Insurance Matters

weald insurance brokers

Autumn / Winter 2020

The hardening market — what it means for you

Inside this issue:

What you need to know:

- The HSE continues to prosecute companies who are in breach of the law. Here are a few examples of the results from December 2019 and January 2020
- A new report suggests thow you can act to protect yourself form the spiralling costs of cyber attacks
- Brexit is upon us, and action is required to avoid unnecessary interruptions to your business ....

You may have heard that the insurance industry is entering a hard market period, but what does that actually mean?

Insurance is cyclical, and the market fluctuates, with each insurance 'season' lasting anywhere between two to 10 years. There are two types of insurance cycle conditions – hard and soft – and we have been in a soft market for the past 10 years.

What is the difference between a hard and a soft market?

In a soft market, you are likely to see:

- *Low premiums*
- *Broad appetite and availability of cover*
- *Increased capacity, meaning insurers write a high volume of policies*
- *Higher limits on policies.*

In a hard market, you are likely to see:

- *High premiums*
- *Reduced appetite due to stricter underwriting criteria*
- *Decreased capacity, meaning insurers write less policies*
- *Lower limits on policies.*

Why are insurance premiums rising?

We mentioned above that in a hard market you typically see higher insurance premiums. Why? During a hard market, insurers place more stringent limits on the cover they can write, which automatically lowers their appetite. This in turn means they are writing fewer policies.

As the insurers' capacity is lower, it can be more in difficult to find insurance solutions and that leads to an increase in demand for cover, all of which drives the premiums up.

The timing could not be worse for UK businesses, but we will have brace ourselves for the fact that prices across all insurance products are likely to increase

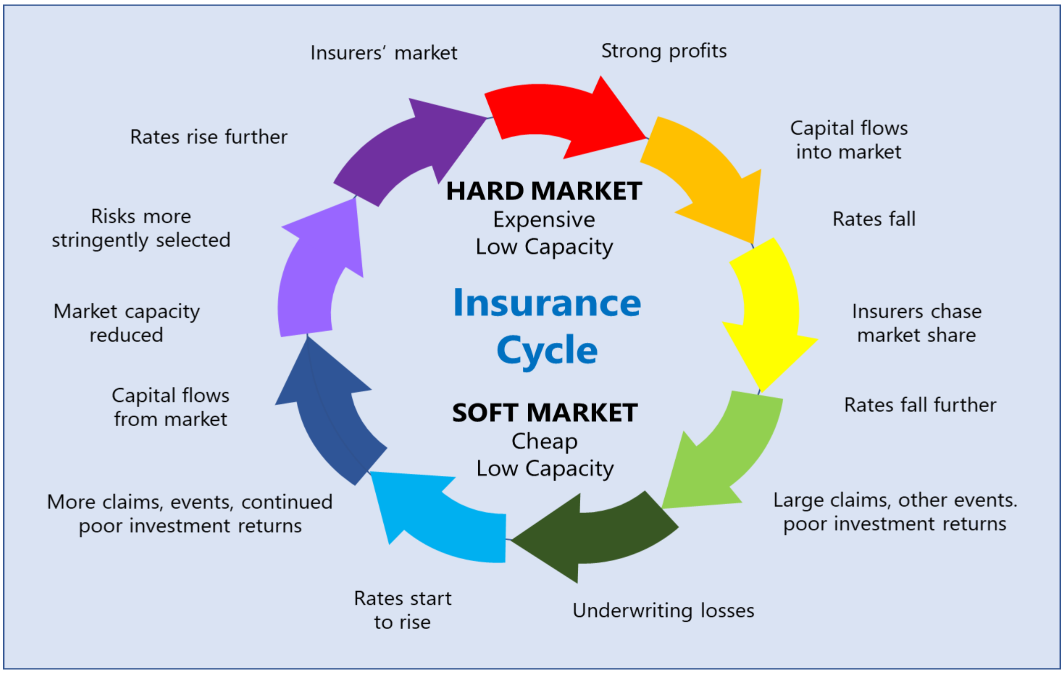
Why is the market hardening?

There are many reasons why we're moving into a hardening market, from natural disasters to rising rates and reduced capacity in the reinsurance market. We've listed just a few of them below.

At the start of 2020 storms Ciara and Dennis created widespread damage, which caused a rise in claims when insurers were already suffering reductions on property premiums.

