

CHALLENGES FOR THE TECHNOLOGY SECTOR IN 2021

The tech sector is constantly evolving in a chain reaction of rapid technological developments. No matter where you are based in the world, it is virtually impossible to escape the way new technologies are reshaping everyday life, as exciting as this is, the tech sector faces new challenges for 2021?



Topics covered

#1 Sourcing and retaining talent

#2 Impact on customer budgets

#3 Regulation and implementation

#4 Cyber security concerns

#5 Emerging insurance trends for
tech sector businesses

The background of the entire page is a dark blue field filled with abstract digital elements. There are numerous vertical and diagonal lines of varying lengths and thicknesses, some solid and some dotted. Scattered throughout are small, glowing blue dots and larger, fainter ones. Some of these elements resemble data points or nodes in a network. The overall effect is a sense of digital connectivity and data flow.

Time for a new approach

No-one foresaw the world-changing events of this year, but one thing is clear: the tech sector has been affected just as much as every other part of our lives.

Driven by innovation and technology, the sector has become increasingly purpose-led and a force for good, playing an important role in reducing inequality and boosting economic growth across the world.

The last 9 months alone have produced more digital transformation than the last decade, with every transformation effort already underway finding itself accelerated at huge scale. While many of the 2019 digital transformation predictions from a year ago benefited from this shift, others were displaced by more urgent needs, like 24/7 secure and reliable connectivity.

Will core technologies like AI and data analytics still dominate headlines, or will we see newer, previously emerging technologies take the lead? What does this mean for sourcing and retaining talent in 2021?

With shifting consumer and business behaviours likely to stick even post Covid-19, it's clear that most old-style tech strategies have become outdated, which is why it's time for a new approach.

#1 Sourcing & retaining talent



Recruitment is a key challenge across many industries but we know there is a global reach when it comes to the tech sector in UK.

It is always a challenge attracting the top talent; as with attracting new clients, “what makes you different and why should I work for you?” There are certainly particular roles within tech businesses where it is very much a ‘candidate buyers’ market and this is likely to heighten in 2021.

Deal or no deal, the UK’s departure from the European Union brings with it many challenges for the tech sector to attract and retain talent.

When industry leaders talk about “skill gaps” in the technology workforce, they are referring to literal tech-focused inadequacies i.e. employees not being up to speed on emerging technologies, advanced security or various types of software development. These are valid, core needs for tech companies and critical for the people they employ in these roles. In today’s environment, though, other skills are becoming as much, if not more essential to tech businesses. Some use the term “soft skills” to refer to these characteristics, but increasingly they are also referred to as “professional skills”.

Basically, it’s about the ability to communicate, lead, make a case, write well and organise a team.

In 2021, we expect to see neurodiversity become a trend as employers look to diversify in terms of thought process. Tech companies will start to look for more ‘outside the box’ thinkers or ‘disruptors’ who will be the new innovators in the company.

Prior to Covid-19, skills shortages remained close to an all-time high. Subsequently, shortages in tech talent have remained high, only marginally dropping compared to the 2008 Global Financial Crisis. In addition to cyber security skills (35%), the next three most scarce technology skills are organisational change management (27%), enterprise architecture (23%) and technical architecture and advanced analytics both at 22%

19 university academic centres of excellence and over 30 MSc courses in cybersecurity promote cyber skills in the UK and guarantee the supply of the future labour force



Take a Different Approach to Attracting EU Workers

Although 25% of UK companies currently employ staff from the EU, net migration from the EU to the UK fell by 95% in 2019. Coupled with the skills shortages increasingly plaguing the tech sector, employers are continually struggling to find top talent.

Whilst EU workers currently make up 7% of the UK workforce, research from the Recruitment and Employment Confederation (REC) suggests that following Brexit, fewer EU workers will choose to fill these roles in the future (Tech City UK).

