DAS MARKET BAROMETER: CYBER

IN CONJUNCTION WITH HSB

Munich RE

1866

HSB Engineering Insurance

DAS FIRST FOR JUSTICE

CONTENTS

ABOUT US

DAS UK Group: www.das.co.uk

The DAS UK Group comprises an insurance company (DAS Legal Expenses Insurance Company Ltd), a law firm (DAS Law), and an after the event legal expenses division.

DAS introduced legal expenses insurance (LEI) in 1975, protecting individuals and businesses against the unforeseen costs involved in a legal dispute. Today it has over nine million policyholders.

The company offers a range of insurance and assistance add-on products suitable for landlords, homeowners, motorists, groups and business owners, while its after the event legal expenses insurance division offers a civil litigation, insolvency, clinical negligence and personal injury product. In 2013, DAS also acquired its own law firm – **DAS Law** – enabling it to leverage the law firm's expertise to provide its customers with access to legal advice and representation.

DAS is part of the ERGO Group, one of Europe's largest insurance groups (the majority shareholder in ERGO is Munich Re, one of the world's largest reinsurers).

DAS Website:
www.das.co.uk

DAS UK Group Twitter:
www.twitter.com/DASLegalUK

DAS UK Group Facebook:
www.facebook.com/DASUKGroup

DAS UK Group LinkedIn:
www.linkedin.com/company/das-legal-expenses-insurance

DAS Law LinkedIn:
www.linkedin.com/company/das-law

HSB Engineering Insurance: www.munichre.com/HSBEIL

HSB Engineering Insurance is a leading specialist provider of engineering and technology insurance, engineering-based risk management and inspection services.

As part of Munich Re, HSB Engineering Insurance comprises of an insurance company (HSB Engineering Insurance Limited) and a subsidiary inspection services company (HSB Engineering Insurance services Limited).

The insurance company provides specialist products to cover engineering and technology risks including construction, energy, equipment breakdown and cyber. Whilst the inspection services company provides third party statutory examinations of equipment and machinery through its national network of engineer surveyors.

HSB Engineering Insurance is the UK-based arm of Hartford Steam Boiler, a leading global provider of specialty insurance, inspection services and engineering consulting. Founded in 1866, HSB's heritage is built on providing specialist engineering insurance and inspection services. HSB holds A.M. Best Company's highest financial rating, A++ (Superior).

The HSB Group is a wholly owned subsidiary of Munich Re, one of the world's leading reinsurers.

HSB Engineering Insurance Website:
www.munichre.com/HSBEIL

HSB Engineering Insurance Twitter:
www.twitter.com/hsb_eng_ins

HSB Engineering Insurance LinkedIn:
www.linkedin.com/company/hsb-engineering-insurance

FOREWORD

It's my pleasure to introduce the third in our series of market barometers. Cyber-crime is big business. Just recently Spanish police arrested a criminal mastermind suspected of stealing an extraordinary €1bn through malware attacks against various banks. Meanwhile developments such as the 'Internet of Things' – enabling a raft of 'smart' devices (from cars to the kettle) to exchange data – have ensured that cyber-criminals have the ability to not only infiltrate businesses, but also our personal lives in a myriad of ways.

Against this backdrop it is of little surprise that the majority of brokers in our survey expect the cyber insurance market to grow rapidly in the next couple of years. There is certainly plenty of potential for growth – whereas cyber insurance products for businesses are being sold by over two-thirds of those who responded, just 13% of brokers are selling similar products for the general public.

Of course, any sort of serious cyber issue can paralyse a small business but it's important to remember the vast potential of the consumer market. For many people technology around the home is no longer a luxury, it is an absolute necessity providing entertainment, a means of communicating with friends and family, organising day-to-day life, and even putting the kettle or heating on.

So whilst the need for cyber protection is clear and undoubtedly the market will grow, delivering the right solution for customers is paramount and in this context some difficult questions are starting to emerge.

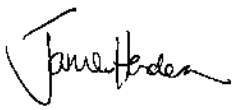
We undertook this research as part of our own cyber development journey because we really wanted to understand the consistencies and potential inconsistencies that might exist between consumers, SMEs and brokers in terms of their level of understanding of cyber, but also how their attitudes and behaviour might affect the appropriateness of any cyber insurance solution.

Our hypothesis, forged in a concern about some of the 'mass market' cyber products that have been launched recently, is that there might be an emerging gap between understanding, attitude and behaviours – and the results of our research certainly support this.