As we're still part of the EU, the Solvency II law continues to apply. This regulatory regime was introduced in 2016 to harmonise EU insurance regulation. Principally, it aims to make sure policyholders across the EU have the same level of protection, regardless of where they purchase their insurance. It achieves this by increasing the financial resources required for insurers to trade, but this reduces the ability of insurers to underwrite business based on the same resources. It has resulted in some insurers leaving the market, meanwhile others have reduced their capacity considerably.

Another factor is that the Ogden Discount Rate has changed; this is a calculation used to work out how much compensation insurers should award someone who has life-changing injuries to cover them for loss of earnings and any care costs. The rate changed from 2.5% to -0.75% in 2017 and then from -0.75% in 2017 to -0.25% in July 2019 in England and Wales, which has resulted in insurers paying out more on big personal injury claims.



What is the effect of COVID-19?

Even before the Coronavirus pandemic hit, the tides were changing. COVID-19 has naturally had an effect on the market, compounding everything.

John Neal, CEO of Lloyd's of London, told the Financial Times back in April that the pandemic is "no doubt the largest insurance challenge the industry has ever faced". In May, Lloyd's forecast that COVID-19 will cost the insurance industry $203billion (£166billon) worldwide and has recently announced that it expects to pay out £5billion in Coronavirus-related claims. Meanwhile, the Association of British Insurers (ABI) still envisages the UK insurance industry will have to fork out more than £900million for COVID -connected claims, as well as £275million to travellers who had to cancel their trips as a result of the pandemic. This may seem strange to businesses which have not been able to make claims as a result of COVID-19, but the principle of shared costs and pooled premiums which underpins insurance means that it will have an effect across the market.

It is, therefore, likely that COVID-19 will extend the duration of the hard market, as the insurance industry tries to recover from the impact of the crisis.

What does this mean for me and my businesses?

The timing could not be worse for UK businesses, but we will have brace ourselves for the fact that, for at least the next 12 months, prices across all insurance products are likely to increase.

Weald Insurance Brokers will do what we can by way of re-marketing to find the most competitive rates, but we will need to bear in mind that competitive alternatives will be less readily available, and that other factors such as the quality of the policy wording and claims service will play a part in our recommendations to you. We will also give you advice about ways in which you can minimise the inevitable impact of a hardening market, including providing details to us of all the measures which you take to minimise risk and mitigate its consequences.

We have access to a wide range of insurance providers (including specialist schemes) that we can access high levels of cover at competitive rates, but in the current market, key factors for obtaining the best quotes will be the quality of information and timeliness.

It is essential in a hard market that underwriters are given a full understanding of the risk which you pose, and therefore it is important that sums insured are accurately assessed, business interruption limits are properly identified, and full detail about your activities, qualifications, security measures, disaster recovery plans and any other factor which will influence an underwriter positively is set out to your broker and then to the insurers. It is also important to ensure that claims records are up to date, and any outstanding reserves are minimised as far as possible. If the market is hard for good risks, it will be extremely difficult for poorly managed businesses or those with heavy claims records.

In a hard market underwriters are under more pressure to quote on more risks because competitive capacity is reduced......

All of this has to be provided in good time. In a hard market underwriters are under more pressure to quote on more risks because competitive capacity is reduced, and therefore it is essential that you start your renewal process early. This issue is also exacerbated by the fact that even now, and going forward into early 2021 many brokers and insurers are working remotely (not least because this enables them to save some cost), and this will increase the time which you can expect to need to obtain terms for your insurance.

The most important issue therefore is to engage early with your broker to ensure that there is sufficient time review your requirements properly, so that we are not trying to place high limits for covers which are not required for example, and to allow underwriters to respond properly to our presentation to them.

Summary—how to help us help you

- *Be aware of the hardening market, and the upward pressure on premiums.*
- *Understand that reduced capacity in the market does not just drive pricing up, but means that it is more difficult to find cover, particularly for large limits, at all.*
- *Engage with us early — ensure that we have the updated information which we ask for as soon as possible*
- *Consider what covers you actually need, and for what limits or sums insured, If in doubt, discuss it with us.*
- *Help us to present the best picture we can of your business to underwriters — tell us about any risk improvements you have made, or process changes to reduce risks for example.*

Health and Safety News

Company fined after worker suffers crush injury

Chemical company, Reckitt Benckiser Healthcare (UK) Ltd (Reckitt Benckiser Ltd), was fined for safety breaches after a worker had his left arm crushed in a bottle filling machine.

