SMBs lack the necessary resources to craft and sustain strong protection against cyber threats

April 2020

Eileen Zimbler

Small and medium-sized businesses (SMBs) generally feel vulnerable to external data threats. Analysys Mason's 2019 survey of around 3000 SMBs worldwide revealed that 32% of small businesses (0–99 employees) and 57% of medium-sized businesses (100–999 employees) experienced a breach[1] in the last 12 months. A shortage of cyber-security skills is central to this problem. Only about 6% of SMBs in the high-income countries surveyed[2] have internal cyber-security staff and, as a result, businesses struggle to understand their security needs and the products that can help them. The lack of both internal and external cyber-security skills is exacerbated by budgetary constraints in all countries.

SMBs are feeling the consequences of the lack of in-house cyber-security specialists. All businesses know that they need some type of protection against cyber threats, but many smaller businesses are not aware of the range of threats that they face and the solutions that they could employ. Others have appropriate security solutions in place, but do not adequately maintain and manage them. Some SMBs in our survey expressed plans to hire more security staff, but they will still need more support.

The disconnect between SMBs' cyber-security needs and their lack of IT specialists is hampering their ability to achieve their security goals. This makes them good targets for security solution providers with attractive service/support offerings. Security vendors and service providers need to consider how they can help SMBs to overcome this lack of internal expertise. They should reinforce messages about the risks of weak security, provide cost-effective ways for helping SMBs to manage these risks (for example, by offering fixed-price vulnerability assessments) and devise alternative pricing models for this market.

SMBs' lack of cyber-security knowledge is hindering the effective development of their cyber-security capabilities

The SMBs in our survey reported many challenges when it comes to crafting and maintaining strong security for their data assets and IT infrastructure, but the overriding issue is a fundamental lack of specialised cyber-security knowledge. The majority of SMBs do not have adequate in-house or external support for the cyber-security solutions that they currently have installed, and they often do not understand what is missing from their existing security strategies. Many businesses (particularly smaller ones) do not regularly update their security solutions. Many medium-sized businesses have relatively complex IT infrastructure, and the security solutions that they have deployed for protecting their data assets are inadequate.

A significant proportion of the businesses surveyed (around one in five) expressed concerns about their lack of awareness of security vendors and the different solutions that they offer. A similar proportion of businesses said

1 A breach is defined as data theft or loss (caused by both internal and external actors) or an attack from an external party (including unauthorised access and hacking; examples include malware, ransomware, phishing and DoS attacks).

2 High-income countries surveyed: Australia, France, Germany, Saudi Arabia, UK and USA. Middle-income countries surveyed: China, India, Indonesia and South Africa.

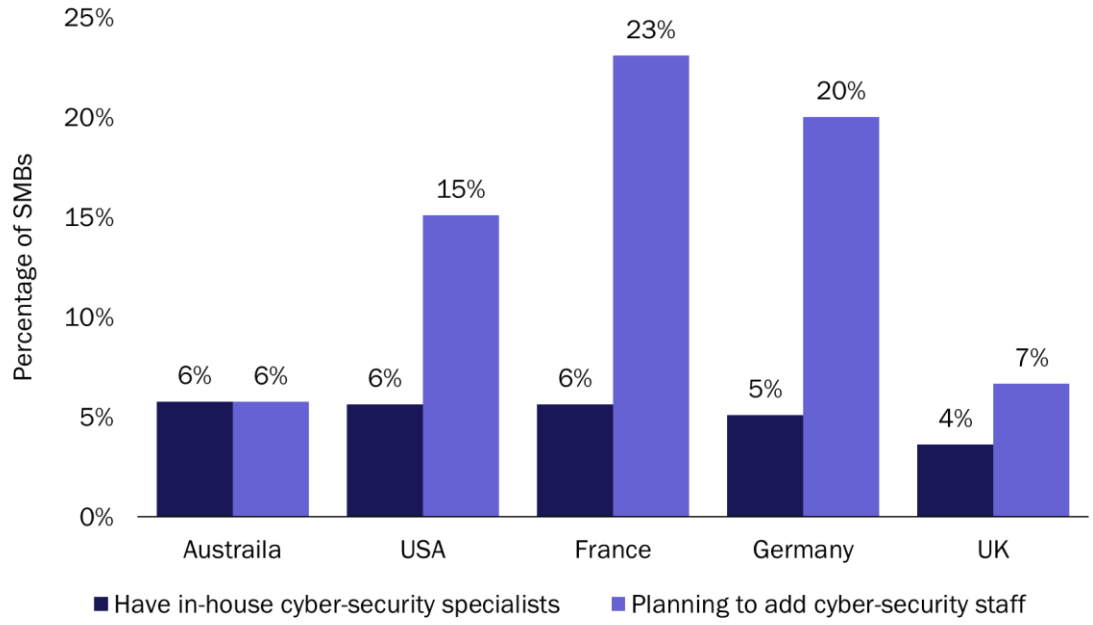
that they struggled to decipher which solutions they really need (they cited "vendor solutions being too complex and time-consuming to implement" as a challenge).