Mis-selling risk would be too strong a statement to use right now, but when you consider the very real differences in levels of understanding between brokers, consumers and SMEs highlighted in our research, combined with the fact that we have identified behaviour we call 'cyber denial' that has the potential to invalidate the cover of many cyber policies, you can see the potential problem on the horizon.

Furthermore, as insurers wrestle with the concept of the silent cyber exposure they already have on their books, the very real risk remains that the consumer or SME is buying cover for cyber that they already have elements of protection for via other insurance products such as legal expenses insurance. This raises the question as to whether a standalone or integrated solution is the best approach. But, regardless of the specifics, cyber insurance is undoubtedly going to become protection that all consumers and businesses will seriously need to consider.

All of these issues are important considerations for insurers considering product design and brokers considering suitability and will be central to the next phase of our own cyber development journey. We took the view that this was context worth sharing, and if this helps others to develop better solutions as well, then that's a good outcome too.



James Henderson
Managing Director Insurance UK & Ireland, DAS UK Group

FOREWORD

I'm delighted that HSB is working in partnership with DAS UK Group on this cyber edition of the market barometer. With more reliance on online activities, smart devices, and connected technology, the impact on businesses and individuals from cyber-crime can be devastating. As cyber criminals become ever more sophisticated and access to our data gets easier, there is no doubt that looking after our identity and data is of key concern to us all.

The cyber insurance market is still relatively in its infancy. Until recently cyber insurance was primarily focused on large businesses and corporates. However, as the commercial cyber market has matured, insurance products targeted specifically at SMEs have become more widely available.

With less available IT security resources, the financial impact of a cyber incident for an SME may be detrimental to their business. Increasingly SMEs are becoming the target of online fraud; which is why it is unsurprising that SMEs rated this as one of their top five cyber security concerns in the survey.

Whereas global ransomware attacks may make headlines, the cost of these incidents are relatively low in comparison to a targeted phishing scam, which (in our experience) can result in a loss of tens of thousands of pounds – a cost which can be significant for a small business. And criminals are becoming more sophisticated in their scams, using employees as the weak link in the chain to gain access.

Cyber insurance is undoubtedly an expanding market and one that is predicted to continue to grow by the majority of brokers interviewed in this research. Education and training is one of the most important things that insurers can do to support brokers; and nearly a quarter of brokers wanted policies to be simpler.

The development of personal cyber insurance is the next stage of the evolution for cyber. With the reliance on our devices for day to day living, together with the advancement in the 'Internet of Things' and connected smart home technology, security risks and vulnerabilities will undoubtedly increase – as will the impact that cyber-crime has on us.

So as technology and cyber-crime continues to evolve, there is no doubt that this is an emerging risk that businesses and individuals will need to be educated on and protect themselves against.

Stephen Worrall
Managing Director, HSB Engineering Insurance

ABOUT THE RESEARCH

This report is based on three pieces of research commissioned by DAS UK Group and HSB:

- A survey of consumers carried out by Jigsaw Research from 4-11 December 2017
- A survey of SMEs carried by Jigsaw Research from 23 February-9 March 2018
- A survey of brokers carried out by FWD Research in March 2018.

SAMPLING

For all groups bear in mind that we cannot guarantee that the views of the survey sample are the same as the wider population.

- Consumers: 1,000 x 10 minute interviews with a representative sample of UK adults.
- SMEs: 200 interviews with SMEs, with around 5 minutes on cyber questions.
- Brokers: 250 x 7-8 minute interviews. Respondents were general insurance brokers: 52 nationals (top 50 firms), 51 super regional (top 51-250 firms) and 147 provincial.

WHY WE COMMISSIONED THIS RESEARCH

Cyber risk is a growing threat, but one that is – we think – poorly understood. With cyber insurance starting to filter down from larger businesses to SMEs, and just starting to appear for consumers, we thought the time was right to look at the subject in more detail. We looked at:

- What do people worry about?
- What have they experienced?
- What precautions do they take?

We were particularly interested in the differences between consumers, SMEs and brokers. Do brokers understand their clients? How different are consumers and SMEs? This research will help us understand the needs of all these three groups, in terms of products, information and other support.

THE RESEARCH: SUMMARY OF KEY FINDINGS

1 The cyber insurance market: the opportunity is here... nearly

Perhaps the key point from the research is that cyber insurance is here to stay. The market appears to be developing rapidly with 58% of brokers surveyed expecting it to "grow a lot" in the next two years.