Grimsby Magistrates Court heard how on 9 September 2017, the 25-year-old worker suffered an open crush injury to his left forearm at the company's site in Dansom Lane South, Kingston upon Hull. He also sustained tendon damage to the forearm, wrist and hand.

An investigation by the Health and Safety Executive (HSE) found that the filling machine had not been electronically isolated and locked off by the injured person, or other persons, which would have ensured that the recalibration task could be carried out in a safe manner.

Reckitt Benckiser Ltd of Dansom Lane, Hull pleaded guilty to breaching Section 2 (1) of the Health & Safety at Work etc Act 1974. The company has been fined £200,000 and ordered to pay £8,261.28 in costs.

Speaking after the hearing, HSE inspector David Stewart said: "Non-routine maintenance tasks must be carried out by trained personnel working to standard safe operating procedures. Reckitt Benckiser should have developed a standard operating procedure for the adjustment process, which if implemented correctly along with their lock off procedure, could have prevented the incident."

The Health and Safety Executive remains active in the enforcement of safe working practices

Engineering company sentenced after apprentice narrowly escapes serious injury

A plant hire company has been fined after an apprentice avoided a potentially fatal crush injury from a mobile crane.

During proceedings at Knights Chamber, Nightingale Court, in Peterborough it was heard that on 3 August 2016, an apprentice at M&J Engineers Limited had climbed on to the roof of an accommodation cabin to attach a power float to the chains of a mobile crane. The crane operator, who had not been appropriately trained, began to extend the boom and move the crane into position. The crane had not been set up correctly and the boom of the crane toppled over toward the apprentice. The apprentice jumped out of the way of the boom avoiding a potentially fatal incident. However, his fall from height caused injuries to his leg and back.

An investigation by the Health and Safety Executive (HSE) found the company did not have a safe system of work in place and the crane operator had not been adequately trained. There was no clear instruction concerning the use of the crane or which areas the crane was prohibited from operating. They also had no way of ensuring that the apprentice was suitably managed.

M&J Engineers of Cashel Works, Cadwell Lane, Hitchin, Hertfordshire was found guilty of breaching Section 2(1) Health and safety at Work etc Act 1974. They were fined £220,000 and ordered to pay costs of £65,443.72.

Speaking after the hearing, HSE inspector Nigel Fitzhugh said: "Those in control of work have a responsibility to provide adequate training to their employees so that they can operate equipment safely and devise safe methods of working. This includes providing the appropriate information, instruction and training to their workers."

HSE publishes statistics for Great Britain 2020

We set out below a few of the facts and figures highlighted in the HSE publication.

Work-related ill health

1.6 million	Workers suffering from work- related ill health (new or long-standing) in 2019/20
638,000	Workers suffering from a new case of work-related ill health in 2019/20
32.5 million	Working days lost due to work-related ill health in 2019/20

Work-related stress, depression or anxiety

828,000	Workers suffering from work- related stress, depression or anxiety (new or long-standing) in 2019/20
347,000	Workers suffering from a **new** case of work-related stress, depression or anxiety in 2019/20
	The rate of self-reported work-related stress, depression or anxiety has increased in recent years.
	Workload, lack of support, violence, threats or bullying and changes at work are estimated to be the main causes of work-related stress, depression or anxiety.

Workplace injury

693,000	Workers sustaining a non- fatal injury according to self- reports from the Labour Force Survey in 2019/20
65,427	Non-fatal injuries to employees reported by employers in 2019/20 (RIDDOR)

Fatal injuries

111	Fatal injuries to workers in 2019/20

Enforcement

325	Cases prosecuted, or referred to COPFS for prosecution in Scotland, by HSE where a conviction was achieved in 2019/20
7,075	Notices issued by HSE in 2019/2
£35.8 million	In fines resulting from prosecutions taken, or referred to COPFS for prosecution in Scotland, by HSE where a conviction was achieved in 2019/20

Agriculture, forestry and fishing, construction, accommodation and food service activities, manufacturing and wholesale and retail trade (including motor vehicle repair) had statistically significantly higher injury rates than for all industries

Full details of these and other statistics can be found on the HSE website at https://www.hse.gov.uk/statistics/index.htm

HSE has released its annual statistics on work-related health and safety in Great Britain

Cyber losses continue to climb, but businesses are now spending more for security

Hiscox has published its fourth annual international cyber readiness report. Drawn from a representative sample of 5,569 organisations across eight countries by size and sector, this survey explores the actions of the people on the front line of the business battle against cyber crime.

