CHANNELPARTNERINSIGHT

On borrowed time?

In association with

WEBROOT®
Smarter Cybersecurity™

Locking down security opportunities

The cybercrime economy is now worth $1.5tn annually, according to a report commissioned by Bromium – that's roughly equivalent to Russia's GDP in 2018.

While the figure might be surprising, the easy accessibility of malware and other malicious tools on the dark web and a growing support structure for would-be criminals has made it easier than ever to be part of a system that is expected to cost the global economy $6tn in damages by 2021.

It is always high-profile cases that make the headlines. The cyberattack on British Airways stole 380,000 customer transactions, while hackers bagged 339 million customer records from hotel giant Marriott, leading to record GDPR fines of £183m and £100m respectively.

But behind the headlines, small businesses are falling victim to cyberattacks every day. The financial impact of a data breach can sometimes even force small companies to shut down their business. One report by Verizon claims that 43 per cent of all email attacks target SMBs. Even small businesses now offer an enticing treasure trove and an easy target for cybercriminals.

Most don't have the resources, staff or time to manage their cybersecurity infrastructure themselves. Couple that with the mobilisation of the modern workspace – with firms adopting BYOD, cloud and digital technologies – and the result is that small businesses have become critically vulnerable.

Research by *Channel Partner Insight* has sought to uncover how channel partners are serving this often overlooked customer base to reveal the key challenges and trends that are shaping the security strategies of both SMB customers and the IT providers that serve them.

■ *Josh Budd is editor of CPI*

Going big with small business

We quizzed 151 executives from resellers, systems integrators, managed service providers and IT consultancies on their security experiences with small businesses. We sought to find out what's keeping small businesses up at night, and assess how vital a bulletproof security solution has become in winning, and keeping, the business of smaller customers.

All those who participated in our research said they are currently serving smaller customers – with less than $50m in annual revenues.

Demographics

Of the 151 respondents who took part, 79 said they work for a reseller or value-added reseller. Forty-one are from an IT consultancy or services firm, 40 are from a managed service provider and 13 are from a systems integrator.

The vast majority (85 per cent) of the channel execs who took part in our survey are from organisations with fewer than 251 employees – so are very much from small businesses themselves. Only 18 respondents work for a company with between 251 and 1,000 staff.

The key to customer loyalty?

Our research was keen to gauge whether our respondents believe there's a correlation between a strong security offering and customer retention.

With repeat business being the most valuable and reliable source of revenue for channel firms, we wanted to know whether investing in security paid dividends in customer loyalty.

Surely, there's no other area of IT where the term "trusted adviser" is more appropriate than security.

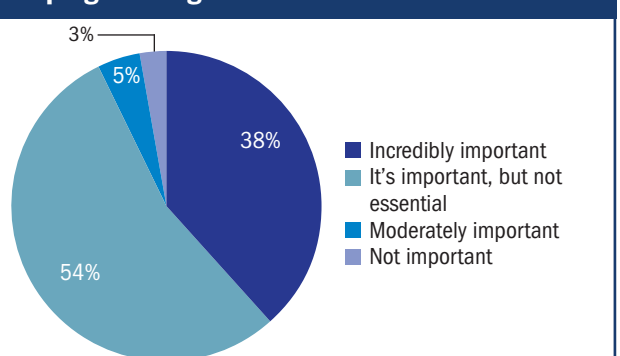
We asked: how crucial is your security business in keeping existing customers? (*see figure 1*).

The response was clear. Thirty-eight per cent of channel respondents went so far to say that their existing customers would leave them if their security offering wasn't up to scratch. A further 54 per cent said that a strong security offering was important for customer retention.

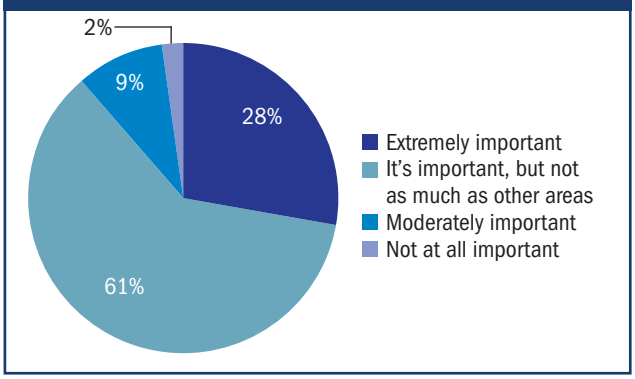
Judging from our findings, investing in your security business is a surefire way of building customer retention.

We also wanted to know how relevant a strong security offering is in helping the channel to acquire new customers (*see figure 2, p3*). Most respondents (61 per cent) said security was "important" in winning new business, but that customers tend to be more interested in other areas of their business. ➔

1) How crucial is your security business in keeping existing customers?



2) To what extent is security an important factor in a customer's decision to work with you?



But a convincing 28 per cent of respondents said customer acquisition hinges on security, claiming that customers want to know more about their security offering than any other area of their business.

This tells us that the channel sees security as a way to help acquire new customers and retain existing ones. Furthermore, they're aware that a substandard security business will make customers look elsewhere.

