SMEs and cyber risk – a ticking time bomb

SMEs are a prime target for cyber criminals because they are believed to have limited resources and employ less technically aware employees than larger enterprises. Despite this, these businesses, their insurance providers and brokers are not assessing their propensity to cyber risk – although tools are available

By Sara Costantini
Managing director,
Crif Decision Solutions

The recent *SME Insurance Risk Survey* commissioned by Crif Decision Solutions in partnership with *Post* has revealed some surprising findings.

It would appear that many insurance providers and brokers are not equipped to accurately assess and subsequently price small to medium-sized enterprise cyber risk. 40% of respondents were currently using nothing to accurately assess SME's vulnerabilities to a cyber-attack. Of the remaining 60%, worryingly, there was a significant amount of confusion about what constituted a cyber risk assessment tool with some respondents citing newspaper reports, questionnaires, marketing materials and discussions with the client as their means of understanding the risk, prior to placing or pricing a policy.

Cyber exposure

This approach clearly leaves insurance providers commercially exposed when underwriting SME cyber insurance policies with the significant potential to negatively impact loss ratios in the event of claims. In tandem, broker reputation related to the placement of SME cyber insurance could equally be threatened should a book of business result in costly claims.

In parallel the survey findings point to SMEs underestimating their cyber risk exposure and holding the belief that attempting to assess the risk would be both costly and invasive. 90% of respondents said that in terms of their overall propensity to be a victim of a cyber-attack and its consequences, SMEs were either totally unprepared or only slightly prepared.

The question that has to spring to mind related to both sets of findings is: Why?

At the time of writing the UK's data privacy regulator has said it plans to fine the US hotel group Marriott International £99.2m. The penalty relates to a data breach that saw the personal details of approximately 339 million guests compromised. This announcement was hot on the heels of the Information Commissioner's Office confirming that British Airways was to be fined £183m over a data breach. Unsurprisingly it is these high profile cyber-attacks which make news headlines and potentially lull SMEs into a false sense of security and associated apathy related to their own risk.

But, in terms of penalties, SMEs can expect the ICO to react with rigour if they cannot demonstrate sufficient control and protection over the data they own - especially in the event of a breach. In addition to fines for lack of compliance, the risks of not adequately protecting data held by the business from cyber criminals are multiple, including exposure to socially engineered attacks and ransomware. These risks can lead to loss of customers and revenue, cause reputation damage and,

> 26

Figure one: What are the biggest concerns among SMEs that might encourage them to be more interested in cyber if better communicated/marketed?

Rank	Option
1	Losing money
2	Brand reputation
3	Data breaches
4	Personal liability and penalties
5	Losing business opportunities
6	New laws and directives
7	Losing competitive advantage

Respondents were asked to rank up to five of the options provided in order of significance

< 25

ultimately, can fundamentally threaten the stability of the business.

Vigiliance is critical

Combined with the backdrop of the *General Data Protection Regulation* environment, the cyber landscape is also rapidly evolving with cyber criminals becoming ever more sophisticated in identifying new ways of penetrating IT infrastructures. Vigilance is critical and this can seem particularly daunting to SMEs that typically do not have large IT departments and budgets. It is for this very reason that SMEs are a prime target for the highly organised criminal gangs operating in the field, as they are seen to be resource limited with less technically aware employees than larger enterprises.

According to the National Cyber Security Centre, SMEs face a one in two chance of experiencing a security breach and statistics from the Government's *2018 Cyber Security Breaches Survey* reveal that 43% of SMEs in the UK have experienced a cyber breach.

Over 64% of the *Post* survey respondents confirmed that the SME market continues to offer their business plenty of opportunity (*see page 22, figure three*). The cross selling of cyber insurance was recognised by respondents as the fifth biggest opportunity in SME insurance, preceded not by lines of business but by operational advantages like efficient use of data, adoption of new technologies and boosting offerings with additional services like risk management tools. In order to reap the benefits of this revenue stream and the associated opportunities to differentiate an insurance provider or broker, education is key. Awareness must be raised with SMEs of the scale of the risk they face from cybercrime and the potentially devastating impact a cyber-attack could have on their businesses. Loss of money, brand reputation and data breaches were cited in the survey as the top three concerns for SMEs which may be used to help to increase appetite for cyber insurance *(See figure one)*.

Integration of risk assessment tools

And what of managing the risk to SME cyber insurance providers and brokers placing the business? The integration of risk assessment tools and services was cited by over 67% as the top means of improving the SME user journey. So there would appear to be an opportunity to enhance the customer experience and protect insurance provider loss ratios and broker reputations. Cyber risk assessment tools, integrated into the sales and underwriting process would afford the insurance provider or their broker the insight to accurately understand the risk being placed and subsequently price accordingly. Alternatively there is the option to direct the SME to a preferred cyber risk assessment tool in order to perform a self-assessment and provide the report during the sales cycle – although this could significantly detract from the customer journey and erode any sense of added value.

The insurance providers and brokers surveyed did not see price as a significant barrier to cyber insurance penetration, ranking it fourth behind: the belief that cyber-attacks only impact large businesses; cyber insurance not being considered a business priority; and poor communication about the benefits of cyber insurance *(See figure two)*.

Set within this context, the cost of an insurance provider using a cyber risk assessment tool or encouraging its brokers to do so, could potentially be offset by the cyber policy pricing. The added value to the SME customer is considerable, arming them with an understanding of their cyber vulnerabilities and presenting the opportunity to address them.

In adopting an integrated cyber risk assessment approach, it will be necessary to address SME concerns about costly consultants, invasive risk management exercises and commercial sensitivities, while reinforcing the scale and impact of the risk and the benefits of cyber insurance. There are tools available on the market which are economically viable and can rapidly identify cyber risk vulnerabilities. Some of these tools offer immediate screening and instantly provide a report detailing the company's cyber risk exposure. IT expertise should not be necessary and the service should be quick and easy-to-use. In some cases only the company domain name and responses to a short set of questions are required in order to perform the cyber risk screening – offering a non-invasive solution. The resulting report should be written in simple business language and delivered in real time ideally using the universal traffic light system, 'red, amber, green', to demonstrate risk severity. Risk exposure and severity can be made immediately clear, informing the insurance provider or broker wthat can share the findings with the SME.

The insurance provider and broker that offers such cyber risk screening has the opportunity to create real competitive advantage, grow market share and build a book of profitable business from customers who have received added value. The only question remaining is who will seize the opportunity first? ■

Figure two: Why do you think penetration of cyber insurance among SMEs is so low?

Rank	Option
1	View among SMEs that cyber-attacks only impact large businesses
2	Not considered a business priority
3	Poor communication about benefits
4	Price
5	Belief cyber products will not pay out in the event of a claim
6=	Belief that it involves invasive risk management exercises/asks clients to reveal too much sensitive information
6=	Words are too confusing/full of jargon
7	Lack of marketing
8	Excessive consultancy costs

Respondents were asked to rank up to five of the options provided in order of significance