If you are planning to recruit from overseas from 1 January 2021, you will need to register as a licensed visa sponsor. You may not be able to legally hire people from outside the UK if you do not have a license. New employees from outside the UK will also need to meet new job, salary and language requirements.

There still seems to be a certain level of uncertainty of how hard or easy this will be for companies to negotiate. Will it simply mean that UK based tech businesses recruit and hire remotely and those subsequently hired staff stay where they are?

We still don't know what kind of mindset shift will be needed when it comes to recruitment post-Brexit transition period. Hiring people from Europe will not be as easy as it once was, incurring addition to the financial and administrative costs.

"There will be additional cost implications and an impact on budgets, as employers wishing to employ EU nationals will need to apply for a Sponsor Licence (for which there is an application fee payable), pay visa application fees, skills charges and IHS charges (a contribution to the NHS)." Said Dhruti Thakrar, head of immigration at law firm Edwin Coe LLP, 2nd November 2020



Expansion of Remote Friendly Jobs

The fact that more and more companies are adopting broader work-from-home policies is no longer breaking news. When asked about their approach to remote work for the near future, according to Forrester, 80% of tech leaders said they will conduct more job interviews remotely while 65% said they will hire more employees to work offsite.

Aside from just giving candidates greater flexibility and promoting a COVID-friendly workplace, though, expanding your remote job offerings can also help you reach a wider, more skilled talent pool. Including the option to work from anywhere some or all of the time as part of your job listings helps you reach candidates who may not have considered a position in the past because of the constraints of working onsite.

Work location & remote working has risen to become one of the five most important factors for engaging and retaining key technology talent during, and after, Covid-19. Tech leaders will need to rethink how they attract and engage their employees in a world where physical location is no longer a prime asset.

#2 Impact on customer budgets



The Coronavirus epidemic has changed both the trajectory and the velocity of digital transformation, and will likely continue to do so into 2021. The trend lines and new priorities facing businesses of all sizes that we observed in 2020 will inform the focus, decisions, and technology investments that drive the list of digital transformation strategies that will define 2021.

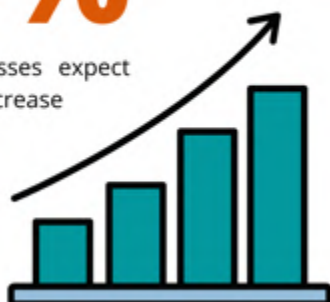
Source: KPMG's Survey of over 4,200 CIOs and technology leaders August 2020 across 83 countries.

As businesses across the economy need to support a new army of workers from a home environment, demand has grown for device sales such as laptops and other networking infrastructure, as well as all-important security services. Channel firms in the coming year will need to assess their own offerings and capabilities in direct relation to customer needs in this new, uncertain environment.

Going into 2020, the majority of UK business owners were optimistic about future business prospects but predictions for 2021 are not quite as bullish.

33%

of UK businesses expect revenues to increase



Despite Uncertainty, tech Budget Growth Continues

As revenues stagnate, one might expect tech spending to get watered down. While year-over-year growth has slowed a little, more tech budgets are expected to grow than contract in 2021. In fact, 80% of businesses anticipate year-over-year tech spending to stay the same or increase (33.3% increase vs. 46.3% stay the same).

Even amid uncertainty, many businesses will focus on tech spending. Just as in previous years, updating outdated IT infrastructure will continue to be the top factor driving tech budget increases, cited by 56% of businesses planning on growing tech spend, followed by an increased priority on tech projects (45%) and escalating security concerns (39%).

Unsurprisingly, the coronavirus pandemic will also influence tech spending in a major way in 2021. Among business's increasing budgets in 2021, 38% cite changes to business operations due to Covid-19 as a reason to increase spend, with 36% citing the need to support a remote workforce during the ongoing crisis.

Employee growth, which was anticipated to be one of the top drivers of budget increases in 2020, is expected to have significantly less influence on spending increases in 2021, as the pandemic puts a lid on hiring.