Brokers are also aware of the burgeoning importance of cyber insurance with 56% rating the cyber threat as either the most important – or among the most important – growing insurance risk faced by SMEs and consumers.

Brokers have certainly been swift to take advantage of this developing new market with cyber insurance products for businesses being sold by over two-thirds of those who responded. The consumer market, however, is still in its infancy, with just 13% of brokers selling similar products for the general public.

2 Cyber risks: does overconfidence and an alarming failure to take basic preventative measures actually render most potential customers either uninsurable or a serious insurance risk?

In March last year the Crime Survey for England and Wales* revealed that cyber-crime has become utterly ubiquitous, accounting for 57% of the 1,920,900 incidences of all fraud reported in the previous 12 months (and this doesn't even include cyber threats such as ransomware, denial of service attacks and malicious damage).

But, despite this, whereas both consumers (88%) and SMEs (89%) are confident when dealing with cyber security, they appear to be breathtakingly over-confident (or simply in denial) when it comes to protecting themselves.

The 'cyber denial' prevalent amongst consumers is demonstrated by the fact that nearly a quarter are failing to take even basic – and well-known – precautions such as using anti-virus software (23%) or 'strong' passwords (24%). This is supported by other alarming statistics such as 34% not using different passwords on online accounts, 41% delaying before installing system updates, and, perhaps most surprisingly, 51% fail to regularly back-up their data.

The hubris amongst SMEs, meanwhile, is even worse. A higher proportion fail to use anti-virus software (47%) or 'strong' passwords (42%), while 50% do not use different passwords on online accounts, 55% delay before installing system updates, and under half (47%) regularly back-up their data.

When we consider that figures† also released last year revealed that 2.9 million UK firms suffered cybersecurity breaches in 2016 – at a cost of an extraordinary £29.1 billion – this is undoubtedly disquieting, even more so when we consider that a cyber-attack is actually potentially far more devastating for the SMEs that make up the vast proportion of our economy than larger companies.

Of course, if consumers and businesses are this cavalier in their approach to cyber security, it could also beg the question as to what the insurance industry can do to help educate potential customers, not to mention whether they are actually insurable – or too large an insurance risk – in the first place.

> "Phishing and social engineering attacks on businesses tend to aim to steal sums over £10,000, a serious hit for a small business. Ransomware attacks usually ask for smaller amounts so that the victim is more likely to pay up – but paying up makes you a target for more attacks."
>
> **James Henderson, Managing Director Insurance UK & Ireland, DAS UK Group**

*www.crimesurvey.co.uk/SurveyResults.html

†www.beaming.co.uk/press-releases/cyber-security-breaches-cost-businesses-30-billion

3 Lack of basic cyber knowledge amongst consumers and brokers

The days of frantically scouring the keyboard to find the 'Any' key may have passed but there is still widespread consternation when it comes to understanding some technology basics.

Among the starkest statistics from the research are that over half of consumers (54%) wouldn't know how to check a website is genuine, opening themselves up to fraud, or the 63% of consumers who did not know that banks are not required to refund money that is transferred to fraudsters. It is of course debatable as to what the financial services/ insurance industries can do to counter such a lack of wider technological knowledge.

For the insurance industry the potential risk of mis-selling also rears its head when we consider that almost one-third of UK brokers (31%) admit to poor or very poor understanding of cyber risks and cyber insurance. Of course, it is hoped that brokers with a low knowledge of the issues are not the ones actually selling the products – and it may simply be a case that brokers are accepting that they have much to learn – but with just 8% feeling they understand these issues "very well", this may not bode well for the future.

4 What are the biggest cyber threats?

Consumers and SMEs are worried about very similar things. For consumers it is identity theft, personal data being stolen, online fraud, malware, and loss of data, while for SMEs it is online fraud, loss of data, identity theft and malware.

When asked what problems they had experienced in the last three years, the most common response from consumers was viruses and malware, which was also the second most common problem for SMEs (23%). However, consumers also said that in most cases a virus or malware infection didn't have a large impact on their lives (63%), suggesting that most infections do little damage or are fixed relatively easily.

The most significant problem for both consumers and SMEs may well be loss of data. Of all the problems experienced by consumers, loss of data had the biggest impact – loss of data stored locally had a large impact for 55% of people and loss of data stored remotely a large impact for 60%. 25% of those who lost remotely stored data said it had a "huge impact" on their lives – these individuals may have lost emails, photos, contacts or important documents stored 'in the cloud'. For SMEs, loss of data stored locally could have a major or moderate impact for 78% of people and loss of data stored remotely a major or moderate impact for 70%.

