The SME cyber insurance market: perception and adoption

The SME Cyber Insurance Market: Perception and Adoption

Cyber risk is one of the most cited and misunderstood challenges facing the global business landscape.

As businesses, ranging from global corporations to sole traders, have embraced digital platforms for commercial purposes, cyber threats have emerged as a significant threat looming over the private sector.

The realisation that cyber risks permeate all aspects of modern business has prompted owners and managers to seek new ways to mitigate their exposure to such threats, with the insurance market responding to the ever-increasing demand knocking at its door.

With high profile incidents ranging from phishing attacks on multinational corporations to ransomware viruses which have paralysed government computer systems, the business community is well aware of the stakes at play.
Any firm that stores data or conducts business digitally is a lucrative target, from healthcare and credit card companies to more traditional enterprises such as Steelite International, a Stoke-on-Trent pottery business that found itself locked out of its own files from a remote server last year.

While cyber risks are a concern, the potentially devastating impacts of such attacks make them an existential threat for small and medium-sized enterprises (SMEs).

Large corporations have plenty of advantages in the market, but none more pronounced than in cyber security.

As the scale of potential disruption from cyber threats has become apparent, procedures are now more prevalent in the workplace to ensure that 'Not Petya-style' system lockouts can't take the whole operation offline, These lockouts are where hackers freeze millions of users, both commercial and consumers, out of their computers and demand a Bitcoin ransom,
SMEs often don't have the luxury of being able to deal with these issues in-house.

While the sector makes up around 52% of UK annual turnover and employs over 16 million people, according to the National Federation of Self Employed & Small Businesses, many firms don't have the comprehensive risk analysis resources available to larger companies.

The picture is further complicated by the sheer variety of SMEs, with the term encompassing everything from the two person tech start-up to mature businesses with hundreds of staff and complex risk transfer requirements.

For these enterprises, the support of the insurance market is even more crucial to ensure that this sector is able to deal with its cyber risk profile and protect itself against the impact of debilitating attacks.

Customer awareness

While the insurance market has risen to meet the challenges customers have been facing in the digital economy, there remain significant barriers to fully ensuring that the sector is meeting the needs of all businesses.

This research conducted by Sedgwick shows that there remains a stark perception gap between SMEs and brokers when it comes to cyber risk.

The market has come a long way in promoting the benefits of cyber cover and ensuring that coverage terms are meeting the needs of customers, but this research highlights that there is still work to be done.

Key findings from the research include: - needs highlighting

- *SMEs are more concerned about cyber risks than brokers perceive.*
- *A majority of micro SME employees have no cyber awareness training.*
- *Phishing, malware and ransomware rank as the top three most prominent cyber risk concerns for SME companies.*
- *Less than 20% of SMEs have purchased cyber-specific insurance coverage.*

The research reveals that the industry is extremely in need of cyber coverage information to understand what protection that it offers and educate the SMEs on the benefits and scope of cyber protection for their specific business needs.

By working with customers to improve understanding of cyber risk, intermediaries can be at the forefront of expanding coverage from digital threats to all sectors of the economy.

Better knowledge is also crucial to understand where the main cyber exposures lie, how customers think about them, and how the industry can support SMEs to meet that demand.

That is why Sedgwick has commissioned this research into attitudes and awareness of commercial brokers and SMEs towards cyber risks.

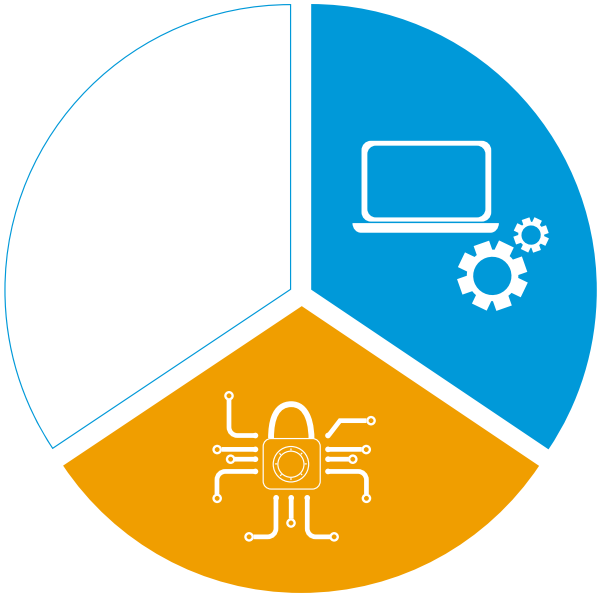
Digital enterprises

All SME businesses surveyed said that they had a digital trading or marketing aspect to their business, with over 88% using the internet for commerce 84.3% relying on digital infrastructure to power their operations.