In 2021, budget drivers will vary by company size. For example, the need to upgrade outdated infrastructure will be the top factor contributing to increases in

IT spending among SMEs (1-999 employees). An increased priority on IT projects is the top factor influencing IT budget growth in larger enterprises (1000+ employees), at a rate significantly higher than in SMEs, likely because larger enterprises are more likely to have experienced changes to their business operations causing them to re-prioritise tech investments to support their needs.

Additionally, mid-size businesses (100-999 employees) and larger enterprises are significantly more likely than small businesses to increase budgets in 2021 due to supporting a remote workforce during Covid-19, and enterprises are significantly more likely than SMEs (1-99 employees) to increase budgets due to changes in business operations during Covid-19, changes in regulations, and/or a recent security breach.

Over the last two years, money allocated to hardware budgets has slowly flowed into other areas. Hosted/cloud services will account for 24% of IT spending in 2021 (up significantly from 21% in 2019) and managed services spend will account for 16% of spend (up significantly from 14% in 2019). Of note, the recent push to remote work has energised cloud spending with 35% of businesses have either already migrated or plan to accelerate migration of workloads to the cloud due to Covid-19.

Directionally, the data indicates that in 2021, SMBs (1-999 employees) anticipate spending a greater percentage of their IT budgets on hardware and software than larger enterprises. Conversely, larger enterprises (1000+ employees) will allocate a greater portion of IT budgets than SMBs to hosted/cloud and managed services.

Source: KPMG's Survey of over 4,200 CIOs and technology leaders August 2020 across 83 countries & Source: Gartner Top Strategic Technology Trends for 2021 October 2020

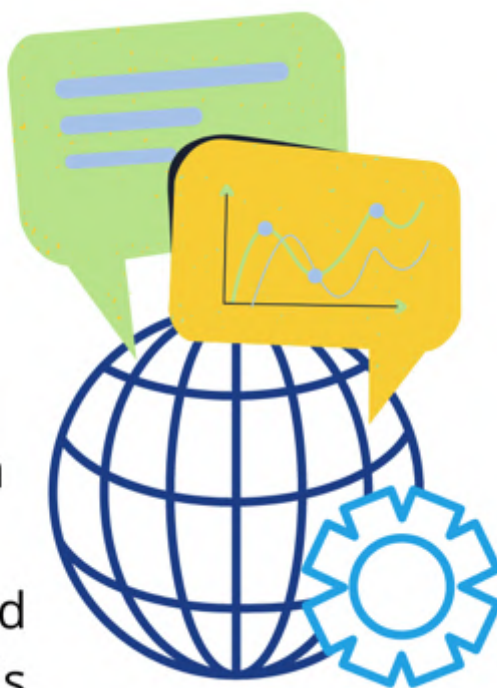
#3 Regulation & Implementation



A common challenge the tech sector faces in 2021 is around the uncertainty with the relationship with EU and data exchange. Many tech companies work with EU customers and the Brexit deal uncertainty will be a challenge.

We are confident there will be an agreement about data exchange. The problem is the lack of clarity around timing and there could be a period where companies remain confused. The issue with data exchange is also complex because it involves the US. With the recent Privacy Shield scrapped, it's a question about what agreements will happen for EU/US data exchange and UK/EU similarly. Both need to be aligned. This impacts UK tech companies, many of which also have US customers and suppliers.

11.5% of global cross-border data flows pass through the UK and **75%** of this traffic is with the EU.



How will the exchange of personal data be affected by the UK/EU future relationship?

Conversations around the UK/EU trade deal has mostly focused on how goods will be exported and imported in the future. However, UK trade with the EU is also conducted away from customs locations at sea, rail and airports, particularly when it comes to the trade in services which make up the majority of the UK's trade with the EU.

The UK is a major data hub. While the UK represents around 3% of global GDP, 11.5% of global cross-border data flows pass through the UK and 75% of this traffic is with the EU. Data will therefore be a major component in the future relationship with the EU, with both the trade in goods and services underpinned by exchanges of data.