Almost 30% of the SMBs that we surveyed said that outsourcing IT management to external IT managed service providers (MSPs) is critical to their business growth. This reasonably low figure indicates that SMBs would prefer to manage their IT in-house, but actually, this is unrealistic for many. There is therefore a large gap in the cyber-security market that could be filled by vendors that offer education and a targeted range of cost-effective support options for such organisations.

Not many SMBs in high-income countries plan to hire cyber-security staff

Only 10% of the SMBs surveyed worldwide had in-house IT staff dedicated to cyber security. Furthermore, businesses in high-income countries tended to have even lower incidences of in-house cyber-security specialists than those in middle-income countries. Businesses in high-income countries were also relatively less inclined to hire such individuals in the future (Figure 1).

Figure 1: SMBs that have in-house cyber-security specialists and those that are planning to add such specialists, high-income countries, 2019



Source: Analysys Mason, 2020

SMBs in high-income countries are less likely to have IT staff that specialise in security than those in middle-income countries because of the much higher costs associated with maintaining full-time IT positions. Less than 15% of SMBs in high-income countries reported having plans to hire cyber-security specialists in the next 12 months.

Half of all SMBs surveyed reported plans to hire full-time IT staff, and 28% reported plans to try to add specialists in cyber security, but we suspect that the actual number of staff hired will be much lower given the salaries demanded by security staff. Some SMBs are looking at outsourcing options, but a portion of businesses

appear to be somewhat less open to offloading the entirety of their cyber-security management to outside providers: 29% of SMBs have plans to outsource IT management to external IT MSPs, while 11% of small businesses and 20% of medium-sized businesses feel that external IT security consultancies/service providers are often unable to provide optimal security solutions.

What this means for cyber-security vendors, service providers and their partners

Offering security assessments and support for SMBs' existing security infrastructure, rather than trying to sell them additional solutions, should enable vendors and their channel partners, telecoms operators and MSPs to more easily secure accounts with SMBs. Almost one fifth of SMBs cited a lack of guidance and "how to" security playbooks as one of their key cyber-security challenges, meaning that providers that can augment and improve SMBs' existing cyber-security capabilities will have an easier time gaining their trust and building relationships.

Both small and medium-sized businesses are reporting cyber-security deficiencies, but solutions tailored to specifically to each business size segment will resonate better. For example, medium-sized businesses state that their top cyber-security challenges are "compliance regulations change too quickly to stay current" and "security needs vary too much across stakeholders/departments, increasing costs and delays". As such, vendor and service provider offerings that focus on managing cyber-security regulations and compliance, and provide security management for larger and more diverse organisations will resonate well with medium-sized businesses in all countries. Security providers that focus on education and relationship-building, as well as product recommendations, deployment assistance and employee training/support, will fare best among smaller businesses, as will security solutions that are simple to understand. Both small and medium-sized businesses want painless implementation that comes with defined onboarding plans and plenty of handholding.