MARSH COMMERCIAL

The evolving risk landscape for tech businesses

What are the risks and how can you manage them?

MARSH

Contents

Balancing risk and reward in technology	3
Challenges facing tech	6
Building resilience in tech	13
Managing risk with Marsh Commercial	21

Balancing risk and reward in technology

‘Every company is a technology company’. This may be a much-used phrase in the tech press and blogosphere, it also happens to be true.

Technology is now a dominant force across the sector spectrum. Exciting developments in automation, analytics, artificial intelligence (AI), the internet of things (IoT), blockchain, cyber security, robotics and more are transforming established markets and driving the fast-emerging fin-tech, med-tech, clean-tech and agri-tech sectors.

The recent coronavirus pandemic illustrated the crucial 'enabling' role of the tech industry: delivering the connectivity and applications to remote working staff; the content and media platforms to offer lock-down entertainment; and the sophisticated ecommerce, retail and distribution systems to keep the flow of goods moving.

Looking beyond the crisis, technology will play an even greater role in today's more virtual world – whether that be the wider delivery of telehealth services, the provision of digital identities to boost remote authentication, or the accelerated adoption of cloud.

As the tech sector rapidly evolves, the already well-established tech skills shortage, cyber threats, changing working models and extended supply chains all continue to create a raft of issues. Those moving into new and highly regulated sectors – such as healthcare and finance, will be subject to new and unfamiliar regulatory environments. So too, as both traditional enterprises and big brand tech companies increasingly employ the skills of smaller specialists and freelancers, the contractual risks to both parties grow. Ultimately, in today's increasingly interconnected high tech world, while the development work or IT support may be outsourced, the liabilities are not.

Balancing risk with innovation and growth may be second nature to the fleet-of-foot tech industry. But faced with growing regulatory scrutiny, evolving employment legislation, growing cyber threats and wider shifts on issues such as data exchange and privacy, it's more important than ever that firms are prepared and protected.

In today's increasingly interconnected high tech world, while the development work or IT support may be outsourced, the liabilities are not.

Challenges facing tech

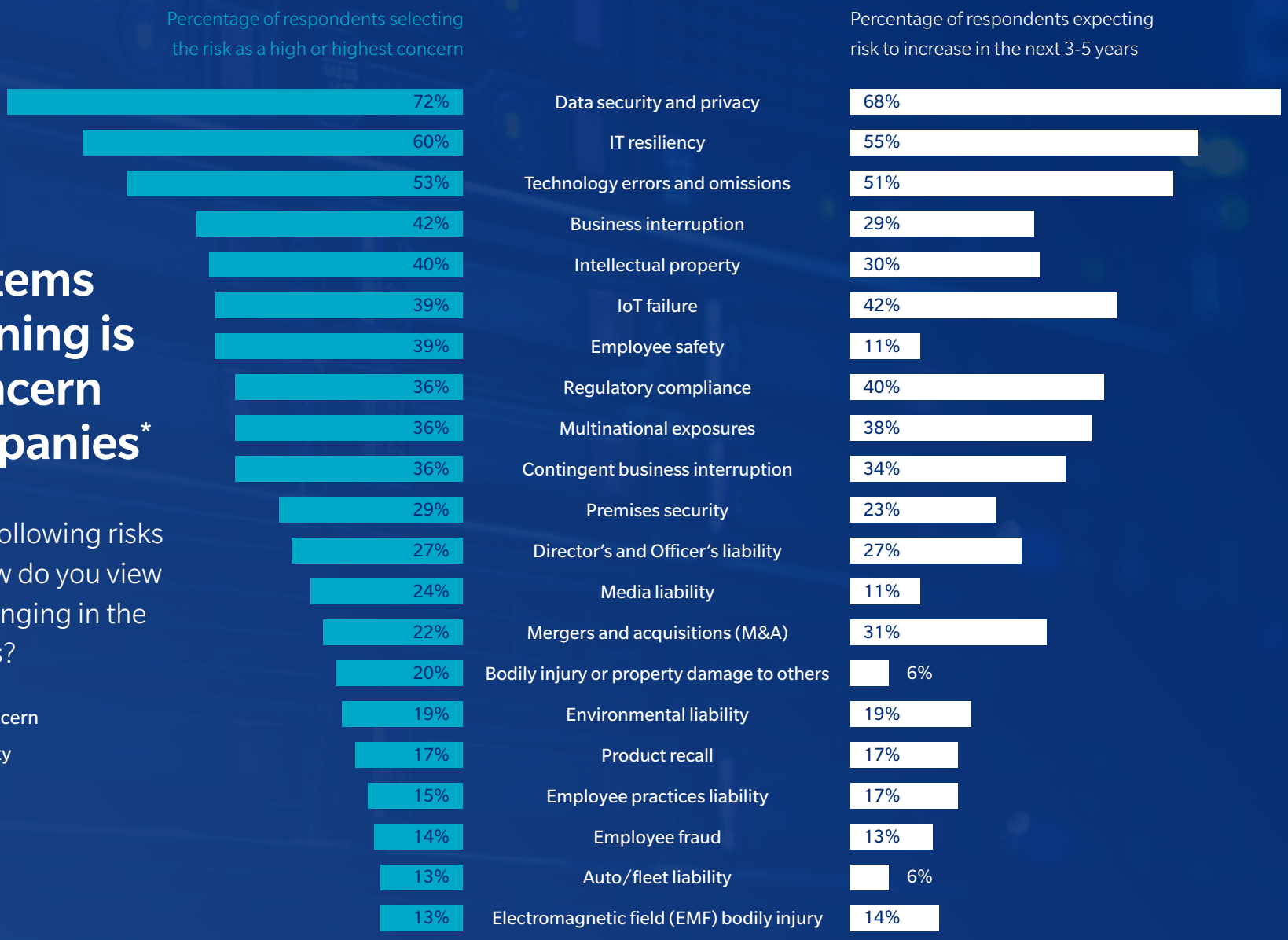
Despite the sector's robustness in the face of a challenging environment, issues remain. Here we take a closer look at the operational risks and liabilities upper most in the thoughts of tech entrepreneurs and leaders.