We also learned that security is a revenue growth engine for the channel. We asked our channel representatives to tell us how much they expect their security business revenues to grow over the next 12 months (*see figure 3*).

A massive 72 per cent of respondents are expecting double-digit revenue growth from their security business over the next 12 months, with 18 per cent expecting above 20 per cent revenue growth.

And security accounts for a large portion of overall revenues for most channel firms. Fifty-eight per cent of respondents said that security accounts for more than 10 per cent of their total revenues. Thirty per cent said security accounts for up to a fifth of their total revenues, while 17 per cent said it's up to a third (*see figure 4*).

It's no secret that security is a key investment area for the channel. From large resellers to small MSPs, the need for security is often quoted as a priority.

Apportioning the blame

Despite cybersecurity's power in winning over and keeping new customers, it can also be a way to lose them.

Research from Continuum suggests that cybersecurity is the number one reason why an MSP would be fired by their customers.

Fifty per cent of our channel respondents said that at least one of their SMB customers has fallen victim to a cyberattack within the last six months.

In most cases, the customer lost one or two days of business as a result of a cyberattack, according to our respondents.

Thirty per cent said it took up to 48 hours for the threat to be contained and their customer's business to resume as normal. Twenty-one per cent said their customers were back to normal in less than 24 hours, while 15 per cent said it took more than a week.

Despite an often-talked-about blame culture in cybersecurity, it seems that customers are perhaps more forgiving than you might think. Our findings suggest that customers didn't point the finger of blame at their IT provider when they fell victim to a breach (*see figures 5 to 8, p4*).

Only nine per cent of respondents said their customer blamed them for being breached. Furthermore, 96 per cent said their customer continued to work with them even after the breach took place.

Vendor partnerships

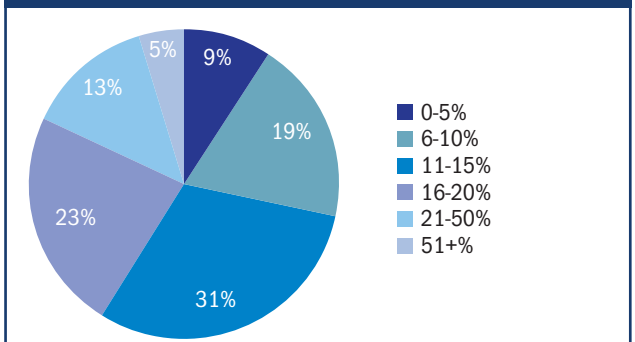
We've established that the channel sees security as a huge revenue growth engine for their business. Not only is it vital in winning over new customers, but a significant portion of the channel community thinks their customers will leave them if their security is substandard.

What about the channel's motivation to invest in more security vendors? The security market is a crowded space, with thousands of vendors vying for market share and the loyalty of channel partners.

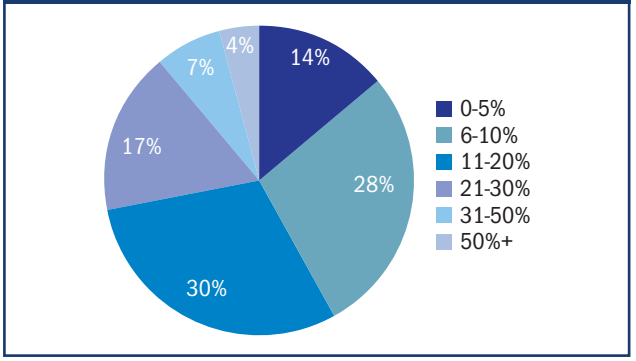
But on average, most channel firms are only working with a handful of security vendors. The vast majority (72 per cent) of our respondents said they're only partnered with two to five vendors. Just 21 per cent said they were working with more than five vendors (*see figure 9, p4*).

Interestingly, a significant 11 per cent are working with ➔

3) How much do you expect your security business to grow over the next 12 months?



4) Roughly what percentage of your business' overall revenues come from security?



5) Has one of your clients been hacked in the ast six months?	6) How long did it take for your client to recover from the cyberttack?	7) Did your client blame you for why they were breached?	8) Has the client continued to work with you?
Yes 50%	<24hrs 21%	Yes 9%	Yes 4%
No 50%	Up to 48hrs 30%	No 91%	No 96%
	Up to a week 16%		
	Over a week 15%		
	>48hrs 18%		

10 or more vendors, which suggests that a fair portion of our respondents are building a large ecosystem of partners in the security space.

Will the channel grow its cybersecurity vendor network?

A slim majority (53 per cent) of our survey participants said that the number of vendors they work with will remain roughly the same over the next three to five years. But a sizable portion (36 per cent) said they will look to add more security vendors to their stable, with only 11 per cent saying they will have fewer vendor partners (*see figure 10*).

We asked our participants to tell us why their partner ecosystem will grow, shrink or stay the same over the next three to five years.

Of those who expected to grow their security vendor count, one said: "There are so many good security vendors coming into the marketplace that I can see more niche vendors offering niche services which we would utilise."

Another said: "We like to keep our options open. We also believe it's important to maintain relationships with as many vendors as possible. Also, customers often dictate which vendors to go with, therefore we need to work with as many as possible."

But others said limiting the number of vendors they work with often produces a better quality of service for customers.

"We feel that by working exclusively with key security vendors, we can provide the software but also the support services without the need for conflict. In the past, resellers have sold whichever security software vendor that is flavour of the quarter. We choose to have long-term relationships with a few security vendors to satisfy our customers and also to ensure long-term support for them," one participant wrote.

Opportunities abound?

The introduction of GDPR in 2018 was regularly touted as an opportunity for security providers to acquire more business, as organisations looked to do everything they could to prevent a breach, and a hefty GDPR fine.

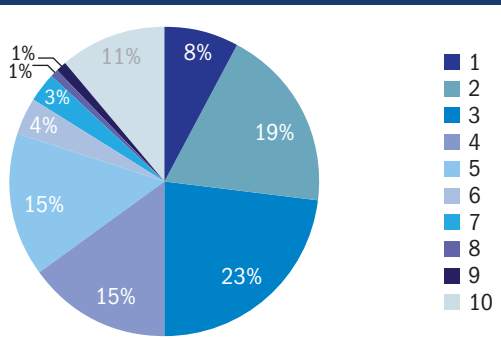
According to the European Data Protection Board, 281,088 GDPR cases were logged by authorities within the first year of GDPR coming into effect. As of September 2019, the EU will have issued, or announced its intent to issue, more than €372m in fines.

Google was the first high-profile company to be handed a fine. In January this year, France's CNIL fined the tech giant €50m, followed by a record £183.39m fine handed to British Airways in July.

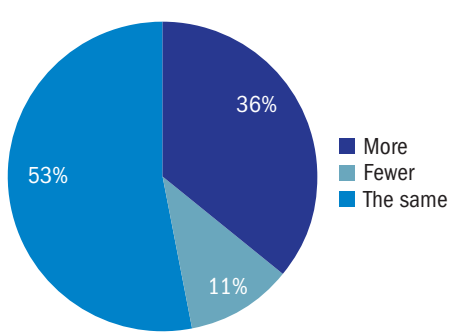
But have these huge fines had an impact on how smaller businesses view their IT security? (*see figure 11, p5*).

According to our findings – yes. Out of our channel respondents, 71 per cent said high-profile GDPR fines have created an opportunity for them to gain new business, with 13 per cent claiming they "strongly agree". ➔

9) How many security vendors are you currently working with?



10) Can you see your firm working with more or fewer security vendors in the next 3-5 years?



Even small companies are being mobilised by the legislation, and the channel sees GDPR as a growth engine for its security business.

Another security opportunity facing MSPs and resellers is the encroaching end of Windows 7 support from Microsoft. By January 2020, Microsoft will no longer update the much-loved operating system, leaving it vulnerable to security attacks.

A survey by Adaptiva found that around 22 per cent of end users still expect to be running Windows 7 by the end of the January 2020 deadline.

We asked our channel participants to tell us whether they saw a security opportunity in Microsoft ending support for Windows 7.

Forty-four per cent of respondents said that Windows 7 will create opportunities to sell more security to their customers. A sizeable 24 per cent agreed that Windows 7's end of life "will mean our customers will depend on us more than ever".

And it looks like the channel's efforts will be geared towards migrating customers away from Windows 7 leading up to the 2020 deadline. Fifty-six per cent of respondents named Windows 10 migrations as the biggest opportunity to come from Windows 7 end of life.

Twenty-five per cent of respondents said they see migrating customers to cloud-based solutions as the biggest opportunity. Lastly, 17 per cent said filling in Microsoft's role in securing and updating customers' existing Windows 7 systems presented the biggest opportunity.

Partners told us that a large portion of their existing customers are still running Windows 7. Forty per cent of respondents said at least 21 per cent of their customers are still using the old operating system, while 60 per cent said Windows 7 usage stood at 20 per cent or lower.

But this figure changes drastically when we asked them how many customers they expect to still be using the operating system in January 2020. A whopping 77 per cent of respondents said that less than 20 per cent of their users would be using Windows 7 after the deadline.

Partner feedback

We gave our respondents the opportunity to anonymously give feedback on how well their security vendors are engaging with the channel.

The replies were a mixed bag – many players claim that there are far too many vendors operating in the security space today, with several saying they'd like to see more integrated solutions on offer to the channel.

"The cyber market is crowded and it is harder for companies to stand out from the crowd," said one partner. "There needs to be more focus on strategic, relevant planning and roadmapping as well as more co-operation between vendors for the good of the end user."

Another partner said many vendors are looking for immediate wins, and are poor at earning the trust of partners through long-term planning.

"Too many security vendors are looking for short-term wins which are driven by shareholders or the board of directors. The reality is, they don't breed trust in the resellers or customers. Long-term realistic investment and returns are key in maintaining a successful business model," they said.

11) To what extent do you agree that high-profile GDPR fines have created an opportunity for you to gain new business?