



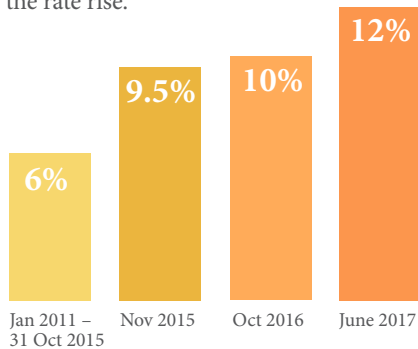
The Perfect Storm

After a long period of stable insurance costs, the perfect storm is brewing that is likely to see your insurance premiums increase significantly. There are two big changes afoot in the industry, both created by regulatory bodies, the impact of which will be felt this year.

What are the big changes in the industry?

Insurance Premium Tax Rise

Insurance Premium Tax (IPT) is a tax levied by the government on most general insurance premiums. IPT has recently risen to 12%, this is the third time in two years that we have seen the rate rise.



What does this mean for me?

With two rises in the last 12 months some policyholders will be seeing tax charged of 2.5% higher than their last renewal, depending on their renewal month. On a qualifying general insurance premium of £10,000 that could mean a rise in the total cost of £250 just on the tax alone.

The Insurance Discount Rate

The change to the Insurance Discount Rate is another important development. On 27th February 2017, the Lord Chancellor announced a cut in the discount rate, moving it from +2.5% to -0.75%. The discount rate is applied to lump-sum payments made by insurance companies to claimants following injuries sustained in motor accidents, accidents suffered at work or on another's premises.

What does this mean?

The percentages concerned might sound like small numbers but when applied to large settlement figures will have a dramatic impact on the amounts that insurers will need to pay out. An example of this is a brain injury suffered by a 30 year old plasterer may have previously been settled at £2.24m but would now rise to £6.14m. *

How will this impact my premiums?

Whilst it is unclear exactly how much of an increase will be faced by the average customer, insurers will need to factor increased settlements into their premium calculations. The overall cost for the insurance industry across all current claims that are impacted is estimated to be £7billion.

We are all working hard in the industry to manage the implementation of the changes and lessen the impact to our clients.

Is there anything else I should consider?

The increased settlements required in respect of liability claims may leave shortfalls for businesses that do not have sufficient levels of indemnity in place. Whilst the government sets the minimum levels of compulsory Employers Liability cover at £5 million, they will not step in to meet a shortfall should the limit be inadequate – the company concerned would be expected to fund the gap. Most small businesses would be unable to meet a demand for an additional £1.14 million in the case of the example above and might be forced out of business.

What should I do?

Despite the prospect of insurance costs rising, it is vital to avoid the temptation to counteract this by reducing protection. We can help you to assess your current levels of insurance and your indemnity limits and to prepare for the changes ahead.

// The overall cost for the insurance industry across all current claims that are impacted is estimated to be £7billion.

*Claims example provided by AXA.

Inside This Issue

The Perfect Storm

Gone Phishing

Who's Watching You

Data Protection Regulations

Take a break from Modern Life

What happens when you can't get in to work?



Gone Phishing

Did you know it's now possible to insure against the UK's most common crime?... Cyber-attack.

Cyber-crime continues to make headlines on an almost daily basis in the UK. We frequently hear about national companies falling prey to high profile breaches of systems and data. This often results in widespread disruption for their clients as well as financial and reputational loss for themselves.

How does this affect me?

Often the sheer scale of the figures being reported and the intangible nature of the loss make it hard to relate to as a small business owner. However cyber-crime is no longer a large company problem, it is estimated that over 74% of SME's in the UK have fallen victim to a cyber breach.

Whilst the stories hitting the headlines often involve sophisticated ransomware, the types of incidents that hit small business across the UK on a daily basis are often much simpler examples of cyber-crime. Many are caused by simple phishing scams rather than sophisticated cyber-crime. Cyber criminals aren't just interested in targeting big business and in our increasingly connected world it's no longer a case of 'if' a business will experience a loss, but 'when'.

