SMEs' lack of cyber-security expertise gives providers and operators a strong opportunity to upsell services

April 2022

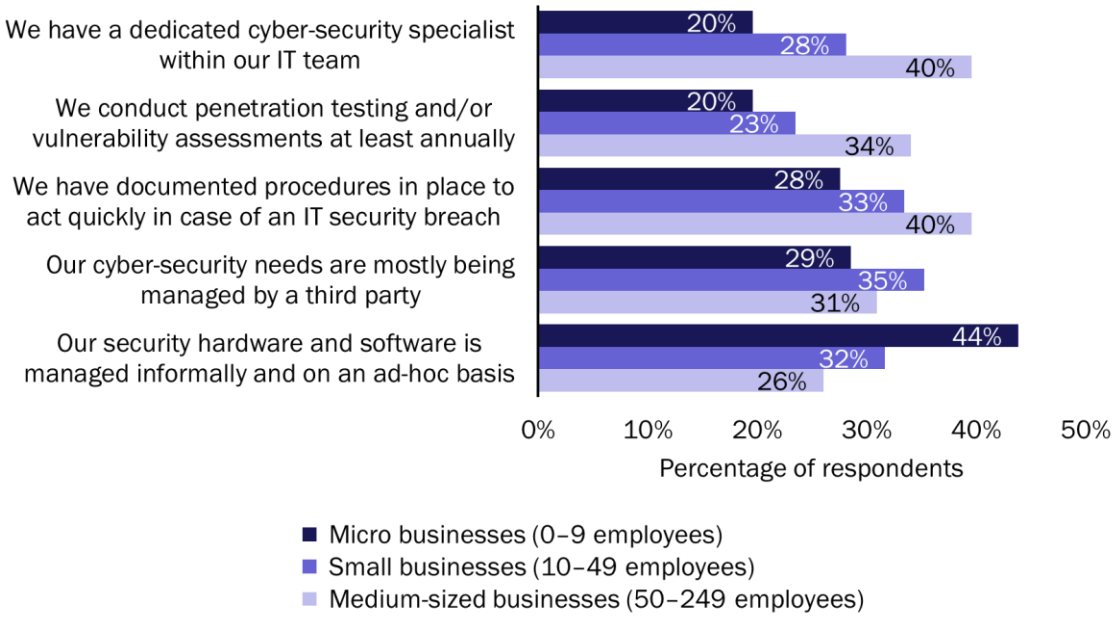
Eileen Zimbler

Most small and medium-sized enterprises (SMEs) are concerned about cyber security, but not actively taking adequate steps to protect themselves from cyber threats. We conducted a survey of 870 SMEs in Germany, Singapore, the UK and the USA between December 2021 and January 2022 and asked respondents about their cyber-security strategies. Businesses' approaches to securing their data vary by the number of employees; medium-sized businesses (50–249 employees) are generally the most likely to have established a variety of cyber-security measures, while micro businesses (0–9 employees) are most likely to manage their security on an ad-hoc basis. Most SMEs purchase their security solutions with other services, such as connectivity or IT services. This gives providers and operators a strong opportunity to upsell security offerings to customers that take other solutions and services.

SMEs lack expert cyber-security support and will look to third parties to provide it

Most SMEs do not have dedicated cyber-security specialists as part of their in-house IT teams and are not taking adequate steps to ensure the security of their data networks. Nonetheless, about a third of SMEs are using third parties to manage their security (Figure 1).

Figure 1: SMEs' methods for managing their data security, Germany, Singapore, UK and USA, 1Q 2022[1]



Source: Analysys Mason, 2022

Micro businesses tend to have the lowest levels of cyber protection. 80% of the micro businesses that we surveyed said that they do not have an in-house security expert, but we believe that the true figure is even higher (perhaps as high as 95%).

Most of these smaller firms are also not managing their security protocols adequately. For example, 80% of respondents in the micro segment reported that they do not conduct security testing/assessments and 72% reported not having documented procedures in place to handle security breaches. 44% of micro businesses also admitted to managing their data security on an ad-hoc basis; again, the true figure is probably higher.

As businesses increase in size, their approach to security tends to become more formalised. Small businesses (10–49 employees) are more likely to have security measures in place than micro businesses, and only a third of them take an informal approach to cyber-security management. Medium-sized businesses are the most likely to have on-staff cyber-security experts (40% of respondents), but many of them are still not conducting regular security tests. Indeed, only 34% of medium-sized respondents conduct regular penetration tests and vulnerability assessments. Furthermore, only 40% have standardised procedures to handle breaches.