Most businesses conduct digital activity daily, with email and Microsoft office the two most commonly used platforms.

To counter this reliance, SMEs have tapped resources for digital training or advice on how to deal with cyber threats.

Over one third of respondents said they had received advice on improving their digital capabilities, such as web site improvements or digital security, another 33% said they had received cyber security advice to support their business.

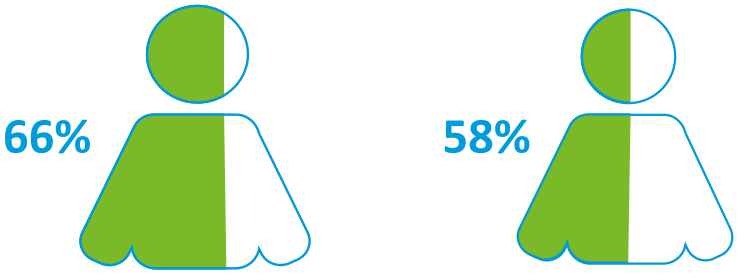


- *33% received advice on improving their digital capabilities (web site improvements or digital security)*
- *33% received cyber security advice to support their business.*

Perception gaps

The research found that SMEs claim to be fairly knowledgeable over cyber security system risks and the integral role that digital technology plays in the daily running of their business.

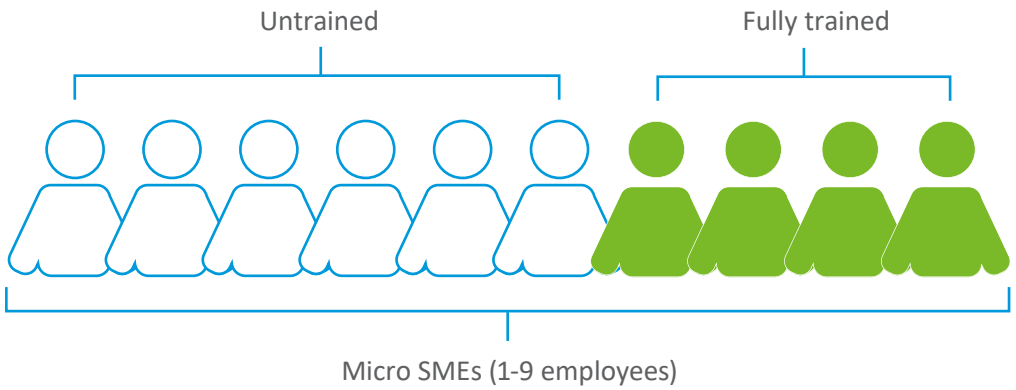
Over two-thirds of respondents claimed to have received some form of digital advice and/or training to deal with cyber threats, 58% aware of the importance of data encryption and cyber-crime rated as a higher risk concern than Brexit.



Received digital advice

Aware of data encryption and cyber crime

However, for the smallest enterprises in the cohort the picture was notably different. For micro SMEs, companies with between 1 and 9 employees, 6 in 10 had received no cyber security training of any sort.



Cyber awareness and training received increased in line with the size of the company, with largest SMEs having the greatest stated awareness of cyber risks.

Brokers on the other hand are aware of the growing importance of the issue and the opportunity that it provides.

Of the intermediaries surveyed, just under half placed cyber-specific risk either as a stand-alone policy or additional offering.

On top of that, 9 out of 10 respondents from national brokers pointed to the impact of so-called 'phishing' attacks where attackers target employees as the main reason that SMEs approach the market to purchase cyber cover.