Brokers' assessment of the cyber risks their clients face is fairly close to the reality. They are well aware of the risk of data theft or loss for SMEs, although they miss the fact it is a major problem for consumers.

> "The biggest risk for SMEs and consumers at the moment may be ransomware (and subsequent data loss), which encrypts the information on your computer or device and stops you using it unless you pay a ransom (and even paying a ransom is no guarantee that you'll get your data back). In most cases it's not possible for an expert to unencrypt this information, so the only options are to pay the ransom or to wipe the computer/device. This is just another reason why it's important to regularly back up your data!"
>
> **Stephen Worrall,**
> **Managing Director, HSB Engineering Insurance**

THE RESEARCH: CONSUMERS

As we've seen, consumers are in 'cyber denial' when it comes to dealing with issues of cyber security. They largely believe that they have the knowledge of what needs to be done, but significant numbers are failing to take even the most basic of precautions.

They are also seemingly oblivious to many IT and technology basics, including the range of threats to their shiny new devices. Of course, what is difficult to assess is whether they really don't know what to do, or that they know what to do and simply aren't doing it...

OVERALL CONFIDENCE DEALING WITH COMPUTER/ONLINE SECURITY

64% fairly confident

24% very confident

18-24 years **32%**

25-34 years **30%**

12% not very confident

75+ years **22%**

65-74 years **18%**

TOP PRECAUTIONS TAKEN TO PROTECT THEIR HOUSEHOLD AGAINST CYBER RISKS

77% use anti-virus software

76% use 'strong' passwords

66% use different passwords on different online accounts

59% install operating system updates promptly when they are available

49% regularly back-up data

> "The threat to mobile devices from viruses and malware is a growing one, with ransomware a particular problem."

James Henderson,
Managing Director Insurance UK & Ireland,
DAS UK Group

BUT DO YOU ACTUALLY KNOW? CONSUMER KNOWLEDGE OF CYBER RISKS

1 Social media sites like Facebook rarely verify people's names, ages or other personal details

This statement is **TRUE**, but almost half of people got it wrong or didn't know.

The lack of knowledge demonstrated here may have implications for parents who may mistakenly believe that social media sites are better moderated then they really are.

2 You retain full ownership and control of all photos, videos and data published on social media sites

This is **FALSE** but 49% of surveyed consumers didn't know this (23% thought it was true and 26% didn't know).

People are seemingly unaware that social media sites can retain various rights over things people post which also makes it hard to ever completely delete or remove your 'digital footprint'.

3 An SSL certificate is a way of checking if a website is genuine

Less than half of people knew this was **TRUE**. The largest number of people (47%) simply didn't know.

How can you be sure that a website is genuine? Look for a little green padlock next to the address. This shows the site has a valid SSL certificate, and will tell you who the owner of the site is. If there's no SSL certificate, or the owner is not who you expect, don't give them any sensitive details!

4 Banks are required to refund money that is transferred to fraudsters

Just 37% recognised that this was **FALSE**, with 35% believing it to be true and 28% blissfully unaware.

5 Longer passwords are always more secure

This is actually **FALSE** but 63% said it was true.

Passwords are a notoriously complex issue, with lots of different advice. Longer passwords, however, are not necessarily more secure: 0r63Ejck is more secure than password1. Unfortunately it's also a lot harder to remember.

"People should also pay attention to what information they share on social media. Information like the town you were born in, your mother's maiden name or age of your first child can be used by fraudsters. Social media can be a goldmine for anyone wanting to impersonate you or even break in when they see that you're away on holiday."

Stephen Worrall,
Managing Director,
HSB Engineering Insurance

TOP CYBERSECURITY CONCERNS AMONG CONSUMERS

74% identity theft

72% personal data being stolen

70% online fraud

70% computer/devices being infected by viruses or malware

66% loss of data, files, photos etc on computer/devices

TOP CYBER PROBLEMS IN THE LAST THREE YEARS

19% your computer/devices being infected by viruses

11% loss of data, files, photos etc on your own computer/devices

9% social media accounts being hacked/broken into

8% online fraud

"If you're transferring a significant amount of money to someone, always check the provenance of the account details you have received. Validate any account details sent to you by email by talking to the company directly (the good old fashioned telephone is much safer!), particularly if you receive emails informing you that the company's account details have changed."