When the U.K. was a member of the EU it was bound by common rules on data protection with the UK's data protection authority, the ICO, sitting on the pan European data protection forum, the European Data Protection Board (EDPB). As part of this the flow of data between the UK and the EU was relatively free, meaning individuals, companies and public authorities could transfer data across the EEA as if it were a single state, as long as data protection rules (the GDPR) were followed.

During the transition period there will be no change to UK data protection rules; it will be business as usual. Policy and regulation can have a significant impact on tech sector businesses, especially where innovation is a constant.

Innovative businesses are at risk of falling foul of outdated laws or hastily introduced new ones that could harm their operations and growth. However, changes to policy and regulation can also open up new commercial opportunities for existing companies and start-ups, especially those addressing public sector markets.





Taking a proactive approach

Since policy and regulation can have such a big impact on a business' operations and growth prospects, it is in the best interest of organisations to stay ahead of the curve, so they can spot potential threats or opportunities early on.

Many of the most successful organisations have developed strategic engagements with policy makers and regulators in order to create relationships where government, regulators and industry can work together to achieve better outcomes. This does not mean you need to spend the amount of time and money that Google, Amazon and Apple spend lobbying governments around the world. However, by approaching engagement with policy makers as a dialogue, you can build trust, which will help influence emerging policy and regulatory changes. This practice will become even more prevalent throughout 2021.

Keeping abreast of the opportunities is just as important as tracking the threats. A new development may mean you are able to move into a previously untapped market or move to a more profitable business model. If you do not take advantage of these opportunities, you can be sure that at least one of your competitors will.

The amount of information shared with tech companies has grown year-on-year and it is only going to increase during 2021 as new innovations materialise. Just consider life before Amazon, Deliveroo, Trainline...did we really go out and collect our takeaways before? It is with the knowledge of the highly sensitive information we share that trust has become such a big issue in recent years. Data protection regulations such as the highly publicised rules of the EU's GDPR present significant challenges for tech companies, and must be considered as part of all ongoing strategies.

In light of the changes required by GDPR, tech companies must pay close attention to the ways in which users' data is stored, and what any new products or ideas might mean for user privacy. As we move into 2021 and awareness of privacy processes grows amongst users and businesses, regulation and implementation will become ever more important.

The conversation should be high on the agenda of C-suite personnel and outside stakeholders (such as your insurance broker) as to how this risk is managed. As we hope to find a way to the light at the end of the Covid tunnel it seems only inevitable that new disruptive technological advancements will continue to emerge.

The need for operational resiliency across enterprise functions has never been greater. Tech sector CIO's are striving to adapt to changing conditions to compose their future business. This requires the organisational plasticity to form and reform dynamically.

Developing a strategy for engaging with policy and regulation can be daunting without the know-how or the capability of a dedicated in-house function.

There is a requirement for fingers on the pulse of policy and regulatory trends in your market and understand how they could affect your business. By conducting in-depth, up to the minute research you can identify worldwide trends in your sector.

To achieve this, tech leaders need to develop the right political expertise and connections to draw out crucial information on upcoming policy changes

and regulations and how they might impact businesses.

To start with tech businesses, need to have a process to systematically monitor developments in government, parliament, regulators and the areas of the public sector that are relevant to your business. Most government and regulatory initiatives are announced via press releases and you can subscribe to receive these in your area of interest from the UK Government, European Commission, etc. Parliamentary proceedings can similarly be tracked through email alerts if a particular phrase is used in the Parliament.

There is an important balance to be struck between ensuring your monitoring coverage is broad enough in terms of keywords that you do not miss relevant developments, whilst ensuring that they are not so broad that you are inundated with irrelevant information. It is also important to ensure that you are covering all political institutions that may be relevant such as devolved administrations and city authorities like the Greater London Authority.