Research conducted by Marsh for its annual Technology Industry Risk Study 2020 explored the concerns of senior leaders across the global communications media and technology sector.

Keeping systems safe and running is the main concern for tech companies*

How do you view the following risks to your company? How do you view the following risks changing in the next three to five years?

- Risks of high or highest concern
- Risks will grow in complexity



* Source: 2020 Marsh Technology Risk Study

Cyber risk

For the fifth straight year, data security and privacy tops the list of concerns – which is unsurprising given the number of reported cyber-attacks, losses, and related new regulations. In the UK, for example, the number of businesses reporting cyber incidents rose from 45% in 2018 to 61% in 2019[1].

Cyber risk cannot be eliminated – only mitigated and managed. It is now an unavoidable cost to a business; and those costs can be high – from business interruption and loss of income, through the restoration costs of replacing damaged digital assets, to reputational damage and regulatory action.

The number of businesses reporting cyber incidents rose from 45% in 2018 to 61% in 2019[1].

[1] Hiscox Cyber Readiness Report 2019

Managing IP and data

For upscaling, unicorns and established brands, this latter point is perhaps the most concerning. Falling foul of the Information Commissioners Office (UK's GDPR) can be an expensive business – British Airway's £20 million fine is a perfect illustration[2]. While data breaches and privacy remain real concerns for some, today's phishing, social engineering and ransomware attacks also threaten to disrupt businesses, supply chains and industries for many.

Aside from the very real operational and reputational risks of attack, the threat to intellectual property is considerable. Certainly, for businesses across the tech spectrum – with fin/health/clean-tech businesses, games designers and more at the forefront of disruptive technologies – ensuring the integrity of, and managing the liabilities around, IP is critical.

[2] https://www.csoonline.com/article/3518370/the-biggest-ico-fines-for-data-protection-and-gdpr-breaches.html

Regulatory issues

As tech companies continue to innovate, they find themselves operating in multiple sectors – with unfamiliar and robust regulatory environments. For firms operating in the life sciences, health, legal, telecommunications, advertising and financial sectors this goes well beyond GDPR compliance. Adherence is business critical but not always simple. Certainly, the increasing complexity of overlap among tech sectors further demonstrates the need to understand new liabilities and interconnected risks.

