THE EVOLVING ROLE OF SAAS AND IT OUTSOURCING IN SMB IT SECURITY

Corporate IT Security Risks Special Report Series 2016

Kaspersky Lab

CONTENT

INTRODUCTION

For SMBs, getting the maximum return and efficiency out of every resource is vital to long term success and profitability. The evolution of IT has played a huge role in helping SMBs become competitive alongside larger enterprises, with IDC predicting[1] that these investments will continue to rise to 2019 at a rate of 4.4%, year on year.

By their very nature, SMBs have different IT requirements and challenges to their larger counterparts and despite rising spend in IT, constrained budgets and staffing can make it hard to keep up with the fast-paced, technology-driven world we live in.

The reliance on mobile devices and BYOD in running a lean operation has seen the SMB IT ecosystem change dramatically over the past five years alone, presenting new challenges for small businesses to get to grips with. The IT infrastructure complexity faced by SMBs is highlighted by the rise of BYOD adoption. According to our research, the majority of SMBs currently manage over 50 mobile devices, with more than 60% admitting this has risen over the last three years.

[1] Worldwide Small and Medium-Sized Business Forecast, 2015–2019: IT Spending by Company Size and Region for Key Hardware, Software, and Services Categories, IDC, July 2015

To understand the challenges and threats facing businesses today, Kaspersky Lab conducted a global research study of 4,395 business executives across 25 countries in conjunction with B2B International – asking them a series of questions around their perception of IT security threats, the reality of the threat environment and the impact of data breaches upon operations.

Despite their size, the threat of a cyberattack on SMBs is no less than that of any other business. Indeed, a lack of resources, budgets and security expertise is often cited as a key reason for their attractiveness to cybercriminals and an easier target than larger enterprises. This makes it all the more important to spend budgets wisely and look at other options for remaining vigilant and not becoming a victim.

For many SMBs, Security as a Service (SaaS) could be the answer, by providing a cost effective way for them to take advantage of technology through a cloud-based, subscription model. This can help them remain competitive finding new ways to optimize costs and resources. It has the potential to lift SMBs from being under-prepared and under-resourced to clued up and completely protected. This type of provision also has the benefit of being able to scale up to full blown IT outsourcing along with company need. Working with managed service providers, SMBs can get the next level of security support, intelligence and expertise to help their business continue to evolve and remain fully protected as their technology needs and IT infrastructure grows.

Within this report, we delve into the IT security challenges faced by SMBs and the role of SaaS and IT outsourcing in helping to keep on top of the threat landscape, today and tomorrow.