But with 'great power comes great responsibility' the more data a business 'processes' or 'controls' the higher the risk is. Cyber-attacks and errors become ever more costly and so cyber insurance and professional indemnity insurance (errors & omissions) will continue to be two hugely important considerations for tech businesses to protect their own and their client's interests. There is a lot of choice and it is vital that the broking partner can support in navigating to the most fit for purpose products and solutions.

#4 Cyber Security Concerns



The complexity of new technology solutions creates a world of new opportunities. Unfortunately, it also creates a nasty problem for cybersecurity. The old secure perimeter mindset has been rapidly eroding as businesses place more infrastructure in the cloud and allow more access from remote locations. However, activity moving outside the firewall is not the only problem with the secure perimeter.

The volume of threats and the constantly changing tactics of cyber criminals has shown that businesses can't even trust what's happening inside the perimeter. Various techniques have been employed to combat the new threat landscape, but the overall approach has felt like a growing list of best practices.

Hackers have exploited the Coronavirus pandemic to expand their campaigns of attacks against businesses worldwide.

A 238% rise in attacks on banks, and a 600% increase in attacks on cloud servers was observed from January to April 2020 alone. With fewer employees working onsite on the same secure network, it is imperative that companies shore up their networks and upgrade their cybersecurity strategies, and expand them to home networks and mobile work-from-home devices.

We believe that AI and Machine Learning will be important for this trend as we will see the continued increase in attempted nefarious activities require more sophisticated tools and algorithms to fish out.

Microsoft, is one of many companies that has poured resources into security in areas like active directory, software and cloud. There are many companies playing in this space, but through 2021 we expect software, cloud and hardware makers to all be amplifying efforts to make their products and services more secure to deal with certain growth in threats that we have seen throughout 2020.



92% of European businesses have experienced a cyber **breach within the last 5 years**



The UK is the world's **4th largest exporter** of security services. Cybersecurity accounts for the largest share of these exports at **40%**



Cybersecurity firm Avast's listing on the London Stock Exchange was the **largest tech IPO** in Europe and largest IPO on the LSE in 2018, **raising over \$800m**



£1.9bn of cyber security investments by 2021.

The Government is committed to making the UK one of the most secure places in the world to do business



The **UK** cybersecurity industry employs more than **30,000** people



The **City of London Police** have a national responsibility for **tackling cybercrime** and supporting businesses to build an ever more **cyber resilient business** ecosystem





Privacy and Confidential Computing Gains Momentum

Another approach to shoring up cybersecurity, particularly when addressing communications and data privacy, is confidential computing. The idea of confidential computing is to encrypt the entire computing process, not just the data, creating additional layers of security around sensitive information. Google, Microsoft, IBM, Alibaba, and VMware are helping develop new protocols and best practices by way of the Confidential Computing Consortium. The tech is still in a state of relative infancy, but we should begin to see confidential computing slide into the mainstream in 2021.

Managed Service Providers Build Deeper Cybersecurity Expertise

Zero trust is emerging as the new paradigm that guides all the new practices. Instead of trusting any network behaviour or user access that appears to come from a secure location, everything must be verified. That leads to up-front risk analysis to determine which pieces need the highest levels of security. There have been some high-profile instances that have gone towards 'breaking' trust in technology companies and this problem isn't going away any time soon.

Security and privacy are prominent concerns amongst individual users and businesses alike. Everyone is becoming more aware of the sharing of either commercial or personal information and ultimately who is responsible for this information. Pressure will rise on companies whose cyber-security measures aren't robust.

A zero-trust mentality is something that many managed services providers are beginning to understand in earnest. In fact, in the last year, MSPs themselves, based on their position as a management hub for hundreds or thousands of end customer environments, have become a target for hackers seeking access to those customers' networks and data.

MSPs have had to double down on protection. In a CompTIA study last year of MSPs, more than half of respondents said that having cybersecurity skills in their arsenal was the No. 1 factor necessary to sustaining a healthy and successful MSP market throughout 2021.