James Henderson,
Managing Director Insurance UK & Ireland,
DAS UK Group

THE RESEARCH: SMEs

SMEs are as hubristic as consumers... and then some. 89% are confident when dealing with cyber security issues but an even higher proportion fail to take basic precautions such as using anti-virus software (47%) or 'strong' passwords (42%).

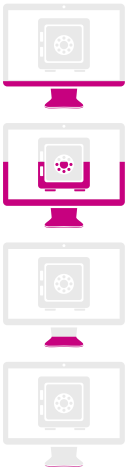
OVERALL CONFIDENCE DEALING WITH COMPUTER/ONLINE SECURITY

26% very confident

63% fairly confident

10% not very confident

1% not at all confident



THE IMPORTANCE OF CYBER INSURANCE TO THEIR BUSINESS

12% not important

18% not very important

48% quite important

18% essential

4% don't know

THE TOP FIVE PRECAUTIONS SMALL BUSINESSES HAVE IN PLACE TO PROTECT AGAINST CYBER RISKS

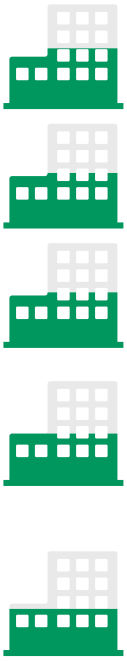
58% use 'strong' passwords

53% use anti-virus software

53% regularly back-up data

50% use different passwords on different online accounts

45% install operating system (e.g. windows, iOS, android) updates promptly when they are available



TOP CYBERSECURITY CONCERNS AMONG SMEs

62% online fraud (i.e. someone deceiving a person out of money or goods)

62% loss of data, files, photos etc being stored remotely ('in the cloud')

62% loss of data, files, photos etc on computer/devices

62% identity theft (i.e. someone using your identity or business details without permission)

61% computer/devices being infected by viruses or malware

TOP CYBER PROBLEMS IN THE LAST THREE YEARS

24% social media accounts being hacked/broken into

23% computer/devices being infected by viruses

21% online fraud (i.e. someone deceiving a person out of money or goods)

18% loss of data, files, photos etc on computer/devices

18% somebody damaging the company's reputation online e.g. spreading lies rumours or fake news about you

18% identity theft (i.e. someone using someone's identity or business details without permission)

"The National Cyber Security Centre gives advice for small businesses on protecting themselves from cyber threats. They give five areas to initially focus on:

- Backing up your data;
- Protection from malware (including using anti-virus software, installing the latest patches etc);
- Keeping smartphones and tablets safe (tracking processes in case they are lost etc);
- Using passwords to protect your data;
- Avoiding phishing attacks (educating staff on the techniques used etc)."

Stephen Worrall,
Managing Director, HSB Engineering Insurance

THE RESEARCH: BROKERS

Cyber insurance is certainly a burgeoning market with 58% of brokers expecting the cyber market to "grow a lot" in the next two years.

But whereas cyber insurance products for businesses are being sold by over two-thirds of brokers, cyber for consumers is still in its infancy and is sold by just 13% of brokers surveyed.

In terms of what insurers can do to help sell cyber insurance products then making policies simpler and explaining them more clearly was a key point, along with the provision of better training for brokers.

BROKER UNDERSTANDING OF CYBER RISKS AND CYBER INSURANCE

8% understand very well

61% understand fairly well

23% understand poorly

8% understand very poorly

HOW MUCH WILL THE CYBER INSURANCE MARKET GROW IN THE NEXT TWO YEARS?

58% grow a lot

34% grow a little

2% not grow at all

6% don't know

THEREFORE 9/10 EXPECT THE CYBER INSURANCE MARKET TO GROW IN THE NEXT TWO YEARS...

