Business survey 2019: almost 25% of small businesses feel that their cyber-security protection is inadequate

September 2019

Igor Babić and Tom Rebbeck

The cyber-security market for micro, small and medium-sized businesses (SMBs) is large, and rapidly growing. Analysys Mason estimates that enterprises with fewer than 1000 employees will spend around USD50 billion on security solutions in 2019 and that this will grow at an average rate of 13% between 2019 and 2024.

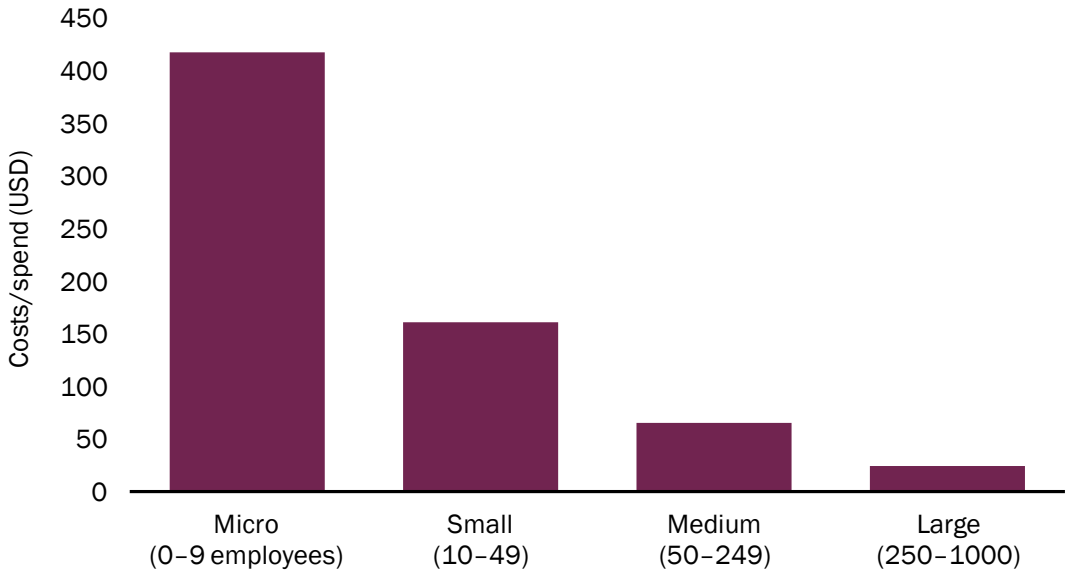
However, the market may not achieve this growth unless security vendors do a better job of servicing it. Vendors that want to succeed in the SMB market need to do more to explain the security risks that small companies face and increase awareness of products that can help these companies mitigate such risks.

Our recent survey of around 3000 businesses worldwide shows that the smaller a business, the larger the relative impact of a cyber-attack. Despite this, small companies are not well served by security vendors.

Cyber attacks have a relatively larger impact on smaller businesses

High-profile cyber attacks on large businesses such as British Airways or Equifax may make headlines, but rarely have severe long-term consequences for the business. In contrast, a cyber attack can threaten the existence of a small business. According to our survey, the average cost per employee of all attacks in the past 12 months was over USD400 for a micro business, compared to costs of USD25 for a large business (see Figure 1). (All data is self-reported and should be treated with caution.)

Figure 1: Estimated cost of security-related incidents experienced in the last 12 months, by business size, per employee[1]



Source: Analysys Mason

Security incidents are also relatively common for smaller companies. In our survey, 32% of micro businesses and 39% of small businesses reported that they have experienced a security-related incident in the last 12 months. These figures are lower than for larger companies (61% of large companies had some sort of incident in the last 12 months), but given that larger companies have more of everything (people, PCs, servers etc.), this difference is unsurprising. Again, if we compare the data on a per employee basis, smaller companies are more vulnerable than larger ones.

This vulnerability is reflected in how smaller companies feel about their level of protection. Only 77% of micro businesses said that they felt fairly or extremely well-protected against cyber-security attacks and threats from external parties (compared to 90% for large businesses). The remaining 23% of micro businesses felt either somewhat or not satisfactorily protected, compared with just 10% of large businesses.

Security vendors are not serving smaller businesses well

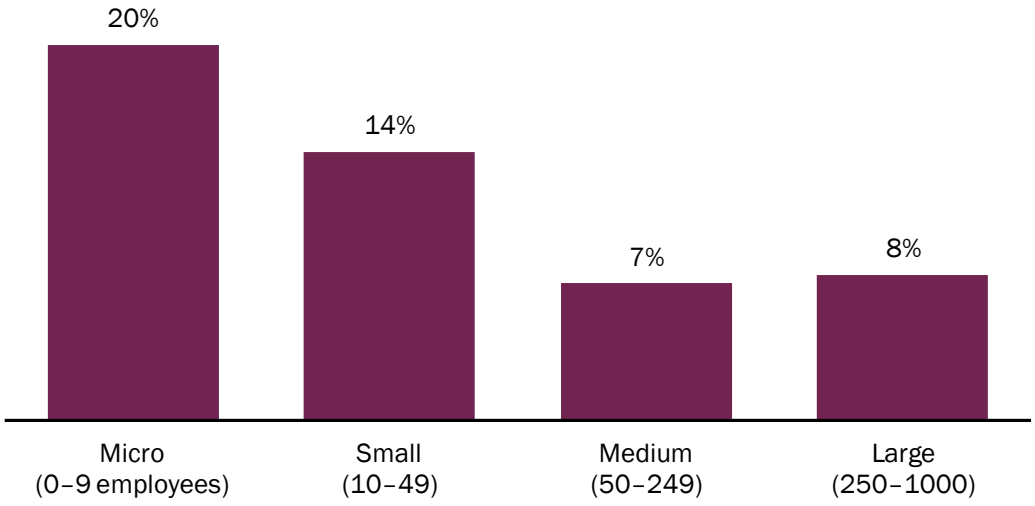
Few micro or small businesses have dedicated security personnel. Security is often the responsibility of an office manager, or even of the company owner. This makes it more difficult for security vendors to target the right person than when targeting larger organisations. However, this should not be mistaken for a lack of interest in security; our survey shows that the security priorities of smaller businesses (for example, protecting customers' data, ensuring business continuity) are almost identical to those of larger organisations.

The lack of specialist security staff and limited budgets are considered to be barriers to the development of security capabilities by surveyed businesses of all sizes. However, smaller businesses were more likely than larger ones to cite the lack of awareness of new security vendors and their products as a challenge (see

1 Questions: *"Has your company experienced any of the following IT security-related events in the last 12 months?"*and to companies that suffered a security-related incident *"How much would you estimate that the incident(s) cost your company (including direct losses as well as costs incurred to recover from the breach(es) and restore the lost information, legal costs to your business, and costs of repairing your business' reputation)?". n = 2983.*

Figure 2). Large and medium-sized businesses identified the lack of awareness of new security vendors and their solutions as the least of their challenges out a list of 12 options.

Figure 2: Percentage of businesses that cited the lack of awareness of security vendors and their products as a challenge[2]



Source: Analysys Mason

Vendors should see this large, growing and underserved market as an opportunity

Vendors might regard smaller businesses as unattractive business propositions for many reasons: spend per company will be low relative to larger organisations; prospects can be hard to find and expensive to serve; price may be more important than technical capabilities in decision making, as may ease of use.

For vendors that are willing to tackle this market though, these negatives create an opportunity. As our survey reveals, even the smallest enterprises have expressed interest and increasing awareness of the need to improve security. A security breach is likely to cost at least a few thousand dollars, and for a small business with tight cash flows, that amount could represent the difference between surviving or not. Despite this (or perhaps because of it), smaller enterprises are less likely to feel well-protected than their larger counterparts.

Vendors that want to sell to micro and small businesses need to:

- highlight the impact of a security breach
- show how their products can help to mitigate the risks
- make it easy for businesses to adopt their services.

Vendors should experiment with self-serve options, freemium models and free trials that can be used to demonstrate the threats that businesses are facing.

2 Question: "Which of the following are challenges to your company having a highly effective cyber-security capability?". *n* = 2983.