While this was a pre-pandemic finding, the emphasis on cybersecurity skills and customer demand for them has only grown. One of the more notable trends among MSPs in the last few years has been the shift to redefining their businesses almost

exclusively around security, creating the category known as managed security services providers (MSSPs). In 2021, that category will strengthen.

MSSPs apply security-specific expertise across all customer systems, infrastructure, applications and data. Their portfolio spans a much more plentiful number of security services than the average MSP, including things like penetration testing, SIEM, ransomware protection, compliance audits and governance consulting. And most run a secure operations centre (SOC) either internally or via a third party for added rigor and authenticity.

Nearly 3 in 10 MSSPs said they expect significant growth in the next two years, with just over half predicting modest growth. That said, cybersecurity, especially during this wave of remote working, is a discipline that is table stakes for all kinds of channel partners. It's not a nice to have, but a need to have. Not having security expertise is a dealbreaker for many customers considering whom to work with as a technology provider.

The next step is recognising that data and applications need to be secured individually, and user access needs to be defined at a granular level. Finally, the entire operation must be monitored continuously, using data analysis techniques and machine learning algorithms to check for anomalies and report on overall health. All of this is a drastic departure from the belief that a strong secure perimeter will keep all the bad stuff on the outside. As companies become more comfortable with a zero-trust framework, they will also gain an appreciation for the new investments they have to make, the new processes they have to build, and the new skills they need to acquire.

Technology companies need to have more conversations than ever about their management and protection. As technological usage and advancements continue, we can expect to see more challenges in regards to liability.

51%

of UK businesses in the financial services sector expect revenues to increase



50%

of UK educational institutions expect overall revenues to decrease



41%

of UK businesses expect overall revenues to decrease



#5 Emerging insurance trends for tech sector businesses



Will today's protection be relevant tomorrow?

Technology is one of the world's fastest growing sectors, composed of a highly diverse set of businesses and activities. In an evolving industry, risks change rapidly and that means businesses need to constantly review and evaluate exposures.

With risk being such a moving target, the tech sector requires insurance products that provide evolving and responsive coverage. As part of the evolution in the sector, there is a significant increase in non-tangible threats that come from increased global outsourcing, changing customer demand, intense competition and complex legislation. As we enter 2021, it's imperative tech business leaders ensure their insurance protection today remains relevant tomorrow.

New rules will come into effect from January 2021

As the UK will leave the single market and customs union at the end of 2020, a new free trade agreement will need to be agreed. Currently, guidance is unclear as to what the specific changes will definitely be.

How Brexit will impact the tech insurance sector is still unconfirmed as trading agreements are still to be put into place. Currently, UK insurers will not have passporting rights to EU countries following the withdrawal. At this stage, there are still three possible trading agreement scenarios (all of which result in different outcomes).

Passporting rights allow insurance companies registered in the EEA to do business in other EEA states without additional authorisation being given from each country.

Without passporting rights, insurance brokers in the UK may not be permitted to place certain European risks with insurers. It's worth noting that there might be a difference between individual insurers as each will have different regulatory permissions. UK insurance brokers must instead work with a broker partner local to the country in question to insure the risk.

Some insurers (but not all) have been restructuring their business for a while now, relocating or opening new branches of the business in EU member locations. This should allow them to continue to operate within the EU following Brexit, thus avoiding lost revenue or huge business disruption.



So, if you have locations, employees or trade with customers or suppliers in the EU, it's essential that you ensure your current insurance contracts remain valid and fit for purpose from 1st January 2021. In most cases brokers won't be able to insure European risks without a broker partner in the EU. So, it's important tech businesses work with a broker that has a trusted network of international brokers to support them.

What are the key tech considerations for 2021?

The pandemic has made tech businesses reflect on the adequacy and resilience of their insurance programmes as the sector adjusts to different ways of dealing with the ongoing crisis.