Regulatory risk

The interconnected nature of technology, its extended supply chains and the growing trend of larger brands contracting out work to smaller firms and specialist freelancers all makes for a complex partnership ecosystem. So much so, Hiscox data suggests 65% of claims they handle for tech companies are a result of breach of contract.[3]

In the IT space, for example, system integrators placing client systems in a third party data centre may be offered service levels, but may not always be aware of exactly where liabilities lie. In such a case, data breaches or systems failures in one area can have significant consequences for partners and clients up the chain, with acute regulatory, legal or financial consequences for many. Clarity here is essential when contracting out services. This is as critical for end-user businesses utilising the services of an IT provider, as it is for tech ecosystem partners.

Things can be more complex still, certainly for smaller firms and individuals, when accepting contract development work from larger tech brands. This is particularly prevalent in the software (and gaming) space as major publishers draw on outside resources to support their own development activities. This 'David and Goliath' relationship often involves complex contractual conditions and transfer of liabilities to the smaller partner – requiring considerable due diligence (or transfer of liabilities through insurance) at the outset.

There is another dimension here in the UK with the advent of IR35 anti-avoidance tax legislation for off-payroll working. Here, new rules will apply to those who provide services through their own limited company or another type of intermediary to the client. Across the tech spectrum, designers, developers, engineers and so on will be affected and will have to ensure they become IR35 compliant. Failure to do so will result in considerable fines and regulatory action. Again, understanding the risk will ensure contractors can mitigate and manage it.

65% of claims in the tech sector are a result of breach of contract

[3] https://www.hiscox.co.uk/sites/uk/files/documents/2020-01/Technology_PI_client_brochure_20388.pdf

Workforce risks

In a connected point, the ongoing skills gap will continue to challenge businesses. This is certainly true as organisations accelerate down their digital paths. According to global consulting firm Protivity[4], the growing adoption of advanced technologies such as artificial intelligence, robotics and more will require new tech skills sets.

These are likely to be in short supply and will require considerable upskilling. While this poses a significant risk for affected organisations, it does offer opportunities for specialist tech firms and contractors to plug the breaches. But only, of course, if they are able to effectively mitigate the contractual and regulatory risks noted above.

Growth in IT sophistication and the increasing demand for skills also pose retention and succession risks for both tech consultancies and client organisations. No firm wants to invest in its people only to see these newly upskilled experts eagerly sought (and bought) by competitors. So too, more established organisations will also face pressure from 'born digital' businesses – both in terms of growing competition in their markets, and in the demand for top talent. Getting competitive positioning, workforce and recruitment strategies right will be crucial.

[4] https://blog.protiviti.com/2020/02/25/economic-conditions-digital-adoption-and-talent-shortage-headline-the-top-risks-list-for-tech-companies-in-2020/

Building resilience in tech

Whatever the risks, you can sandbag against their impact by focussing on some core business practices. Next we explore three key areas that, if strengthened, could significantly improve your resilience against the risks facing technology companies in the future.

Cyber security

It is estimated that 46% of companies experience a cyber breach of some sort in a 12-month period. The severity of the issue is understood, with eight out of ten UK companies saying that cyber security is a high priority for senior management, according to the latest UK government figures.[5] However, globally nearly four out of five small companies (those with one to nine employees) are "cyber novices", according to Hiscox,[6] with nearly half having no defined cyber security role.

While cyber security is an essential investment, it needs to be supported by cyber-resilient processes and practices. Two areas in particular will require additional attention due to the current climate: a resilience culture, and insurance provision.

Educate the workforce

Even though many of your employees may be tech-savvy due to the nature of your sector, make cyber resilience education part of your core training process. All members of staff, from the digital natives to back office, should be educated, engaged, and involved in incident planning and response.

Train staff to spot and avoid phishing emails by implementing the following into their practices:

- Log in using a trusted network, and where possible multi-factor authentication (MFA)
- Validate any information before acting on it
- Never click on links in unsolicited emails or hand over passwords on sites that are not 100% trusted
- Follow up requests for money or information with phone calls using a number from a separate and trusted source
- Check email sources; look for misspellings, suspicious URLs, and public email addresses, such as Gmail
- Be wary of any communication stressing urgency and asking for immediate action.

Your cyber resilience strategy should ensure you fully involve your workforce in the following ways:

- Make security training a basic requirement for all new employees
- Engage with staff to gain insight into their operations, processes, and security concerns
- Make security awareness and resilience training available to all employees throughout the year.

[5] gov.uk/cyber-security-breaches-survey-2020

[6] Hiscox 'Hiscox Cyber Readiness Report', 2020

Understand your insurance needs

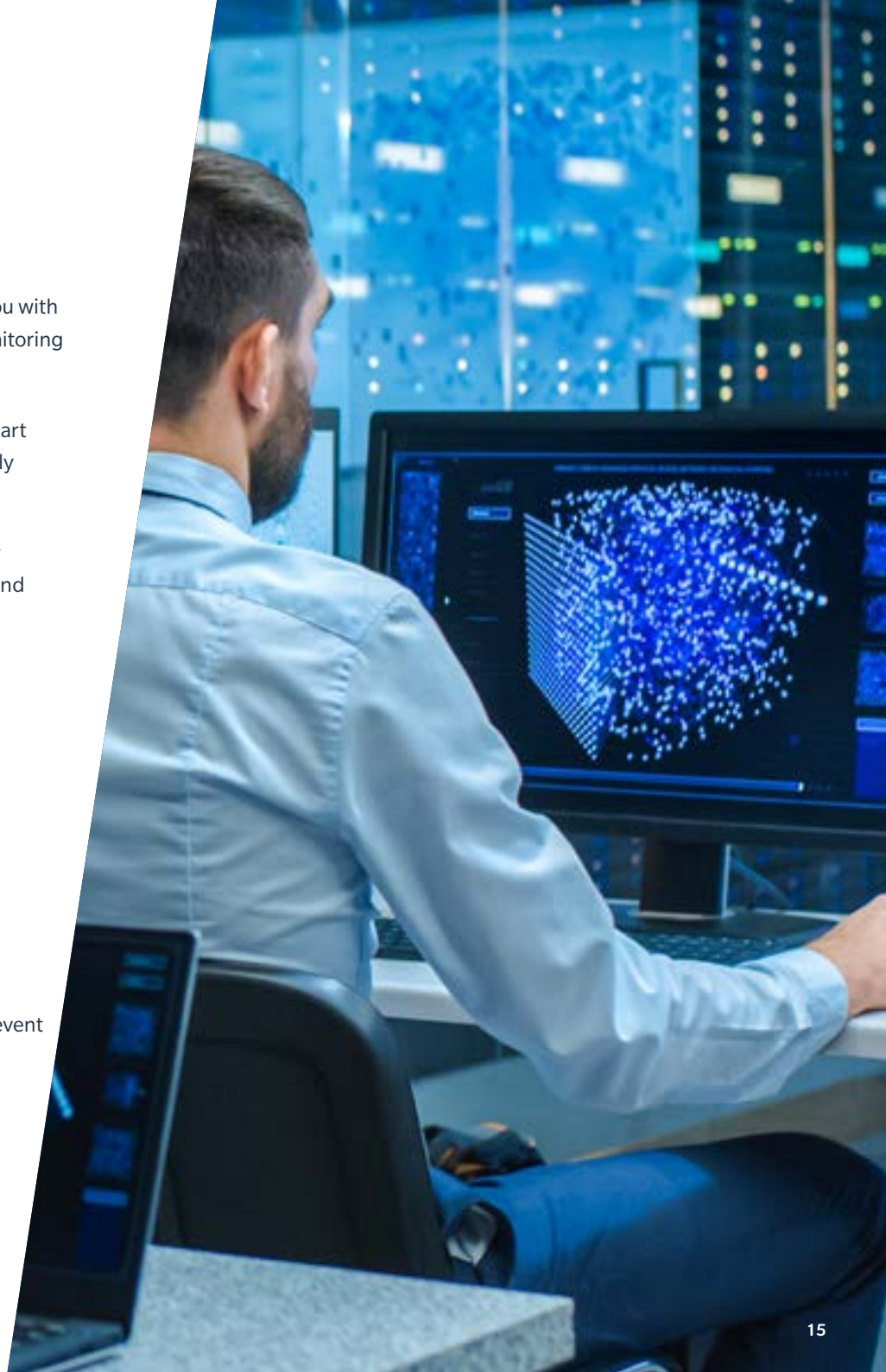
Should you suspect a cyber-attack is taking place, you will need the support of a readily available network of breach response experts. Robust insurance policies will provide you with access to a suite of third-party vendors, including IT forensics, legal, PR, and credit monitoring agencies, in order to project manage any response.

Assess how any cyber coverage you have would operate in practice, particularly if it is part of another policy. Invest in cover that caters to your specific business needs, and will fully support your recovery.

A complete cyber insurance package should arm your company against potential cyber threats, from loss of network, data breach or corruption, business interruption losses, and reputational damage, to online media and cybercrime.

Key areas of cover to look for in a good cyber and data liability policy include:

- Access to the provision of immediate breach response services, including forensic investigation and recompilation of data
- Cyber extortion
- Cyber business interruption including reputational damage
- Costs associated with any breach notification and management
- Protection from GDPR non-compliance claims
- Public relations and crisis management costs
- Cybercrime
- Defence costs and awards in respect of any third-party liability arising from a cyber event
- Payment of civil fines and penalties as a result of a cyber event, where insurable.



D&O

Directors and officers liability (D&O) insurance provides protection for directors and officers against investigations and claims arising from their decisions. The policy is triggered by allegations that a director or officer has committed a failing or "wrongful act".

The cost of D&O insurance has been rising for a number of years. Average pricing in the UK increased 46% in 2019, according to analysis by Marsh Specialty. This followed a 35% pricing increase in 2018. These increases accelerated in the second half of 2019 and this continued to be the case throughout 2020.

Despite premium levels trending up, D&O insurance could very well be the most important cover for companies today. This is due to the growing potential of action against directors and officers.

Allianz highlighted in its 2020 D&O market report[7] a number of megatrends to look out for in 2021. The insurer predicted D&O claims coming from a range of new areas driven by rising insolvency exposures, cyber threats and environmental, social and governance scrutiny.

The pandemic and its economic fallout has also increased exposure for directors and officers to be held accountable for poor performance or management decisions.

[7] Allianz 'DIRECTORS AND OFFICERS INSURANCE INSIGHTS', 2021 https://www.agcs.allianz.com/news-and-insights/news/directors-and-officers-insurance-insights-2021-press.html

During times of crisis, directors and officers are expected to react quickly and with agility to mitigate the effects of supply-chain disruption, drops in consumer demand, and office closures on balance sheets.

Gaps or failings in contingency plans or communications from management could result in employees, clients, or stakeholders questioning whether the fault lies with the senior executives. If directors and officers are deemed to have made mistakes in the development of appropriate risk management and preparedness strategies prior to the pandemic, they could face actions from a broad range of stakeholders including employees, customers, creditors, and regulators.

The following failings are examples of contingency planning and decision-making issues that could lead to directors and officers facing investigations and claims:

- Poor communication to staff, with inconsistent messaging.
- Failure to have adequate systems in place allowing access to company servers, ensuring business as usual is maintained while staff are off-site.
- Lack of alternative technology to maintain engagement with clients.
- Mismanagement of the supply chain, which could slow or halt service or production.
- Lack of planning on how to monitor systems and controls at the required level with increased remote working.
- Lack of cyber resilience capabilities to ensure data security when there is a very high level of remote access.

Directors and officers are also potentially at risk under the General Data Protection Regulation (GDPR), should inadequate security controls result in a data breach. In the same way, they are exposed if a cyber-attack causes business interruption. This threat is growing as remote working has become more widespread.

D&O has commonly been provided under the umbrella of management liability insurance, and has previously been perceived as a “nice to have”, as it is not legally mandated. It is increasingly recognised as a business cost – and an expensive one.

Many directors and officers face choosing between protecting themselves against uncertainties surrounding the wider economic outlook, litigious environment, and even employee actions, and the need to reduce costs and avoid further financial outlay in the short term.