While brokers seem to be sticking with markets that reflect their own size-30% of national broker cyber risk gross written premium (GWP) is placed in larger SMEs of 50-250 employees, dropping to 21% for provincial brokers' books- overall brokers surveyed believe that nearly half (47%) of SMEs would have concerns over cyber and data risks.

However, the research shows that SMEs and brokers are not aligned when it comes to perceptions of where the major risks lie and how they can be tackled.

Headline risks

Despite the perceived importance of cyber risk to SME customers, brokers questioned revealed that cyber insurance makes up only around 5% of their current book despite the high priority

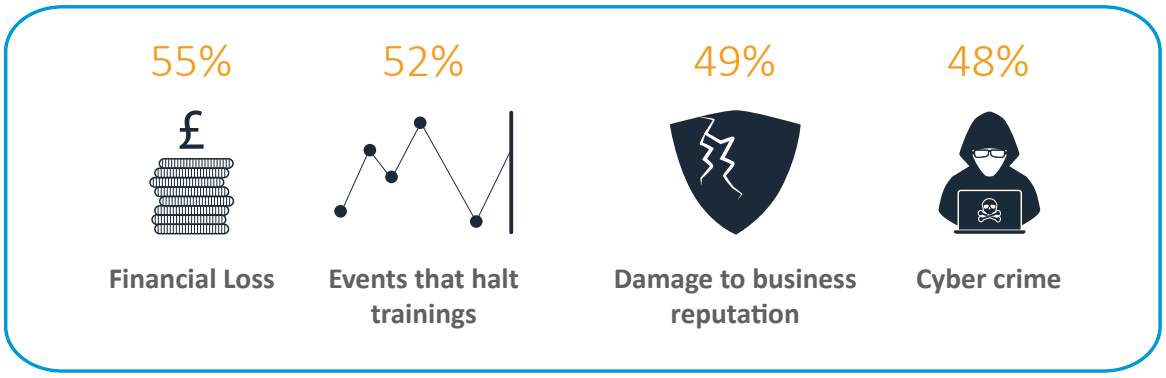
placed on such risks by customers, underscoring the gaps of understanding between the market and its customer base.

Much of the confusion comes down to the gap between brokers' understanding of how SMEs weigh up cyber risks and the harm it can do to their business.

Incorrectly, brokers believed that nearly one third of SMEs surveyed, around 31%, have suffered a data breach in their trading history. However, in fact just 14% of SMEs said they had ever suffered a security breach of any sort. Of those that had been the victim of an incursion, two-thirds claimed to have cyber security coverage or cyber liability insurance in place before they had a cyber breach.

For those that had purchased coverage prior to an incident, 63% were expecting reimbursement from any financial loss stemming from the attack, which aligns with SMEs claim that financial loss, events that stop you trading, damage to business reputation and cyber-crime are the top three business risks facing the sector.

SMEs Top Business Risks



Broker perceptions

Cyber has risen to the top of the risk agenda over the past few years as the devastating impact of attacks has become more widely known to the business world.

Attacks ranging from WannaCry to Not Petya have crippled entire computer networks across large swathes of the private and public sectors, prompting a jump in awareness around the specific types of threats facing today's commercial environment.

Such incidents have enlarged the pool of people aware of the impact that such attacks can have and pushed techniques such as phishing or ransomware to the forefront of the public consciousness.

Brokers surveyed similarly claimed that such types of threats were the main reason why SMEs decided to purchase cyber insurance.

Around three-quarters of intermediaries responded that phishing, malware and ransomware attacks were the main factors behind an SME deciding to purchase cyber insurance, with distributed denial of service (DDos) attacks (61%) and the impact of insider hacking on the business (41%) perceived as the other key drivers.

