data breach, estimated by survey respondents



The remaining 18% answered 'don't know'

Poor cyber hygiene is worryingly common among home workers

Since the first UK-wide lockdown in March 2020:

85% of the general workforce say they have worked on a blend of personal and work devices

67% of the general workforce say they ignore virus security scans for more than two days

57% of the general workforce say they save corporate data to personal devices or cloud-based servers

39% of the general workforce say they have made a note of work passwords on a computer, phone, spreadsheet or notebook

15% ...yet only **of IT decision makers put a block on personal devices**

Failing to follow due process for keeping data protected puts the whole firm at risk, even if only one person is doing it. Yet these statistics suggest it is becoming commonplace, meaning bad habits need to be broken if firms are to avoid costly breaches.

COVID-19 has turbo-charged digital transformation Firms won't catch up in pigeon steps...

While many firms in the legal and financial sectors are now moving in the right direction to improve their security, the survey suggests some worrying gaps in their defences.

Initially, firms may have been too stretched to address this, due to the sudden and dramatic changes thrust upon them by the COVID-19 pandemic. But now everyone is more accustomed to a new way of working, it's vital for firms to address any vulnerabilities and safeguard their 'borderless' network – and fast.

However, there is good news here too. As well as offering huge potential to enhance collaboration and productivity, cloud-based technologies can deliver reliable end-to-end security as long as firms take all the necessary steps to protect their workers, wherever in the world they may be.

Here to help

Doherty Associates has considerable experience and expertise in helping firms in the legal and financial sectors to mitigate risk, unlock potential and grow their business. If we can help in any way, please call 020 8987 1150 or email

enquiries@doherty.co.uk

Cyber security measures have been put in place by some firms since lockdown, but others may still be vulnerable

Since the first UK-wide lockdown in March 2020:

29% of IT decision makers say they have applied encryption to devices

25% of IT decision makers say they have implemented a Cloud Access Security Broker

18% of IT decision makers say they use data encryption

12% of IT decision makers say they have Advanced Endpoint Detection software

These statistics show that while some firms have taken steps to improve their security, others have not. This could be because their cyber hygiene and protection protocols were already first rate. However, some may still be unaware of the risks and the steps they need to take to keep their networks, users, and data safe.

Findings summary: a cause for concern

The most significant survey findings include:

- The fact that IT decision makers may not be fully in the picture with regard to risk, given over half of them report no cyber attack since March 2020, while a significant proportion of the general workforce say they have personally caused or experienced such a breach
- A lack of awareness of the threats posed by cyber attacks and the lack of protection against them when working remotely
- The abundance of bad habits and poor cyber hygiene among home workers with little knowledge of the risks
- The lack of employee cyber security awareness training
- The significant financial and reputation repercussions of a cyber attack or data breach
- The critical need for change and improvement given hybrid working is here to stay

Recommendations

Firms with any doubts or concerns about their cyber security should consider:

- Carrying out a cyber risk assessment at least every six months to identify and address any critical vulnerabilities, gaps or compliance issues
- Adopting cyber security practices and procedures that give greater visibility and detection of attacks, and that are capable of responding quickly and effectively to mitigate threats
- Ensuring all identities are secured with multi-factor authentication, to protect employees against lost or stolen credentials
- Building in regular comprehensive cyber security awareness training for every employee
- Using software that ringfences and encrypts all the corporate data on mobile or 'bring your own' devices. This means the corporate data can be wiped if the device is lost or stolen without this affecting any personal data – such as family photos – if the device is then found or recovered
- Using disk encryption to protect all data on company devices such as laptops, to mitigate the risk of it being lost or compromised if the device is stolen

About Doherty Associates

At Doherty Associates, we draw on deep industry knowledge and business insight to deliver intelligent IT solutions and services that help people work more securely, more productively and more creatively.

Over the past decade, we have successfully migrated over 50,000 people to Office 365 and the Microsoft Cloud.

The company was established in 1991 by Founder and Chief Executive, Terry Doherty, whose vision was to leverage the power of technology to help companies grow. Each year since, IT has become more important to the running of a business and it is now the focal point of a majority of successful organisations – and ever-present in all our lives.

Today, Doherty Associates is a Tier 1 Microsoft Gold Partner employing over 100 people, with offices in London and Kuala Lumpur. Having an extended team in a different time zone means we can provide genuinely 24/7 support to our clients. For example, we are able to take a proactive approach to security, by constantly monitoring their systems for any signs of attack as well as making updates 'out of hours' so there's no disruption to their business.

We may have changed in scale and scope over the past 30 years, but our focus remains on helping businesses to grow by unlocking the potential of technology.

London office

3 Water Lane
Richmond
London
TW9 1TJ

Kuala Lumpur office

D2-3A-5 Solaris Dutamas
No. 1. Jalan Dutamas 1
50480 Kuala Lumpur
Malaysia

Microsoft Partner

Microsoft

Gold Data Analytics
Gold Collaboration and Content
Gold Cloud Platform
Gold Datacenter
Gold Cloud Productivity

ISO 27001 CERTIFIED
British Assessment Bureau

ISO 9001 CERTIFIED
British Assessment Bureau

dohertyassociates