THE SMB SECURITY CHALLENGE

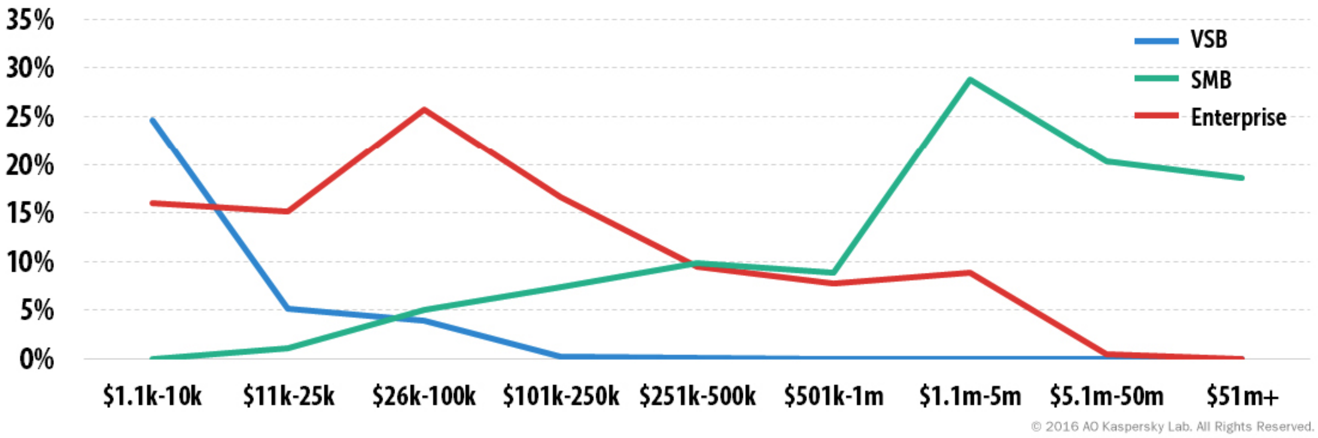
Managing complexity

Having the right resource in place to manage IT and keep up with evolving threats is a key part of the security puzzle. But with over half of SMBs (55%) citing the growing volume of devices they need to secure as a key challenge, this could be easier said than done. The widespread problems such as limited resources, expertise and budget all put a strain on SMBs to keep up with the constantly evolving threat landscape. For many, cloud services have provided a way to manage costs and complexity with overall adoption among SMBs continuing to rise year on year. Recent figures suggest that nearly two-thirds (64%) of small businesses already have an average of three cloud services solutions in place.

However, when it comes to security and integrity of these services, concerns still exist with our research finding that half of VSBs (52%) and SMBs (49%) admit to feeling vulnerable to incidents affecting the third party cloud services they use.

Small budgets, big expectations

As we might expect, budgets allocated to IT security are small - two thirds (66%) of VSBs spend less than $1,000 a year on IT security compared to 68% of enterprises who spend over $1 million each year. To put this into context, VSBs spend an average of 13% of their IT budget on security but do expect this to rise modestly by 12.5% over the next three years. However, despite smaller budgets, for the majority of SMBs, investment in improving IT security is undertaken regardless of ROI (44% VSBs, 59% of SMBs).



© 2016 AO Kaspersky Lab. All Rights Reserved.

Percentage of businesses whose IT security budget lies in each range

Internal IT security resource remains low

Despite over half (54%) of SMBs believing that IT security will be compromised at some point and that preparation is essential, 40% admit that they lack sufficient insight or intelligence on the threats faced by the business. However, when it comes to allocating budget to bolstering IT intelligence and internal resource, we find that less than half of VSBs (44%) employ dedicated IT staff. For those SMBs who employ IT staff, only one in 10 (13%) specialises in IT security. Delving into different sectors, this figure rises to one in five (20%) within real estate & property, and e-commerce/ online retail (18%). In high IP manufacturing the figure is as low as 7%.

When it comes to predicted growth in IT security specialists among SMBs, more than 60% plan to increase numbers over the next three years, one third (32%) expect levels to stay the same, but 1 in 5 (19%) expect it to increase significantly. However, half of SMBs (50%) do not expect the budget allocated to hiring additional IT security staff will also increase and only 10% say it will significantly increase. For a third of SMBs (35%), improving specialist security expertise is the third biggest driver of increased investment in IT security.

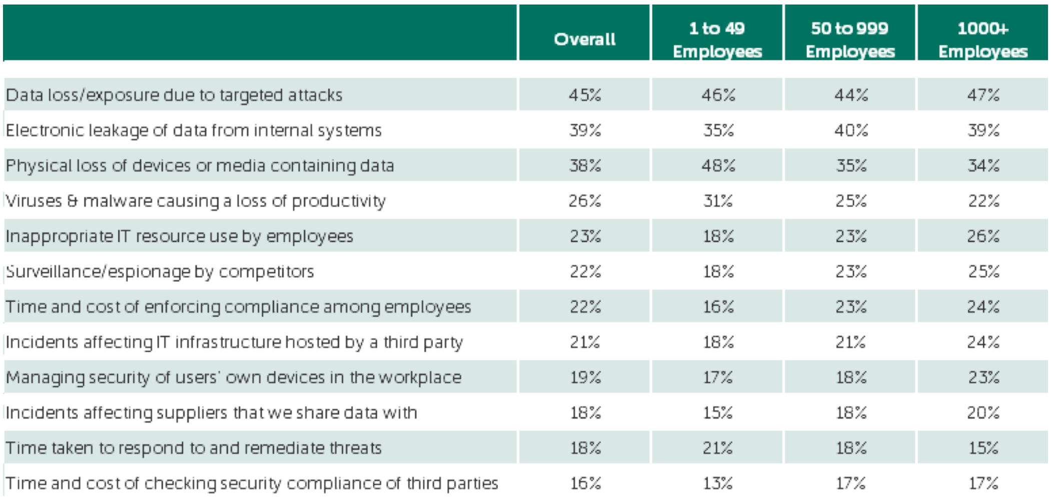
With small budgets, SMBs are struggling to grow the necessary IT intelligence needed to defend themselves against the growing threat landscape. This makes the case for outsourced IT security expertise even more attractive, especially when 53% of SMBs claim that there is a shortage of IT security professionals to hire.