Could you be caught out by the following?

Telephone Hacking

A firm of insurance brokers recently had a new VOIP (web hosted) telephone system installed in their offices to reduce call costs. Fraudsters managed to use a piece of software to crack the password to the phone network and programmed the telephone system to repeatedly make calls to a premium rate number owned by them. One month later, the firm was contacted by their telephone network provider to confirm that they had racked up £25,000 worth of calls. Despite confirming that they had been the victims of hacking, the telephone company insisted on payment of the outstanding bill.

Phishing Scam

The financial controller of a small high street law firm received a call from someone purporting to be from the firm's bank, advising that some suspicious wire transfers had been flagged on the business account. The caller insisted that the firm may have already had funds stolen from their account and were in immediate danger of all of the remaining funds being drained unless they put a freeze on the account, for which the bank would need to be told the password and pin code.

Not wanting to be the cause of any further loss, the financial controller confirmed the pin code and password to the caller, who then confirmed that the freeze had been successfully applied and that they would be in touch again once the situation was resolved. Upon calling the bank the next day to check in, the financial controller was told that the bank had not in fact been in contact and that £89,991 had been wired to three overseas accounts in nine separate transactions. It was now too late to recall the transactions and as they had seemingly been authorised, no reimbursement was offered by the bank.

CEO Fraud

A fraudulent yet almost identical looking e-mail address for the Managing Director of a medium sized building contractor was created by fraudsters who used it to instruct an individual in the accounts department to make a wire transfer payment of £50,000 to a new materials supplier. The e-mail stated that the new supplier was being used to source additional materials for a crucial job and that payment had to be made urgently to secure delivery of the goods. The e-mail was sent whilst the MD was on holiday so that no face to face verification could be made. The account to which the funds were transferred actually belonged to the fraudsters who were able to retrieve the money before the transaction could be recalled. **

How prepared are you for a cyber-crime incident?

Cyber offences now account for over half of all crime in the country. Last year the National Crime Agency revealed that cyber-crime had officially overtaken traditional crime in the UK. Where once it was masked bandits holding up bank tellers, we're now seeing teenagers stealing cash from businesses from the comfort of their bedroom, yet many are still uninsured against the risks this poses.

When an attack happens, cyber insurance can help to cover both the immediate financial fallout and the costs associated with getting specialist help to manage the incident, whether that's forensic investigators, IT specialists, legal experts or even PR support to ensure it is resolved quickly and effectively.

And contrary to popular belief, getting a policy is relatively painless and might not be as expensive as you think.

Contact us today for a full review of your cyber exposure and let us help take the worry of cyber criminals away.

*www.theguardian.com/uk-news/2017/jan/24/uk-fraud-record-cybercrime-kpmg

**Claims scenarios provided by CFC underwriting



Who's Watching You?

Are you aware of just how many governmental departments and independent agencies have powers to investigate and prosecute you or your business for breaking the law or breaching regulations – you might well be surprised!

To name just a few, the Environment Agency has the power to investigate breaches of environmental law; HM Revenue and Customs have the power to investigate tax evasion and the Financial Conduct Authority can investigate breaches of codes of conduct by businesses or professionals that provide financial services.

Whilst regulators provide a vital service, finding yourself under their microscope can be a scary experience.

Investigations can result in punishments being issued by the relevant body or even criminal proceedings in court, the impact of which can be devastating to your business or you personally.