Ensuring you’re appropriately covered with D&O insurance is one of the best ways to insulate yourself and your company from the financial implications of actions brought against you personally, or from any investigations by regulators into your actions.

Directors and officers looking for new policies, or renewing existing ones, may face considerable increases in premium however. During renewal, be prepared for reduced limits and restrictions due to the market’s fluidity and volatility. Very short notice may be given for these changes. Keeping in close contact with your adviser to understand and navigate the evolving market is essential.

Accordingly, companies should work with their brokers to prepare for their D&O renewal early to achieve the best protection possible in this dynamic market.

Futureproofing your workforce

Working patterns have been heavily disrupted over the past several months, with workforces learning new processes due to pivoting business models or being shifted into home working, and many sectors having to furlough staff. These are likely to be long-term changes, or at the very least changes that will have long-term effects.

The Health and Safety Executive (HSE) outlines that work-related stress, depression, or anxiety accounts for 51% of work-related illness and 55% of lost working days.[8] Supporting the workforce through tough periods during times of crisis is essential to a company's success, as their productivity is the engine for a firm's bottom line.

The pandemic has brought workforces, mental health and wellbeing into sharp focus. There has been an increase in anxiety, relating to the pandemic,[9] and also among those worried about job security.

A proactive approach to mental health and wellbeing could lead to fewer sick days and greater productivity. This could include additional resources for those needing support, such as helplines; greater monitoring from managers for signs of mental health issues; and safe spaces for employees to voice concerns. Good company communication will also provide transparency and clarity.

Another growing concern is some peoples' reluctance to seek medical help during the pandemic.[10] For example, some people are not seeing a GP when they need to, for fear of catching COVID-19; others are also not visiting hospital when necessary for fear of overburdening the already stretched health services. Providing access to virtual GP services may help to manage this problem.

[8] Health & Safety Executive (HSE) 'Work-related stress, anxiety or depression statistics in Great Britain', 2020
[9] King's College London 'COVID-19 pandemic significantly increased anxiety and depression in the UK', 2020 https://www.kcl.ac.uk/news/covid-19-pandemic-significantly-increased-anxiety-and-depression-in-the-uk#:~:text=16%20September%202020-,COVID%2D19%20pandemic%20significantly%20increased%20anxiety%20and%20depression%20in%20the,Nottingham%20and%20King's%20College%20London.
[10] GPOnline 'Millions of patients 'avoiding calls to GP' during COVID-19 pandemic', 2020 https://www.gponline.com/millions-patients-avoiding-calls-gp-during-covid-19-pandemic/article/1681384

Special attention and care needs to be given to remote working arrangements, as there may be increased liability for companies.

There is a definite increased potential for carpal tunnel and lower back claims as employees may work on laptops for longer periods of time with fewer breaks; or have laptops on their laps while sitting on beds or sofas – inducing poor posture. If the employer has not taken action to ensure correct setup, then they could be held negligent.

Injuries sustained while working at home, as a direct result of undertaking work required as part of their role, would be covered by the normal employer's liability insurance. The claimant would need to show that the company had been negligent in some way. If an employee has been instructed to work at home it is still the employer's responsibility to ensure that they do so in a safe manner by undertaking the following:

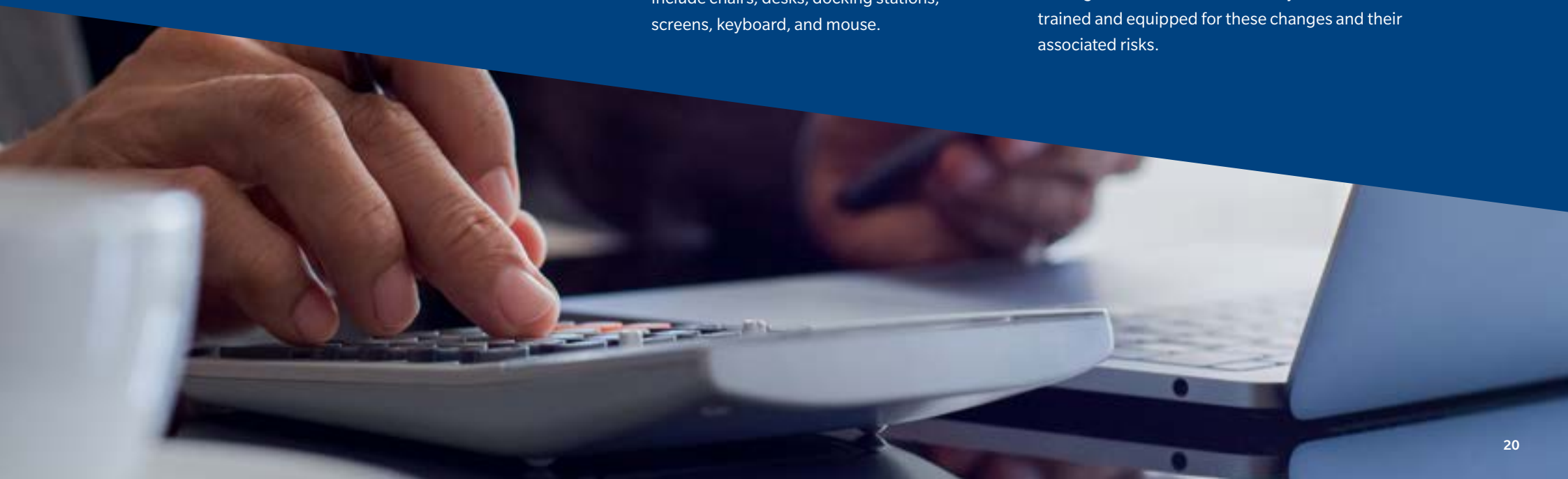
Assessment – undertake a display screen equipment (DSE) assessment to ensure the correct measures are in place to reduce the potential for injuries.

Provision – the DSE assessment may highlight specific needs, which may mean that the company has to provide adequate equipment to ensure a correct setup. These will generally include chairs, desks, docking stations, screens, keyboard, and mouse.

Any injury sustained during work hours at home, such as tripping on a toy or falling down stairs, which does not directly relate to the work being undertaken, would not be covered.

As well as monitoring health and wellbeing, it is important to remember your employees' goals and aspirations. Ensure you are still providing adequate training and development to employees working from home. This will not only help with motivation, but will also support succession. When longstanding members of staff leave, so does their corporate memory. During a time of incredible upheaval, ensuring valuable information is shared across a workforce – particularly to newer employees – is sensible.

As well as training for succession and trying to maintain corporate memory, companies should prepare their workforces for the future. Keep an eye on future trends – such as consumer changes, the growth of e-commerce, and digitisation – and ensure that your workforce is trained and equipped for these changes and their associated risks.



Managing risk with Marsh Commercial

With technology industry companies at the forefront of disruptive technologies and business models, the stakes couldn't be higher.

Well established and significant intangible risk exposures abound, and sustainable growth relies on the ability to understand, identify, qualify and address conventional business, and disruptive technology-related, risks.

Working across the spectrum, and with more than 2,300 clients, our technology experts are dedicated to helping tech firms identify, quantify, manage, and mitigate risks – with tailored advice and customised, industry-specific solutions that match client risk and insurance needs.

But while reducing liabilities is our core business, we don't just focus our time on insurance placement. This is just a small component of the client's overall strategy. Here at Marsh Commercial, our approach is first to gain a deep understanding of each clients' organisation, risk landscape, and see how this fits with their strategic approach to risk. Only then do we define, agree and deliver the most appropriate set of services.

We support clients in the following areas:

Risk transfer of physical and non-physical assets, liability and revenue related risks. This includes technology-specific insurances such as cyber, technology errors and omissions/professional indemnity, credit, intellectual property as well as property damage, business interruption and general liability.

Risk management support and consulting ranging from exposure modelling, risk management consulting and business resilience through to health and safety/ workforce strategies and business interruption reviews.

People risks, including employee health and benefits, insurance and related consulting.

Global service and delivery of insurance programmes.

Email, social media, face to face, or zoom;

when you reach out, we'll be there to connect.

For more information visit:

marshcommercial.co.uk/for-business/technology

Insurance Brokers

Chartered

MARSH