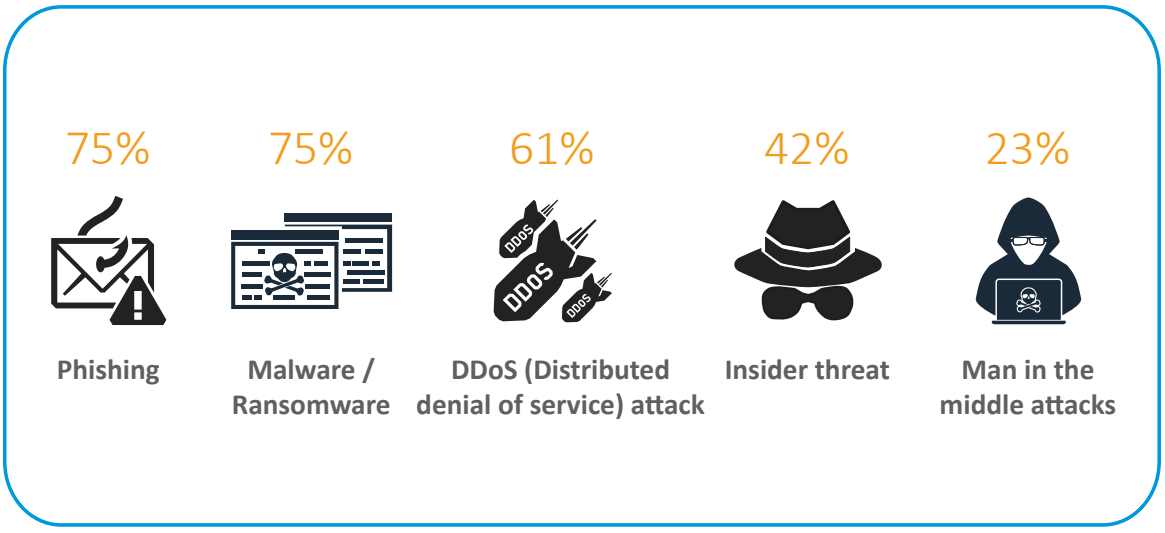
Mirroring this phenomenon, brokers gave SMEs an average qualitative rating of 7 out of 10 for their awareness of the threat posed by the three main threats listed, but perceived that over half of SMEs have no awareness at all of 'Man in the Middle' attacks.

However, brokers appear to not distinguish between different business profile/composition of the SME cyber risk market.

Around 15% of respondents claimed they did not think there are any differences between tech and non-tech SMEs, with just 1 in 10 believing that enterprises involved in the tech industry will be more aware of cyber specific issues than other firms engaged in sectors such as manufacturing or retail.

Moreover, while only 47% of brokers believed that SMEs are worried about cyber and data misuse, 91% of SMEs surveyed indicated concerns over cyber risk, underscoring the gap in perception that still remains between the insurance market and the customer base.

The perceived cyber risks (from our research)



Types of Cyber Attack

- **Phishing** is a method of gaining personal information by way of deceptive emails.
- **Distributed Denial of Service**, or DDoS, attacks occur when hackers overwhelm a web server with malicious traffic.
- **Man In The Middle Attacks** In order to view content online, web browsers must send information back and forth with web servers. When this information is left unprotected, it can be stolen and manipulated by unauthorised third parties.
- **Malware** is any kind of malicious software that can infect a computer or network. There are many common types of malware — viruses, Trojans, worms, keyloggers, and spyware.
- **Ransomware** is sophisticated malware that can prevent you — or your employees — from accessing computers and systems. Hackers ask for exorbitant ransom in exchange for giving you access to your property and your data.
- **Insider Hacking**, employees, contractors, and even clients likely have access to some parts of your network and databases. They can leverage their existing access to look for vulnerabilities.

Insurance buying

Despite cybercrime being listed as one of the top concerns on the mind of SMEs, only around 15% stated that they had purchased specific cyber cover.

Moreover, under half claim to have some form of public liability, employers' liability or property insurance, while over 56% of respondents said they had a bundled insurance policy.

This drops to under half for micro SMEs with between 1 and 9 employees, but at larger companies of between 50 and 250 employees this figure rises to more than two-thirds which have cyber insurance bundled in as part of broader coverage options.

While there are gaps in the perceptions of brokers and SMEs when it comes to why customers are buying insurance, both parties agree that cost remains a significant barrier to securing further market penetration.

Nearly 70% of brokers surveyed cited the cost of cyber insurance as the main barrier to insurance take up in the sector, similar to the 63.6% of micro SMEs that also cited cost as the primary obstacle to securing more coverage.