Regulators have many powers they can use when investigating regulatory offences or related crimes, including the following;

- Interview you under caution
- Search your offices or home
- Freeze your company or personal assets
- Force you to hand over documents or information
- Prosecute you through the Magistrates or Crown Courts
- Charge you with a criminal offence
- Seize and search your computer or other electronic devices

Your business activity may not bring you into direct contact with the regulators mentioned but there are many more including;

- Serious Fraud Office
- Office of Fair Trading
- Competition Commission
- Department for Business, Energy & Industrial Strategy (BEIS)
- Vehicle & Operator Services Agency – VOSA
- Health & Safety Executive (HSE)

If you are the director or officer of a business you may have personal liability for any actions or decisions you make on behalf of your company and could face having to pay the costs of defending yourself, legal costs can run into thousands of pounds. Management Liability Insurance is a type of cover that offers financial protection to those who are the director, partner or officer of a company. It is designed to cover the cost of claims for compensation made against the insured individual.

Speak to us about your existing level of cover and further steps you can take to stay protected.



Whilst regulators provide a vital service, finding yourself under their microscope can be a scary experience.



News In Brief

New General Data Protection Regulations Coming Into Place

As technology advances so does cyber-crime and we're seeing increased threats to bigger organisations such as the NHS and even the writers at Game of Thrones. The government are stepping up their fight against cyber-crime; in May 2018 we will see the new General Data Protection Regulations come into place bringing with them more stringent controls over the storage and use of personal data.

We will keep you informed as we get closer to the launch date.



Take a break from modern life

We are increasingly living in a world where people are adopting a 24/7 mentality and are never really taking the time to switch off. As the digital age continues to grow there are increasing temptations to draw you to your devices, whether to check your social media accounts or read the news.

Businesses are finding that employees don't even switch off when they're on holiday or out for dinner. This may feel like an efficient and responsive culture, but we need to be careful to maintain our usual standards of professional behaviour when communicating with colleagues and clients, not always easy after a bottle of Merlot!

Earlier this year in France, an employment law was put into force that obliges organisations with more than 50 workers to start negotiations to define the rights of employees to ignore their smartphones. Overuse of devices is one of the most common reasons for staff burn out, so this regulation is intended to combat the "always-on" work culture which has led to an increase in unpaid overtime.

In economically challenging times staff can worry about taking a stand and switching off their devices so it's up to businesses to be responsible. Some organisations may rely on employees to still pick up work whilst they are off as they don't have a suitable replacement. This means that employees are never really having time away from work which could harm their overall professionalism and well-being.

Unfortunately, there isn't a quick fix to change cultural behaviours but here are a few things you can do to improve your workplace:

- Hold regular staff meetings, including group and individual meetings. -This way employees have a place to air any grievances.
- Outline job expectations and requirements. -This will help to motivate employees and help them to understand their role.
- Ensure you have provision in place to cover staff absences, that way employees aren't coming back from holiday to deal with problems
- Encourage workers to switch off from work during their holidays.

www.theguardian.com/money/2016/dec/31/french-workers-win-legal-right-to-avoid-checking-work-email-out-of-hours

What happens when you can't get in to work?

How would you cope if your staff and customers were denied access to your premises for a week?

Would your business still be able to operate?

Would you be able to fulfil your orders?

Would your business be able to bounce back?

Traders in London's Borough Market, the capital's oldest market were forced to face these questions recently. The market was closed for ten days after the London Bridge terror attack in June of this year leaving traders unable to operate for the duration. The degree to which this affected their business financially varied greatly depending upon the level of insurance cover they had in place.

Even policies which offer business interruption cover may not mitigate this event as it was classified as a terror incident, many policies will not pay out in response to incidents of terrorism unless the insured suffered material damage to their own property.

We can help you to conduct a full review of your existing insurance arrangements to see exactly when you can trigger cover and the types of incidents your policy will address. We can also discuss products which might help you in the event of a similar attack.



Rees & Co Insurance Brokers,
Suite 2, First Floor,
Thorpe House,
25 King Street,
Hereford
HR4 9BX

CONDITIONS AND LIMITATIONS

The sole purpose of this publication is to provide guidance on the issues covered. It makes no claims to completeness and does not constitute legal advice with respect to any set of facts. The information it contains is no substitute for specific legal advice. If you have any queries regarding the issues raised, please get in touch with your usual contact or the authors of this publication.