COMPARISON OF GROWING CYBER RISK TO OTHER GROWING RISKS OVER NEXT TWO YEARS FOR CONSUMERS/SMEs

14% the most important

42% among the most important

37% fairly important

2% not at all important

5% don't know

CYBER ISSUES: CONSUMERS' BIGGEST THREATS

74% identity theft

72% personal data being stolen

70% online fraud

70% computer/devices being infected by viruses or malware

66% loss of data, files, photos etc on computer/devices

MOST IMPORTANT THING INSURERS CAN DO TO HELP SELL CYBER TO SMEs/CONSUMERS

23% make policies simpler

19% better explanation of policies

15% more training for brokers

11% better advertising of cyber risks/ benefits of cyber insurance

9% provide claims examples to show customers

6% lower prices

CYBER ISSUES: BROKERS PERCEPTIONS OF CONSUMERS' BIGGEST THREATS

28% general hacking

20% online fraud (i.e. someone deceiving a person out of money or goods)

18% identity theft (i.e. someone using a person's identity without their permission)

17% phishing

12% loss of data, files, photos etc

12% specifically attacking/hacking bank account details

12% personal data being stolen

CYBER ISSUES: SMEs' BIGGEST THREATS

62% online fraud (i.e. someone deceiving a person out of money or goods)

62% loss of data, files, photos etc being stored remotely ('in the cloud')

62% loss of data, files, photos etc on computer/devices

62% identity theft (i.e. someone using your identity or business details without permission)

61% computer/devices being infected by viruses or malware

CYBER ISSUES: BROKERS PERCEPTIONS OF SMEs' BIGGEST THREATS

40% online fraud/phishing (i.e. someone deceiving a person out of money or goods)

30% hacking

28% theft of customer or business data

24% loss of data

19% ransomware/denial of service

THE CYBER THREATS OF THE FUTURE?

One of the most intriguing aspects of cyber insurance is the myriad of constantly evolving threats. Here we take a quick look at some of the emerging cyber issues.

1 Internet of Things

It's no longer just your computer, or even your phone, that connects to the internet. 'Smart' TVs are now ubiquitous, and internet-enabled home security systems, doorbells, hi-fi's, fridges, and all manner of other devices are becoming more and more common.

All of these devices need to be designed to be secure – but that is not always the case. Connected devices can be weak points in your network security. In a recent attack, criminals hacked into the thermometer in a casino's fish tank, then used it to access the casino's computers and steal its database of high rollers.

2 The cloud

In the old days, you'd probably store most of your data on your own computer, while if you had a website it was probably hosted by a specific server. Nowadays, your data is probably spread across hundreds of different computers, and your website may be hosted by an array of servers spread across different global locations.

Cloud computing offers great benefits, but comes with risks. What would you do if your iCloud data was corrupted? Do you have an offline backup? Does your business understand what data you're transferring "into the cloud" and where it's going? Are you making sure any sensitive data is encrypted?

So far, data thefts from cloud services have been a result of individual accounts being hacked. But perhaps it is only a matter of time before a provider slips up and hackers gain widespread access to Gmail, Amazon web services, Salesforce, or any one of the many major cloud computing services.

3 Computerised cars

Keyless theft is a rapidly growing threat to modern cars. In a common trick, one thief will stand near the car with a transmitter, while another prowls the perimeter of the owner's house with an amplifier. If the amplifier gets close enough to a key, it sends the signal to the transmitter, and unlocks the car.

As cars become ever more computerised, they're more at risk of hacking attacks. In a demonstration in 2015, hackers were able to turn off a jeep's engine while it was moving. With the prospect of vehicles talking with one-another as they drive, and with driverless cars in development, the battle between car manufacturers and cyber criminals has only just begun.

BIOGRAPHIES

James Henderson
Managing Director Insurance UK & Ireland, DAS UK Group

James joined DAS in 2016 from Centrica, where he was interim Managing Director for the Commercial Division of British Gas.

At DAS, James is responsible for the insurance business across the UK and Ireland.

Previous Experience:

- **October 2015 – July 2016**
  Managing Director, Commercial, British Gas (Centrica)
- **November 2014 – October 2015**
  Trading Director, British Gas (Centrica)
- **September 2009 – October 2014**
  Commercial Director, Police Mutual Insurance

Stephen Worrall
Managing Director, HSB Engineering Insurance

Stephen joined HSB Engineering Insurance in 2007 and has been in the role of Managing Director since October 2014.

Stephen is responsible for the strategic direction and full P&L for HSB's insurance business in the UK and Ireland.

Previous Experience:

- **March 2010 – October 2014**
  Finance Director, HSB Engineering Insurance
- **November 2007 – March 2010**
  Assistant Finance Director, HSB Engineering Insurance
- **September 1998 – November 2007**
  Senior Manager, PwC

FURTHER RESEARCH

The DAS Market Barometers are published on our website:
www.dasinsurance.co.uk/barometer

04.2018 | DAS 12790.01