THE THREAT LANDSCAPE

Cyberthreats to businesses of all shapes and sizes are increasing every day. Cybercriminals are becoming more sophisticated in their approach in a bid to catch businesses and individuals out. With financial and reputational consequences at stake, SMBs are rightly concerned about the impact of a data breach on their businesses.

Data loss tops worry list

For small businesses, the loss of internal and confidential data is the main concern when it comes to IT security. Unlike their larger counterparts, VSBs are troubled with the physical loss of devices which can cause a data leakage (48% of respondents agree with this). Along with concerns on the loss of devices, one in five of VSB representatives (21%) is worried about the speed of threats response and their remediation.

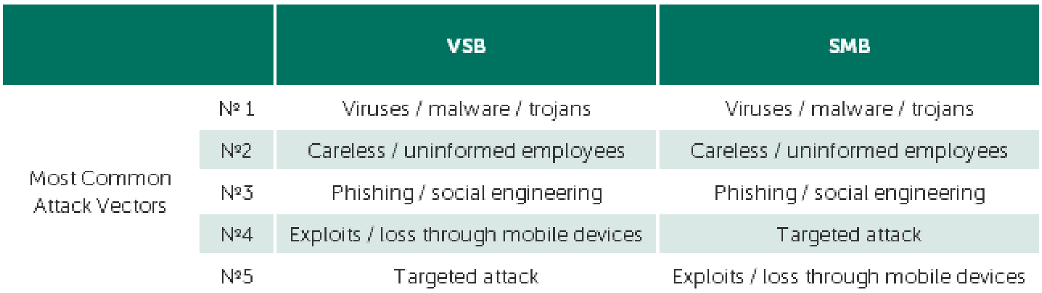


	Overall	1 to 49 Employees	50 to 999 Employees	1000+ Employees
Data loss/exposure due to targeted attacks	45%	46%	44%	47%
Electronic leakage of data from internal systems	39%	35%	40%	39%
Physical loss of devices or media containing data	38%	48%	35%	34%
Viruses & malware causing a loss of productivity	26%	31%	25%	22%
Inappropriate IT resource use by employees	23%	18%	23%	26%
Surveillance/espionage by competitors	22%	18%	23%	25%
Time and cost of enforcing compliance among employees	22%	16%	23%	24%
Incidents affecting IT infrastructure hosted by a third party	21%	18%	21%	24%
Managing security of users' own devices in the workplace	19%	17%	18%	23%
Incidents affecting suppliers that we share data with	18%	15%	18%	20%
Time taken to respond to and remediate threats	18%	21%	18%	15%
Time and cost of checking security compliance of third parties	16%	13%	17%	17%

Top IT Security Concerns (Main Differences By Company Size)

When we look at the number of attacks experienced by SMBs over the last 12 months, their concerns are rightly justified. It also becomes clear that measures in place to combat the threats are not necessarily providing the right levels of protection in all cases.

Among all the incidents experienced by SMBs viruses & malware causing a loss of productivity leads the list– more than 41% of respondents faced this problem.