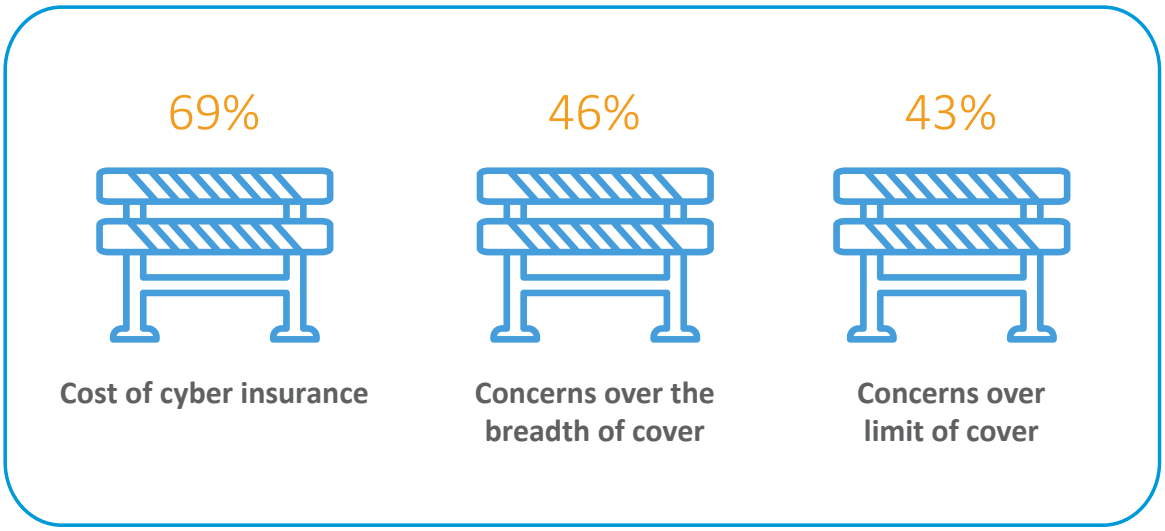
However, the survey also revealed stark differences in broker attitudes towards cyber risks in SME companies that had suffered a breach which had impacted their business and those that had escaped any serious attacks.

While of the businesses surveyed, three quarters of which used internet security systems such as Norton or AVG, just 14% had experienced any sort of security breach, while six out of 10 said that the attack had spread across their business networks.

Of the SMEs that had not been subject to a serious breach, 85.1% of brokers ranked the low importance of cyber to their business as the reason for not purchasing insurance, 24% who had clients that had suffered an attack said cost was the major barrier to securing better coverage.

Notably, 75% of SME respondents said that they had purchased their cyber insurance cover over the internet, and11% securing policy terms through a specific cyber advisory portal online that helps businesses identify their exposures.

Key barriers for cyber insurance take up for SMEs



Cyber Insurance Terminology

- **Cyber security coverage:** Also known as Privacy Notification and Crisis Management Expense Insurance. This coverage includes coverage for first party damage to you and your business. This coverage does not protect your business from damage done to third parties.
- **Cyber liability insurance cover:** Also termed Information Security and Privacy Insurance, covers the insured's liability for damages resulting from a data breach.
- **Technology Errors and Omissions Insurance:** Also referred to as Professional Liability or E&O, is a form of liability coverage that protects businesses who provide or sell technology services and products. This coverage prevents businesses from bearing the full cost of defending against a negligence claim made by a client, and damages awarded in a civil lawsuit.

Conclusion

Key findings

This report shows that substantial gaps remain between brokers' perception of the cyber threat facing SME businesses and the work that needs to be done to address customer concerns.

While brokers have developed products to meet the growing cyber demand, it is clear that the sector can do more to work with clients to educate them on the risks facing their business and build an insurance market which meets their needs.

Brokers have the opportunity to bridge the perception gap by providing training and support for SMEs, but the market must be ready to ensure that the policies on offer are consistent with the risk transfer needs of customers and priced at a level which encourages, rather than dissuades coverage buying.

The research

The Sedgwick brokers and SMEs cyber research surveyed a representative sample of brokers and SMEs in the UK. 250 provincial, super regional and national brokers were surveyed, while 350 SMEs with up to 250 employees also responded to the survey.