Its headlines are stark — cyber losses among businesses have risen nearly six-fold during the past year, from a median cost of $10,000 per firm to $57,000, and total cyber losses among the study group rose from $1.2 billion to nearly $1.8 billion during the same period.

The highest recorded total loss for any one company over the duration of the year was $87.9 million (a UK financial services firm) while the highest loss from any one event was $15.8 million (a UK professional services firm).

The most heavily targeted sectors were financial services, manufacturing and technology, media and telecoms (TMT), which Irish firms suffered the highest median costs, at more than $103,000.

Firms increased their cyber security spending by 39%. Expert firms spent more and plan to go on doing so

The one bit of good news cited by the study is that the proportion of firms reporting a cyber security event in the past 12 months is down from 61% to 39%.

The numbers were strongly influenced by a relatively small group of firms that reported 500 or more events, but it confirmed that "More than half of all enterprise firms (51%) – those with 1,000 -plus employees – said they had at least one cyber incident," but not all of the targeted businesses were large. The report points out that there were super-targets in each of the five size brackets, and a surprising number were among the smallest.

There are a number of reasons for this result. In many sectors, the majority of micro-firms have nobody managing cyber security. The smallest transport and distribution firms look particularly vulnerable with 59% saying they have no such role, either internal or external. Equally, dependence on a managed service provider (MSP) may backfire when that MSP is itself attacked. Some firms could simply be over-counting by including spam emails. A lack of effective counter-measures among some smaller companies provides one explanation. Analysis of the data suggests firms with fewer than 12 computers, and where anti-virus or anti-spyware was not deployed consistently across the organisation, were particularly likely to be super targets.

The report points out that, worryingly, 11% of overall respondents said they did not know how many times they had been targeted. That was up from 4% the previous year. Surprisingly, too, the largest percentage of 'don't knows' (15%) was among enterprise firms with more than 1,000 employees.

The report looks at the rise of ransomware attacks in particular. Hiscox are seeing hackers' ransomware techniques evolve. Typically in larger attacks there are two distinct phases after the initial infection. The first phase is lateral movement. This is where attackers look for valuable assets (e.g. finance data) and assess the size of the target to set the ransom amount. The second phase is ransomware attack. This often happens at the weekend when there is less chance to react and when hackers can cause the most damage. There can typically be a period of one to three weeks between these two phases. Companies with good detection capabilities can stop the attack in this time and therefore suffer shorter outages, lower overall costs and less impact to business.

The softer impacts of a cyber breach are often not mentioned or are simply too hard to quantify. Their gravity should not be doubted. Significantly more respondents this year mentioned either increased difficulty in attracting new customers (15% of firms that had been targeted, up from 5% before), the actual loss of customers (11% compared with 5% before) or the loss of business partners (12% compared with 4%). Nearly one in five French firms (19%) reported greater difficulty in attracting customers after an incident or breach. Sixteen percent of Belgian firms lost business partners (compared with a mean 12%). Overall, 15% of firms that were targeted said they had reevaluated the cyber security of their supply chain (up from 8% the previous year) or been subjected to increased evaluation by their own customers (15% compared with 10%). Bad publicity, affecting the brand or the company's reputation, was mentioned by 14% of respondents (up from 5% before). One in eight (13%) said they had experienced a reduction in business performance indicators such as their share price (up from 5% the previous year).

Cyber readiness — the ability to deal with cyber attacks — is clearly an area where size matters. Big businesses have big resources. There is a clear correlation between the numbers employed in the security function and a firm's readiness score. For instance, firms employing more than 50 people in their security team constitute only 11% of the sample, but represent 19% of experts. Among businesses with 1,000-plus employees, 29% boast security teams of this size. Big firms spend an order of magnitude more than their smaller counterparts. While the average micro business spent $13,000 on cyber security in the past year, firms with 1,000-plus employees spent on average $8 million.