Insurance has a critical role in helping society to #BuildBackBetter, which is the context for insurance companies looking to lead with purpose. Even prior to Covid-19, insurance companies were playing a leading role in grappling with some of the biggest societal challenges: how to assess and insure against the growing impact of the climate crisis, how to price risk in the face of fast-paced technology disruption. A purpose-led approach requires innovation and resilience.

If the experience of 2020 is anything to go by, as we approach 2021, it's vital tech business leaders explore insurance protection against the things we ordinarily can't see coming. The rapid pace of technological change makes businesses decisions more challenging. As tech businesses evolve, they need to ensure that their insurance cover evolves with it.

One of the key risks to tech businesses is contractual liability from a failure in the product or service they provide. They become exposed to tangible risks, i.e. those associated with a physical product, and/or intangible risks, i.e. those associated with advice or design on a third-party basis.

In our experience, over 90% of tech sector claims relate to breach of contract and delay. So fit for purpose Professional Indemnity cover for both tangible and intangible risks is crucial. A crisis can galvanise change quickly as it evaporates norms, but the tech sector will not recover from the crisis by reverting to factory settings. Instead, it must ensure to create positive, lasting, and sustainable change.

Contract Reviews

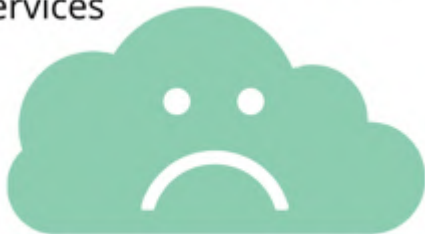
It's important to understand the extent to which liabilities entered into in commercial contracts are protected by insurance. A key challenge for tech businesses in 2021 is to align insurance programmes with new regulatory changes and to ensure indemnity clauses in customer and supplier contracts continue to provide protection against new forms of contractual exposures.

Tech leaders need to examine contract clauses to fully understand the insured and the uninsured exposures, such as hold harmless agreements. Hamilton Leigh provides this service to its clients free of charge. Lee Cohen, Managing Director of Hamilton Leigh Insurance Brokers said "when it comes to tackling risk, insurance should be the last line of defence, not the first - prevention is better than a cure"

When asked what cyber security incidents are likely to occur in their industry in 2021...

58%

of UK companies cited an attack on cloud services



51%

of UK companies cited a disruptionware attack on critical business services



50%

of UK companies cited a ransomware attack



Risk prevention related to each tech business' unique infrastructure, or the complex area of contractual liability and Service Level Agreements (SLAs) should be carried out through a thorough process of risk assessment, education and support services, to identify and limit exposures.


Errors and omissions, cyber threats, supply chain management, business continuity, protecting intellectual property and reputation management have never been more important given the rise in litigation costs, cyberattacks and the expected new UK/EU trading conditions.

Building Resilience

Being at the forefront of innovation can expose tech businesses to risks that aren't covered by standard insurance policies.

A vital component of any technology insurance policy is Professional Indemnity cover for lawsuits brought against the business. Policies should also protect you against the ever-increasing array of cyber risks faced by businesses today; from ransom demands to defamation claims. These are followed by cover for IPR. Tech companies struggle with these insurance areas as the exposures change on a daily basis. Traditionally, most businesses have cover for fire and theft, yet according to Travelers Insurance Company (one of the leading tech specialist insurers in the UK), they are 15 times more likely to have a cyber incident (30% in UK) compared with a fire or theft (2% in UK).

The insurance industry hasn't helped with multiple and extremely varied cyber and tech policy offerings which make comparisons extremely difficult.



Hamilton Leigh currently offers a free insurance audit to help UK tech businesses ensure their post-Brexit insurance programmes continue to be relevant and provide the necessary protection.

Your
Business
Our
Focus

hamiltonleigh
Insurance Brokers

Hamiltonleigh.com | info@hamiltonleigh.com | [@hamiltonleigh](https://www.instagram.com/hamiltonleigh)