

# Business survey 2019: cyber-security vendors need to change their approach to win in middle-income markets

September 2019

Igor Babić

Analysys Mason's recent survey of almost 3000 small and medium-sized businesses (that is, companies with fewer than 1000 employees) worldwide shows that businesses in middle- and high-income countries have similar cyber-security requirements, and share similar views on the threat landscape.<sup>1</sup>

Despite this, the challenges that these businesses face in developing their security capabilities vary considerably. Vendors that want to grow in middle-income markets (such as India and Indonesia) need to understand that the prices and complexity of their standard solutions are significant barriers to adoption. They should address this problem by adapting their offerings.

## Businesses in middle- and high-income countries have similar views on what will affect their cyber-security plans

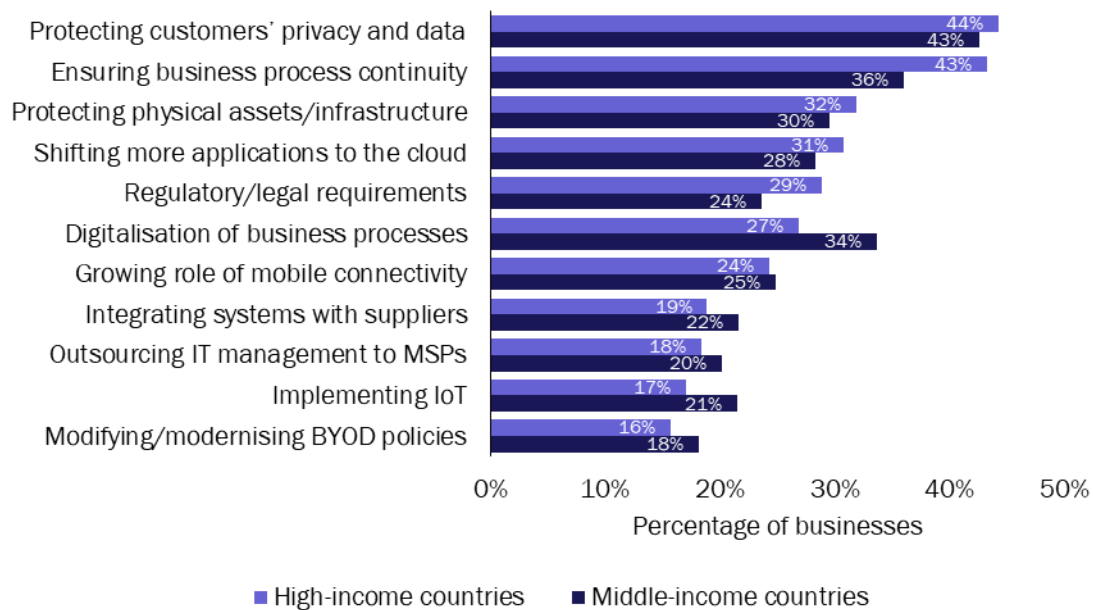
Businesses in both high- and middle-income countries perceive the need to protect their customers' privacy and data as the main factor that will have an impact on their security plans in the next 12–18 months. This comes as no surprise; 32% of businesses in middle-income countries and 22% of those in high-income countries experienced a security incident involving theft of data during the last 12 months, according to our survey.

Businesses in these two country groups share similar views regarding the factors that will affect their short-term cyber-security plans (see Figure 1).

---

<sup>1</sup> Middle-income countries: those with a gross national income (GNI) per capita of between USD1026 and USD12 375. High-income countries: those with a GNI per capita of above USD12 375.

**Figure 1: Factors that will affect businesses' short-term cyber-security plans, averages for high- and middle-income countries<sup>2,3</sup>**



## The security-related challenges that businesses in middle- and high-income countries face are markedly different

Our survey also asked about the barriers that businesses face in developing their cyber-security capabilities. The results were starkly different by country income level (see Figure 2).

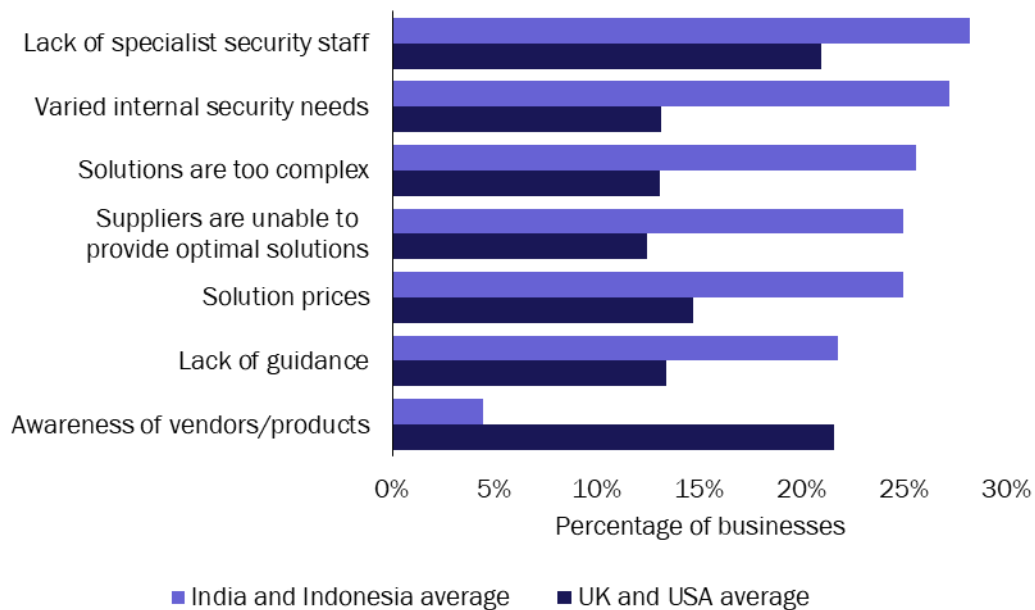
A lack of awareness of vendors and the products available in the market is the biggest problem for businesses in the UK and the USA. In all of the middle-income countries surveyed, this is the least significant barrier for the adoption of security solutions. In these countries, factors under vendors' control – such as solution pricing, solution complexity, the guidance provided and vendors' ability to provide optimal solutions – are all perceived to be more important barriers.

A lack of specialist security staff is a problem for businesses in both middle- and high-income countries; but again, a higher proportion of the surveyed businesses in middle-income countries listed this as a challenge. It is notable that European businesses (those in France, Germany and the UK) are the least worried about this issue.

<sup>2</sup> Question: "Which of the following business goals and developments will have an impact on your cyber-security plans over the next 12-18 months?". *n* = 2983.

<sup>3</sup> MSP = managed service provider; BYOD = bring your own device.

**Figure 2: Barriers to businesses having highly effective cyber-security capabilities, selected high- and middle-income countries<sup>4,5</sup>**



Security vendors should see the challenges that businesses in middle-income countries face as an opportunity. These businesses may be unattractive targets to vendors for many reasons – such as their security spend being lower than that of companies in high-income countries and pricing being a more important factor in purchasing decisions – but they represent a growing market that vendors can serve with existing capabilities. Few security vendors report their regional revenue splits, [but from the revenue of those that do](#), we can conclude that revenue growth is significantly faster in the rest of the world than in North America, easily the largest region currently for many vendors.

To address the growing opportunity in middle-income markets, security vendors could consider providing lower-cost versions of their standard offerings. Solutions would need to be less complex and faster to implement, and would need to come with an appropriate level of guidance (given that around a fifth of surveyed businesses in middle-income countries reported that the lack of guidance around solutions was a challenge, and a quarter stated that they lack specialist security staff). Vendors could also experiment with freemium models in such markets, allowing businesses to use specific features of their solutions free of charge. If businesses are satisfied with the level of service offered for free (particularly in terms of simplicity to use), they may be easier to convert into paying customers.

For more information about the topics discussed in this article, see Analysys Mason's [Business survey 2019: cyber-security trends in high- and middle-income countries](#) report.

<sup>4</sup> Question: "Which of the following are challenges to your company having a highly effective cyber-security capability?". *n* = 2983.

<sup>5</sup> The survey results for these four countries are indicative of the results obtained for middle- and high-income countries in general.