On the whole, spending appears to buy expertise. Firms ranking as experts spent on average $4.2 million on cyber security in the past year, compared with the average novice spend of $1.3 million. Though there was an increase in smaller businesses in the report this year, the overall readiness score has still improved. That is largely down to a doubling (or more) in the numbers of medium, large and enterprise firms ranked as experts compared with last year.

While a smaller number of firms experienced cyber events in the past year, the costs spiralled.

By contrast, nearly four out of five micro businesses with between one and nine employees (79%) ranked as novices. Across all respondents, the number saying their firm had 'no defined role' for cyber security increased from 16% to 20% (nearly half of micro businesses had no such role). The proportion using external service providers remained constant, at 19%.

What lessons should you learn?

1. **Do the basics well.** Identify every device in the organisation. Back data up off-site and learn from each incident or breach.
2. **Follow a framework.** Make sure that all the virtual doors and windows are shut. A framework such as CyberEssentials will help you with the five important areas: identify, protect, detect, respond and recover.
3. **Don't penny pinch.** Cyber experts direct a larger proportion of their IT budgets to cyber security and more of them plan to lift spending in every cyber-related area in the year ahead.
4. **Invest in training.** Novices suffered more breaches resulting from successful phishing and malware attacks. Regular training to drive awareness throughout the workforce is vital
5. **Get management involved.** Nine out of ten experts agree that cyber security is a top priority for executive management. Only half of novices feel able to say the same.
6. **Build resilience.** No business will ever be completely secure. But all can build resilience by preparing for a breach, testing for it and having the capability to respond quickly and effectively. A standalone cyber insurance policy helps build that resilience through certainty of cover and specialist expertise such as risk assessment, crisis management and training.

"*Take-up of standalone cyber cover remains patchy, with more than half of firms in our report relying on more general cover*," said Gareth Wharton, Cyber CEO, Hiscox, in a forward to the report. "*This is a conundrum. Almost certainly, they would all have cover for fire and theft, yet the report suggests they are 15 times more likely to have a cyber incident (30% in UK) compared with a fire or theft (2% in UK).*"

It makes you think, doesn't it…….

For the full report, go to:

https://www.hiscoxgroup.com/sites/group/files/documents/2020-06/Hiscox-Cyber-Readiness-Report-2020.pdf

Weald Insurance Brokers Ltd

Falcon House
Black Eagle Square
Westerham
Kent
TN16 1SE

Phone: 01959 565678
Email: info@wealdinsurance.com

www.wealdinsurance.com

Take action to prepare for Brexit

It is fair to say that owner-managers can be forgiven for allowing Brexit to fall down their list of priorities; there have been one or two other pressing matters to attend to.

However, this month, the Business Secretary, Alok Sharma, has written to all businesses at their registered office address to remind them that the transition period ends on 31st December 2020 and there will be new rules to follow from 1st January 2021 for businesses that deal with Europe.

You need to act now if you are:

- Importing goods from the EU
- Exporting goods to the EU
- Moving goods to or from Northern Ireland
- Travelling to the EU
- Living and working in the EU
- Staying in the UK if you are an EU citizen

You should also check with your key suppliers and customers that they are also taking action.

The impact on your business and the changes you need to make will depend on your business sector and how it operates.

Please visit www.gov.uk/transition where you will be able to complete a two-minute questionnaire to get a complete list of what you need to do. The Government is providing a range of support, including webinars which are available to watch on demand at www.gov.uk/transition-webinars

There is a risk that your business operations will be interrupted if you are not ready for the new rules from 1st January 2021.

Our business accountancy partners A4G are happy to give further advice on the issues at stake here. You can contact them on 01474 853856 or at enquiries@a4g-llp.co.uk

Take action to survive and thrive

Whether or not you agree with the Government's assessment that Brexit will bring new opportunities to your business and the UK economy, there will be issues within your business that you need to tackle if you are to survive and thrive.

A4G's Breakthrough programmes are designed to help four types of business owners:

1. Those who are just starting their business
2. Those who want to grow
3. Those who want more freedom by either selling up or making their business less dependent on them
4. Those who need help emerging from the Coronavirus pandemic and rebuild their business in a profitable and efficient way