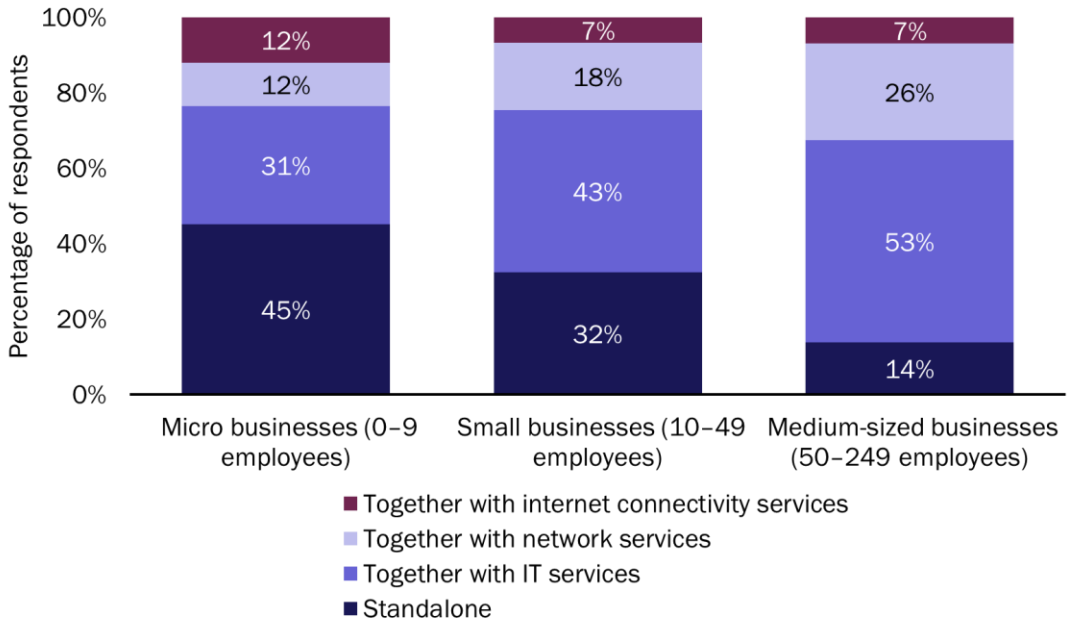
There is strong opportunity for solutions providers and telecoms operators to provide SMEs with security solutions. Indeed, many SMEs are already using such third parties for this purpose. For example, 35% and 31% of respondents with 10–49 employees and 50 or more employees, respectively, reported employing third parties to manage their data security. Bundling security solutions with other services can be a convenient route for upselling.

1 Question: "Which of the following statements apply to your organisation?"; *n* = 870.

SMEs prefer to purchase cyber-security solutions with other services rather than buying standalone products

60% of respondents prefer to purchase their cyber-security solutions in conjunction with other services, and this tendency increases with the size of the company. Indeed, 45% of micro businesses reported a preference for purchasing standalone security solutions, compared to only 14% of medium-sized businesses (Figure 2). This highlights a key opportunity for security providers.

Figure 2: SMEs' preferred methods of purchasing cyber-security solutions/services, Germany, Singapore, UK and USA, 1Q 2022[2]



Source: Analysys Mason, 2022

Medium-sized businesses are not only the most likely to purchase security as part of a bundle; they are also the most likely to have in-house security experts. Cyber-security professionals often purchase security as part of another solution. For example, purchasing network security from the WAN solution provider tends to be the easiest option and results in one point of contact and one point of responsibility for all aspects of a particular service.

SMEs' appetite for managed security solutions is strong. Indeed, 26% of SMEs reported currently subscribing to managed security services via a monthly or annual contract, and a further 32% are interested in doing so. There is therefore a clear opportunity for managed service providers (MSPs) to bundle cyber-security services with other managed services, especially for medium-sized customers (53% of medium-sized respondents reported having a preference for taking security bundled with IT services). A total of around 25% of respondents reported having a preference for purchasing security solutions that are bundled with their IT internet or network services, thereby providing an excellent opportunity for telecoms providers.

2 Question: "What is your organisation's preferred way of purchasing cyber security solutions/services?"; *n* = 870.

SMEs are open to using third parties for data security management, thereby representing a significant opportunity for cyber-security providers

SMEs are open to using third parties for data security management. Some are happy to use third parties for all of their data security management needs, while others may only want selected pieces of their cyber-security infrastructure to be managed. 73% of respondents said that they are looking for partners that can upgrade their security to cover new problems such as remote working, collaboration and bring your own device (BYOD) policies.

Nonetheless, service providers and operators have some hurdles to overcome in order to win SMEs' business. We asked respondents what the key challenges are to having highly effective cyber-security capabilities; the top responses were:

- limited IT security budgets (29% of respondents)
- lack of specialist security staff (23%)
- cyber-security solutions are too complex and time-consuming to implement (23%)
- external IT security consultancies/service providers are often unable to provide optimal solutions (23%).

These challenges suggest that MSPs, managed security service providers, value-added resellers, telecoms operators and other security solutions providers need to address SMEs' underlying concerns and educate them on which cyber-security solutions will best suit their needs.

Offering security solutions that are bundled with other managed IT services or connectivity services (such as managed networking, fixed broadband and SD-WAN) could enable MSPs, telecoms operators and other providers to win a greater share of SMEs' security spend.