		VSB	SMB
Most Common Attack Vectors	№ 1	Viruses / malware / trojans	Viruses / malware / trojans
	№2	Careless / uninformed employees	Careless / uninformed employees
	№3	Phishing / social engineering	Phishing / social engineering
	№4	Exploits / loss through mobile devices	Targeted attack
	№5	Targeted attack	Exploits / loss through mobile devices

Time costs money

For many SMBs, the financial impact of a data breach can be severe with reactive measures and costs taking precedence. Indeed, figures from the National Cyber Security Alliance suggest that 60% of SMBs suffering a breach will go out of business within 6 months. Continuing to think “it won’t happen to me” and focusing on a reactive approach could be a major downfall.

An estimated $14k of additional internal staff wages are required to steady the ship after an attack, with a breach resulting in an average of $13k in lost business. Improving software and infrastructure as a result of a breach costs SMBs $10k, on average. The average total financial impact of a data breach is estimated to cost **an SMB $86.5k**.

The longer data breaches go unnoticed, the more it will cost an SMB in monetary and data integrity terms. Even when breaches are detected almost instantly, SMBs estimate a cost to their business of $28k, rising to $105 if undetected for more than a week.

Data is also more vulnerable the longer a breach goes unnoticed, with an average of 417 sensitive customer/employee records compromised even with instant detection, and over 70k at risk if undetected for over a week.

EXTERNAL SUPPORT AND CLOUD SERVICES COULD BE THE ANSWER

So how can SMBs bridge the gap between smaller budgets and less expertise, and the very real and growing threat of cyber attacks?

Alongside a traditional on-premise security approach, SMBs can look at two viable alternatives to give them the additional expertise and support they need, within their budget and resource capabilities. One problem can be solved in different ways and for small and mid-sized businesses, the main thing is to find the most beneficial solution.

We have already discussed the merits of cloud services as a way to reduce complexities and take advantage of economies of scale and the same is true when it comes to IT security.

By taking a SaaS approach to security, SMBs can take advantage of endpoint security solutions without having the hefty budgets of enterprise counterparts. It can help VSBs easily control costs, simplify and centralize their IT security whilst gaining access to vital protection and expertise.

Despite the diverse range of security solutions on the market today, SMBs are still limited by resources and budgets when looking for their best-fit solution. SaaS security products available via subscription - such as Kaspersky Endpoint Security Cloud - enable smaller businesses to take advantage of market leading technology that meets their needs, avoiding hefty hardware costs. This gives them a great alternative to help make the most of available budgets and expertise, ensuring that vital resources are left available to invest into strategic business development and future growth.

40% of SMBs and 26% of VSBs agree that outsourcing could be the answer and are looking to outsource IT infrastructure and processes to third parties.

However, when it comes to the second option - using external IT security service providers - a third (36%) of VSBs do not use one but one in five (20%) plan to, in the next 12 months. For SMBs, only 17% have no plans to use an external IT security service provider but almost a quarter (23%) see this changing in the next 12 months.

With our research suggesting that many SMBs are seemingly dismissing third party support and also not investing significant funds in internal IT security resources, they could be missing a vital part of IT security protection which technology alone can't fix. In fact, those who do outsource and prioritise Security as a Service (SaaS) feel it is an effective security measure (57%).

To meet the growing complexities around the volume of mobile devices they need to protect and the fast evolving threat landscape, working with an expert to garner intelligence and insight will bolster SMBs defences and help them make the most out of available budgets for complete protection.

By working with a third party, SMBs can bring on board experts in the field without having to find the high budgets to hire someone internally and will have access to a high-level of IT security support and expertise. This is particularly important as skills need to be constantly enhanced, in line with the changes and implications of threat vectors.

To help SMBs combat the ever growing number of threats with limited budgets and expertise, SaaS and IT outsourcing are viable options, alongside traditional on-premise security approaches, to help small businesses make the most of available spend and resources.

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy