KASPERSKY lab

Growing businesses safely: cloud adoption vs security concerns

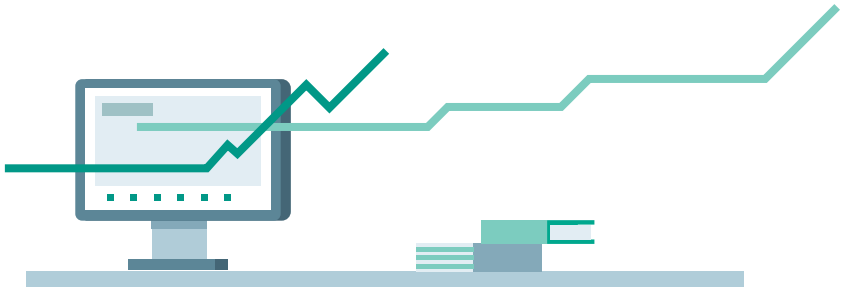
kaspersky.com

Contents

Introduction

With the world having experienced something of a start-up revolution over the last few years, the chances are you have either started your own businesses, or you know someone who has.

Whether they failed or succeeded, one thing's for sure: it's a very interesting time to be a small business – for the purposes of this report, very small businesses (VSBs) are classified as having 1-49 employees, while medium sized businesses (SMBs) have 50-249 employees.



On the one hand, there's more competition than ever before. Millions of new businesses are established around the world every year, as entrepreneurs look to go out on their own. This increasing competition is shown by the number of businesses that fail. **Approximately one-fifth of start-ups close down within the first year, due to factors such as insufficient management, a lack of capital or changing market conditions.**

On the other hand, there is also a huge amount of opportunities. From the moment they are launched, businesses have more ways than ever to engage with customers, expand into new markets and roll out new products or services.

Thanks to technologies such as cloud computing, small businesses can expand their operations without breaking the bank and realise efficiencies across all areas of the business, from HR and marketing to finance and IT.

Depending on how an individual business uses technology, modern innovations also enable rapid growth, with cloud in particular leading the way.

Cloud technology drives business development

The power of cloud has clearly been shown by the industry's steep upward trajectory over the last few years, which is set to continue in the future. **Gartner predicts that worldwide public cloud services revenue will reach $411 billion by 2020, nearly doubling in four years from $220 billion in 2016.**

And this spending isn't just coming from large enterprises. It is estimated that **78% of small businesses will host their IT environments in the cloud by 2020**, driven by a need to expand their operations and compete in ever-more competitive marketplaces.

That's why many VSBs and SMBs are actively embracing the likes of cloud computing and consuming business applications as-a-service. Ultimately, cloud is an enabler for innovation. For example, Infrastructure-as-a-Service (IaaS) is being used to accelerate and simplify technology deployments, while Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) platforms are opening up new business models and driving efficiency improvements for businesses of all sizes.

So, why exactly are small businesses continuing to adopt cloud platforms? Firstly, there are cost-efficiency benefits. Moving to the cloud enables businesses to cut expenses on IT infrastructure, create efficient operational environments and only pay for what they actually use instead of having a set price every month.

It can also make businesses more agile as they grow and develop. For example, cloud platforms enable employees to work from anywhere, at any time, which is essential as more and more small businesses enable their employees to work remotely. **Today, half (50%) of VSBs and 40% of SMBs regularly allow their employees to work outside of the office, highlighting how prevalent the trend has become. Not only does this increase productivity, it can also boost morale and help businesses maximise their capabilities.**

Finally, cloud enables businesses to move quickly and adapt to market trends in a way that simply isn't possible without the technology. This might help them win new business, or attract a new group of customers, both of which play a vital role in business growth.

Clearly, cloud computing should now be an important part of any business strategy but – as with any technology – there are likely to be some bumps in the road.

The IT security tipping point

Despite the opportunities SMBs now have access to during their development, there are also some very real security risks that they should be aware of. As they grow and their IT infrastructure becomes more heterogeneous, businesses can quickly find themselves having to deal with increasing levels of complexity and confusion.

66% of companies

see the main challenge in managing the heterogeneous IT environment

For example, adopting a combination of public and private cloud platforms may give SMBs the flexibility to get ahead of their competitors and grow. But, continuously adding new workloads and integrating different vendors as their business needs develop has the very real potential to result in security vulnerabilities that may not even become apparent until a breach occurs.

What's more, security often tends to take a back seat in the early days of most businesses. The priority for start-ups and small businesses is all about growth and increasing efficiencies, with cybersecurity typically being relegated to an afterthought.

This will eventually lead to a tipping point where businesses have to seriously start thinking about IT security, or risk having all their hard work undone by a cyber-attack that could have otherwise been prevented.

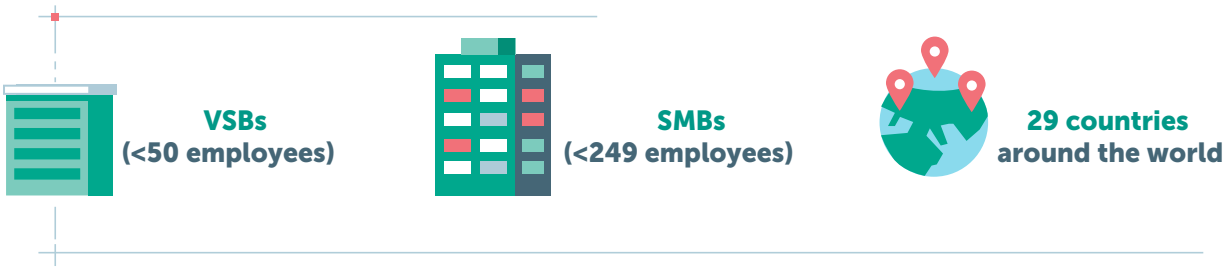
For business leaders, such an event can prompt some rather uncomfortable questions. Who is responsible for IT security? How can they efficiently manage a growing IT infrastructure? How can we stay secure without impacting our ability to move quickly? And do we really need to be worried about suffering a cyber-attack?

This journey is all part of the 'growing pains' that are present in the majority of small and medium sized businesses. Cloud adoption brings with it new cybersecurity implications that companies have to respond to if they truly want to grow and succeed. This is especially true as today's threat landscape continues to develop and new threats emerge on a daily basis.

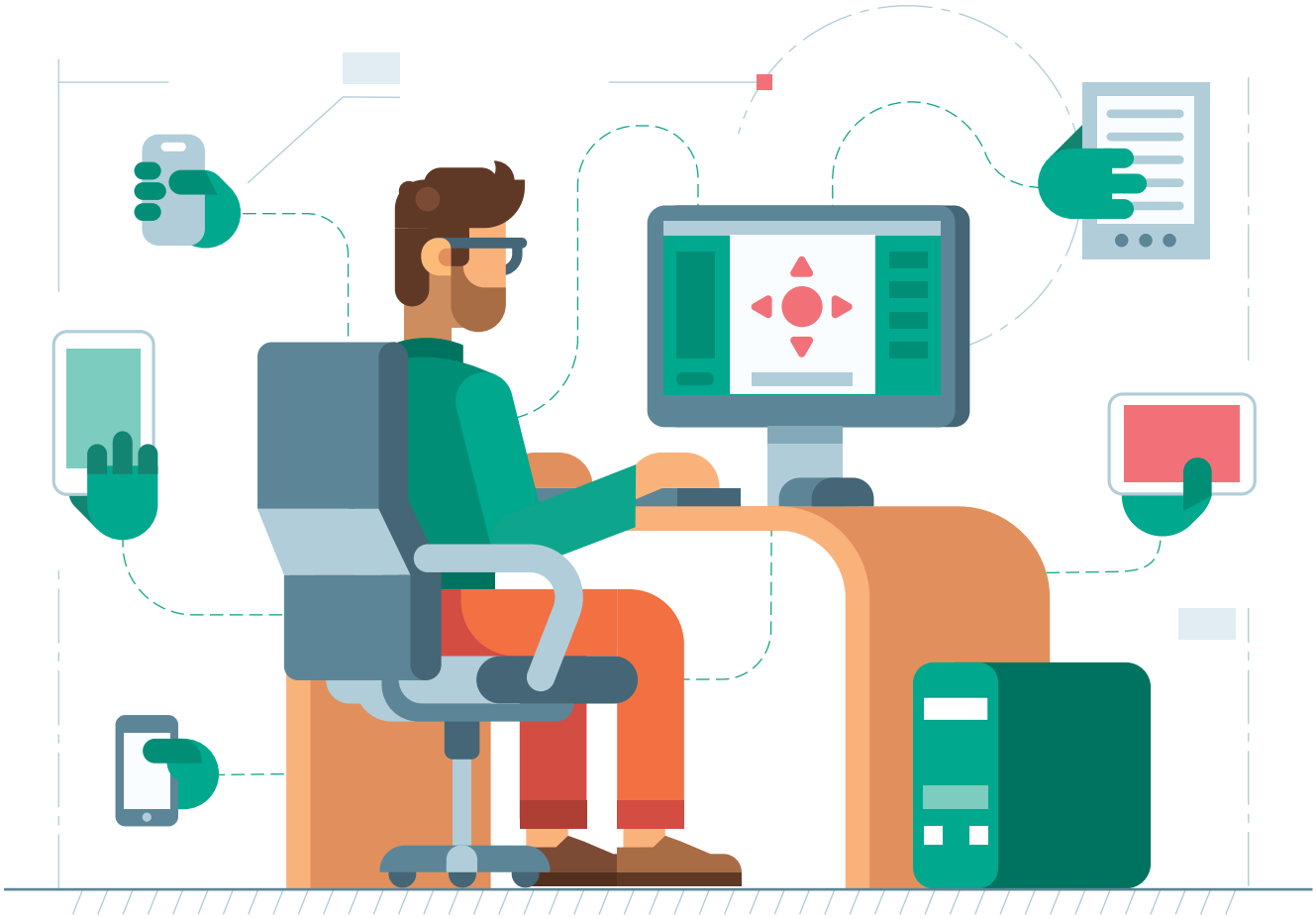
From the smallest companies that may be only have been trading for a few months, to those that have a few years of trading under their belts, cybersecurity has to be given the attention it requires. If it's not, SMBs will likely find themselves having to deal with security incidents rather than focusing on growing their business.

Methodology

The Kaspersky Lab SMB report questioned a total of **3041 IT personnel** from small and medium-sized businesses in **29 countries around the world**. Respondents were asked about the structure of their IT infrastructure, the people involved in managing IT security and their adoption of cloud tools and services.



Throughout the report, businesses are referred to as either **VSBs** (very small businesses with fewer than 50 employees) or **SMBs** (small & medium sized businesses with 50 to 249 employees).



Key findings

Half (50%) of VSBs and 65% of SMBs have adopted some form of cloud platform, with Google Cloud Platform – adopted by 48% of VSBs and 47% of SMBs – being the most popular provider.

Nearly three-quarters (73%) of SMBs and 56% of VSBs make use of at least one SaaS-hosted business application, with email, document sharing platforms and collaboration software being the three most popular among both VSBs and SMBs.

The percentage of companies using SaaS-hosted apps is higher among SMBs then VSBs across all application types, showing that companies tend to adopt cloud on a greater scale as they mature.

Data protection is seen as the number one challenge facing businesses, identified by **28% of VSBs and 26% of SMBs.**

IT security management is often an afterthought rather than a priority. **Nearly a third (32%) of VSBs and 14% of SMBs** entrust the task to non-specialist internal staff, while 11% of VSBs and 2% of SMBs admit that the role isn't managed at all.

Reducing costs, mitigating risk through an SLA and outsourcing all of IT to a third party are the three biggest drivers for businesses planning to use MSPs/MSSPs for their IT security.

Two-thirds (66%) of people responsible for IT in VSBs and SMBs face challenges around managing a heterogeneous IT infrastructure.

Growing businesses experience more attacks than their smaller counterparts. SMBs reported a larger number of incidents than VSBs over the last 12 months related to any cloud platform — public, private or hybrid (10 vs.7).

Going mobile: The need for greater flexibility and efficiency

With VSBs and SMBs today facing more competition than ever before – no matter what the industry – having the ability to make flexibility and efficiency improvements has never been more important.

These improvements can come and many shapes and forms, with one of the most effective concerning employee working habits. SMBs around the world are frequently leveraging cloud technology to embrace a more flexible way of working by allowing their employees to work from anywhere.

As well as meeting changing market demands, offering remote working can also reduce costs and increase employee satisfaction. **Its prevalence is clearly shown by the fact that 50% of VSBs and 40% of SMBs regularly allow their employees to work at locations outside the office, which could include their home, a public place such as a coffee shop, or while travelling.**

And the reasons for granting employees this freedom to work anywhere can vary significantly, depending on the size of the business. For example, geographical distribution and recruitment are clearly more relevant to SMBs than VSBs. This is shown in the figures, as SMBs are more likely to offer remote working due to the geographical nature of their workforces **(31% vs. 20% of VSBs)**, or in order to attract more qualified personnel **(24% vs. 14% of VSBs)**.

However, efficiency and productivity increases are key drivers for both business segments. A third of VSBs (36%) and SMBs (38%) allow remote working to increase the effectiveness of the business, while 36% of VSBs regularly allow employees to work from outside the office to increase their productivity, along with 31% of SMBs.

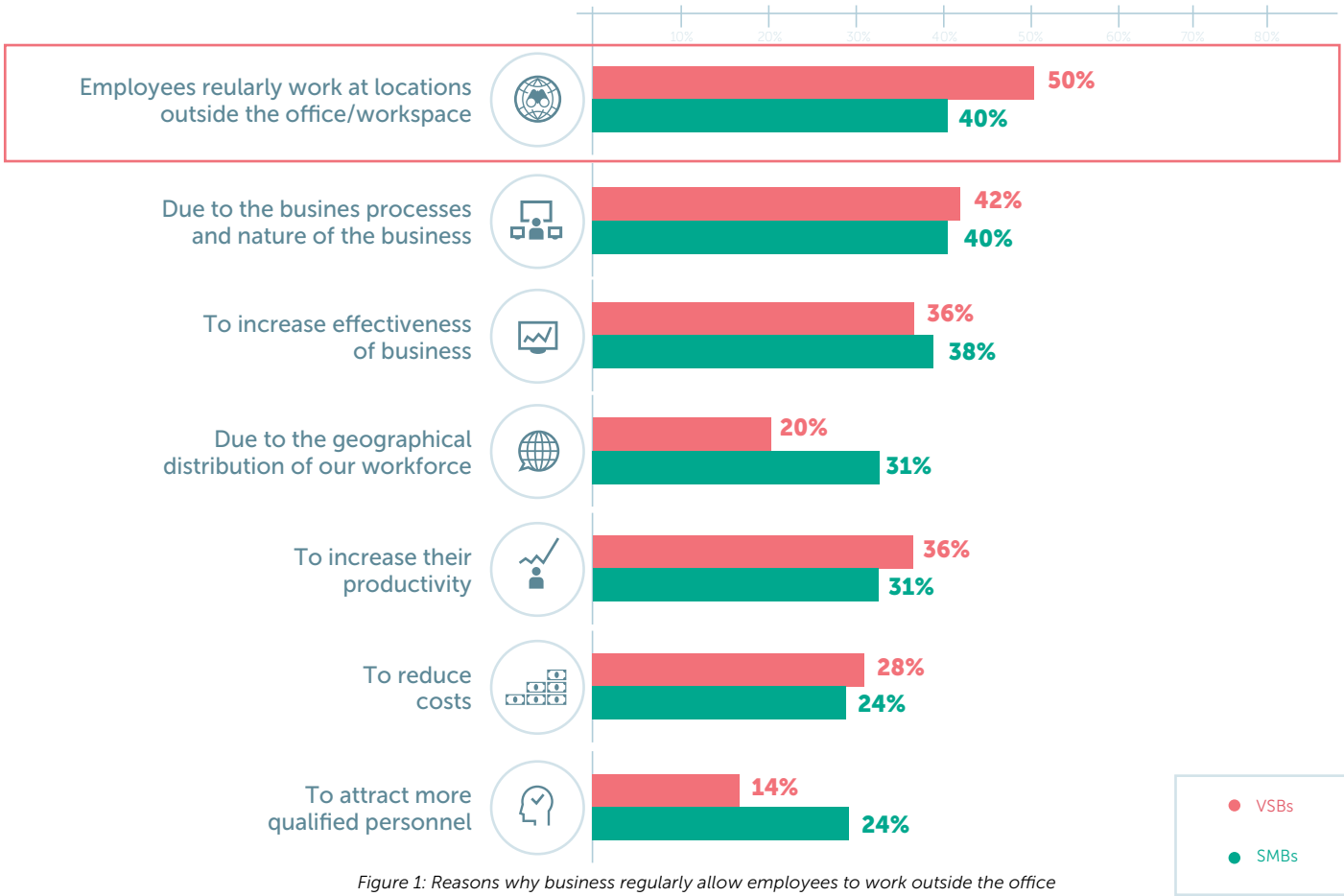


Figure 1: Reasons why business regularly allow employees to work outside the office

As the table above shows, the nature of the business is the biggest reason why companies allow remote working for both VSBs **(42%)** and SMBs **(40%)**, suggesting that the way businesses operate today requires them to grant employees a certain level of flexibility.

Whatever the reason, mobile working is clearly a key component of many medium sized businesses as they look to grow and make themselves more efficient. However, this trend can present complications when it comes to managing an increasingly distributed IT infrastructure.

Business growth: The right use of cloud services or an IT mess?

More so than ever, cloud computing platforms and services are driving business growth. As companies develop from the smallest start-ups, to larger and more mature entities, they are frequently embracing cloud to open opportunities for innovation and make themselves much more agile.

Indeed, the majority of VSBs and SMBs have adopted at least some form of cloud platform, with SMBs appearing to be more active cloud adopters than their smaller counterparts. VSBs are fairly evenly spread across public clouds **(22%)**, hosted private clouds **(25%)** and internal private clouds **(29%)**, with **18%** opting for a hybrid cloud approach.

Adoption is slightly different among SMBs, with internal private clouds clearly leading the way at 46%. This is followed by hosted private clouds – which has been adopted by 37% of businesses – and public cloud at 32%.

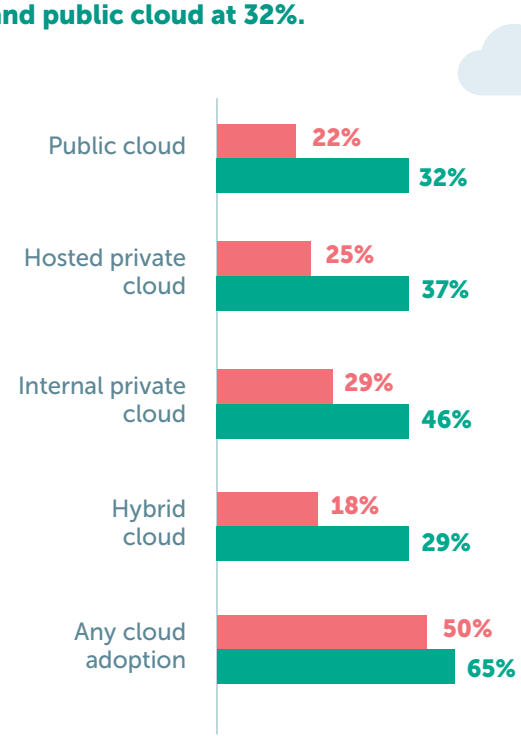


Figure 2: The adoption of cloud platforms

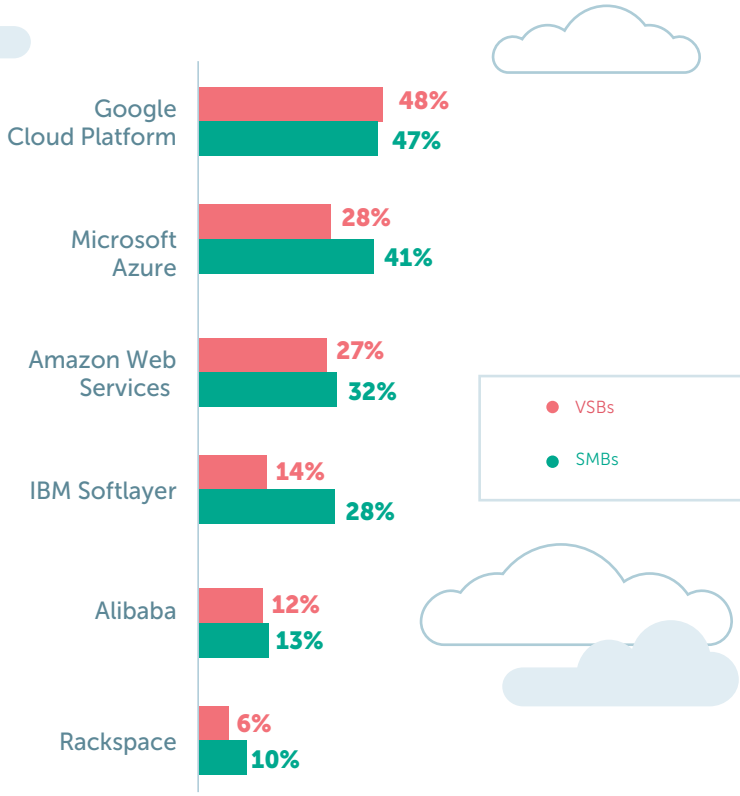


Figure 3: The top cloud providers being used

In terms of specific providers, Google Cloud Platform (GCP) is the number one provider for both company sizes, having been adopted by **48% of VSBs and 47% of SMBs.** Microsoft Azure comes in a close second for SMBs with **41%** adoption (**28%** of VSBs), followed by Amazon Web Services (AWS). Rackspace shows the lowest adoption rate, having been chosen by just 6% of VSBs and **10%** of SMBs.

The next question to ask is; which applications are businesses today hosting in the cloud? Nearly three-quarters **(73%)** of SMBs and **56%** of VSBs make use of at least one Software-as-a-Service (SaaS) hosted business application, covering finance, human resources and virtually every other business unit.

Email and document sharing (such as Dropbox) are the top choices among both VSBs and SMBs. Unsurprisingly, email is the most popular business application, used by more than 90% of businesses. SaaS-based email applications are being used by **21% of VSBs and 29% of SMBs**, followed by document sharing platforms at **18% and 26%** respectively. As the table below shows, the percentage of companies using SaaS-hosted apps is higher among SMBs then VSBs across all application types, showing that companies tend to adopt cloud on a greater scale as they mature.

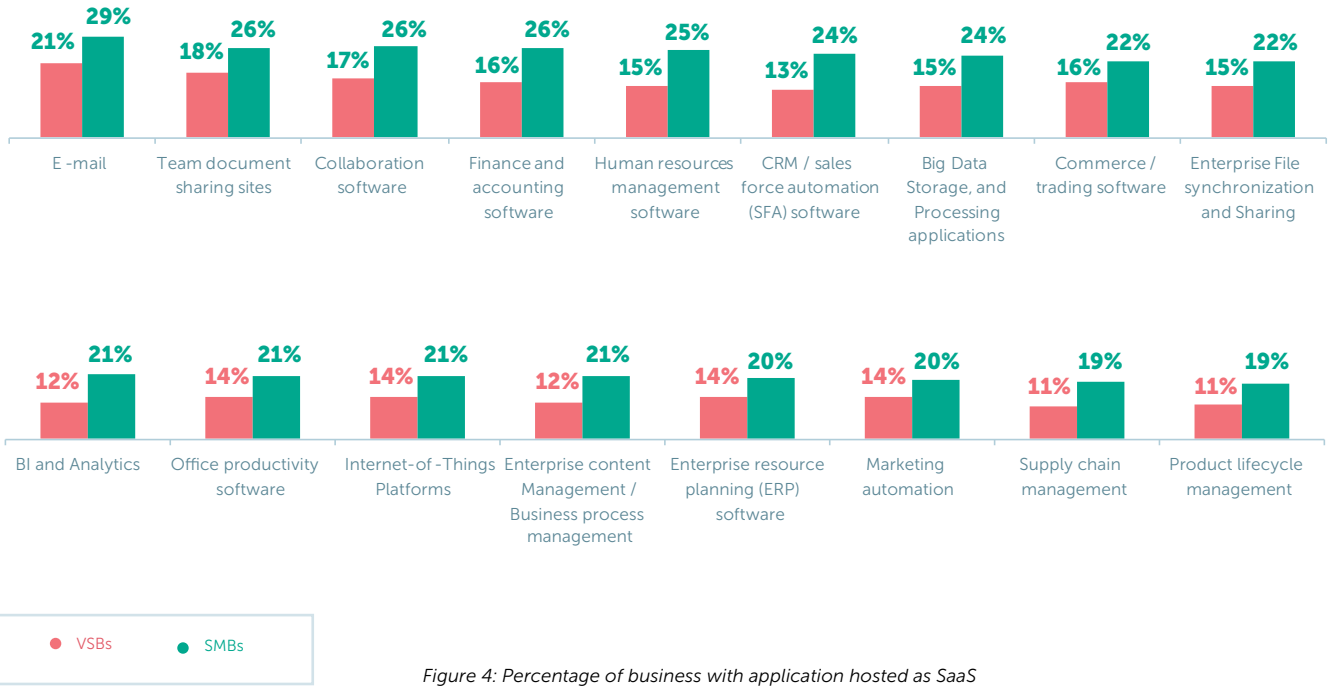
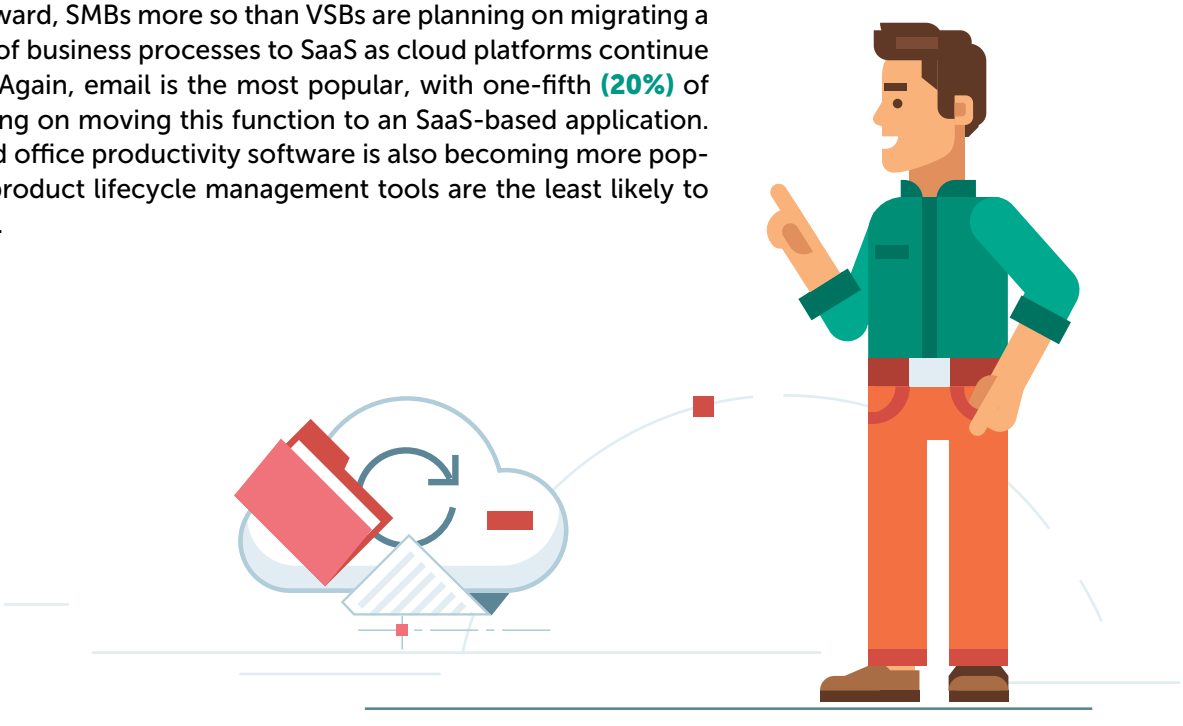


Figure 4: Percentage of business with application hosted as SaaS

Looking forward, SMBs more so than VSBs are planning on migrating a large range of business processes to SaaS as cloud platforms continue to develop. Again, email is the most popular, with one-fifth **(20%)** of SMBs planning on moving this function to an SaaS-based application. Cloud-based office productivity software is also becoming more popular, while product lifecycle management tools are the least likely to be migrated.



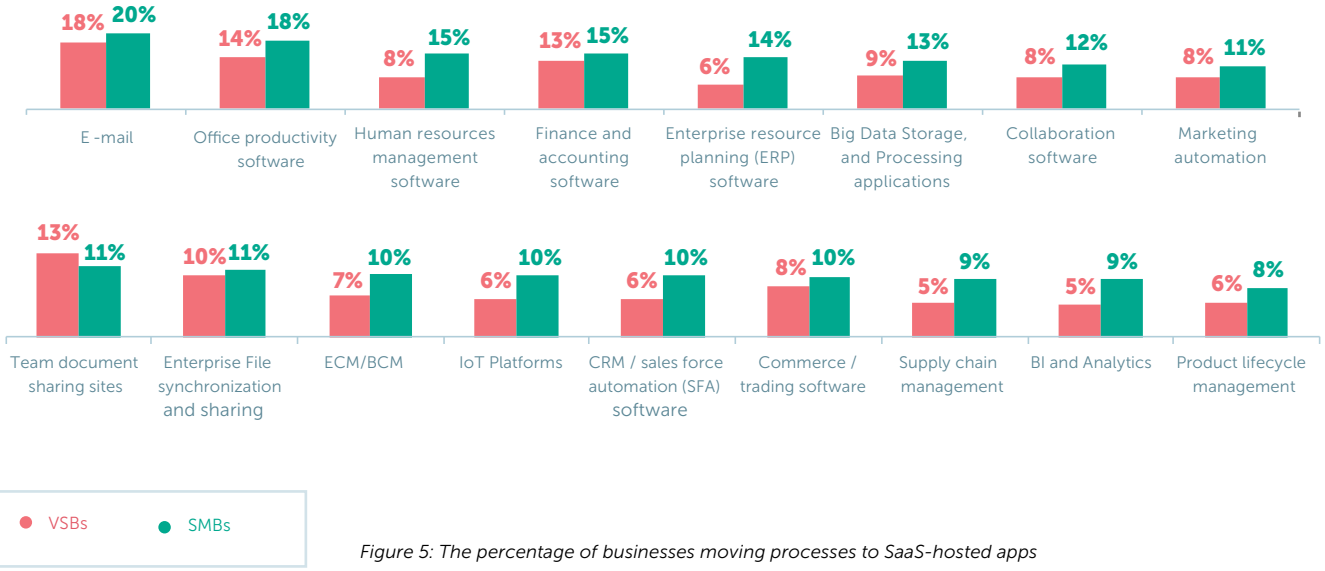


Figure 5: The percentage of businesses moving processes to SaaS-hosted apps

The age of the business can also have an impact on the extent of cloud and SaaS adoption. **For example, VSBs over 20 years old are more likely to adopt internal private clouds (32%) than younger VSBs – 30% for those aged 5 to 20 and 27% for those under five years old.**

Furthermore, SaaS-based business processes are far more likely to be deployed among younger VSBs. The percentage of VSBs under 5 years old that deployed email **(24%)**, document sharing sites **(22%)** and commerce/trading software **(19%)** is significantly higher than those over 20 years old **(15%, 12% and 10% respectively)**. This is partly because cloud services allow start-ups to get up and running instantly, while on-premise solutions often require additional time and effort to get started. However, for more mature companies that already have processes and operations in place, on-premise solutions can sometimes be seen as a more cost-efficient option in the long term.

When it comes to SMBs, those aged 5 to 20 years old were the most likely to have adopted cloud solutions, especially public cloud platforms **(36%)** and hosted private clouds **(41%)**. Interestingly, just 18% of SMBs over 20 years old had adopted a hybrid cloud solution, which is significantly lower than all the other types of platform.

As with VSBs, younger SMBs were also more likely to be using SaaS for a wide range of business applications than their older counterparts. For example, over a quarter **(28%)** of SMBs under 5 years old had adopted SaaS-based BI and analytics applications, compared to just **12%** of SMBs over 20 years old.

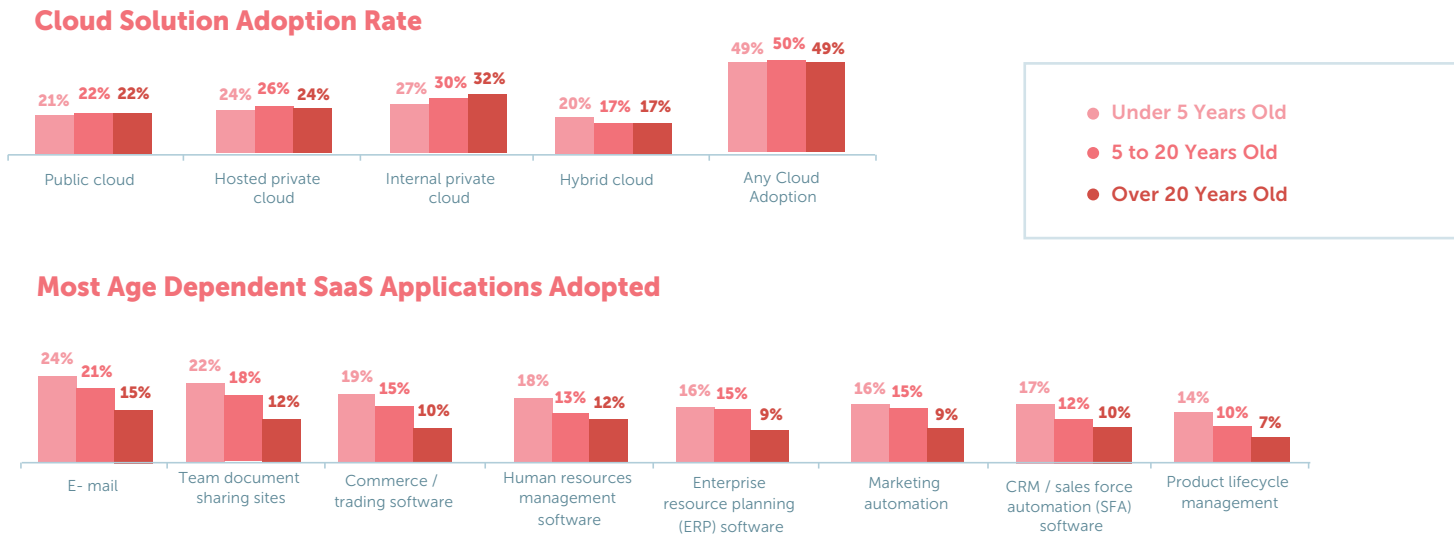


Figure 6. VSB business age and cloud/SaaS adoption

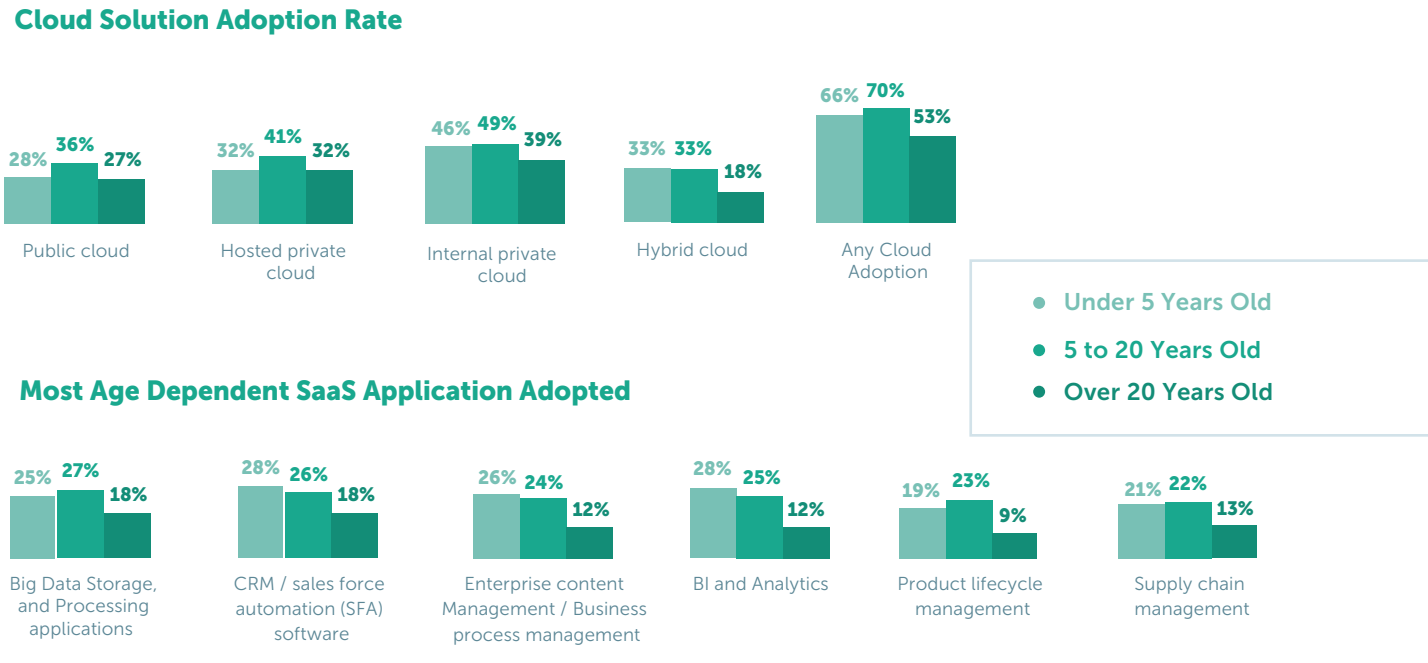
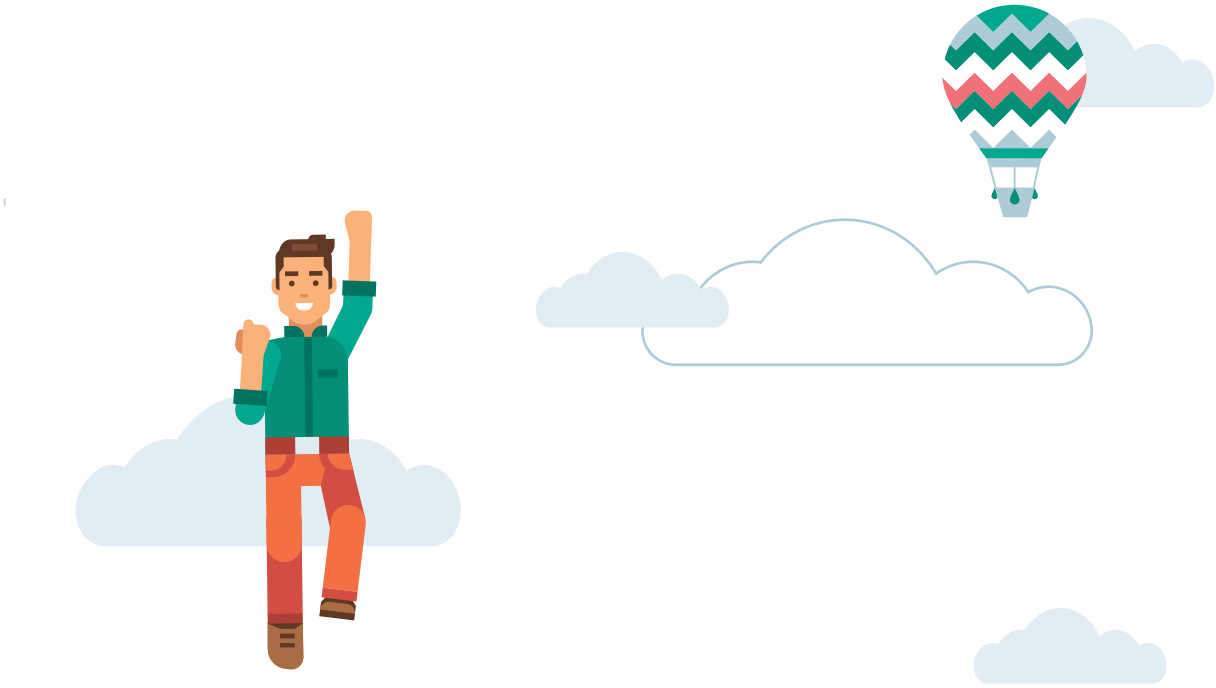


Figure 7. SMB business age and cloud/SaaS adoption

With businesses readily adopting cloud services as they grow, there is a danger that the additional flexibility cloud provides comes at the expense of security. While this might not be a problem initially, there will come a point when security can no longer be an afterthought.

This balance is a challenge that all growing businesses struggle with and one that has to be carefully managed if they want to avoid opening themselves up to vulnerabilities and putting all their hard work at risk. However, when it comes to SMB growth, confusion and complications around infrastructure management frequently get in the way.



In-house or outsourced? IT infrastructure management in SMBs

In large enterprises, infrastructure management is usually an extremely structured process. There will generally be a dedicated IT security team with experienced personnel and certain practices in place to ensure that the infrastructure is managed as efficiently as possible.

However, in VSBs and SMBs, the setup is very different. Indeed, IT security is often a secondary consideration for these smaller businesses, as shown by the resources dedicated to managing it. Nearly a third **(32%) of VSBs and 14% of SMBs** entrust the task to non-specialist internal staff, while **11% of VSBs and 2% of SMBs** admit that the role isn't managed at all.

Furthermore, **32% of VSBs** only have one employee dedicated to managing security and **43% of SMBs** have a security team smaller than ten people. While this could be down to the fact that the simpler IT infrastructure in smaller companies doesn't require extensive resources, it also highlights how it isn't always a key consideration.

The good news is that nearly a third (31%) of VSBs and 44% of SMBs have a role or department dedicated to IT security, showing that plenty of businesses are recognizing its importance.

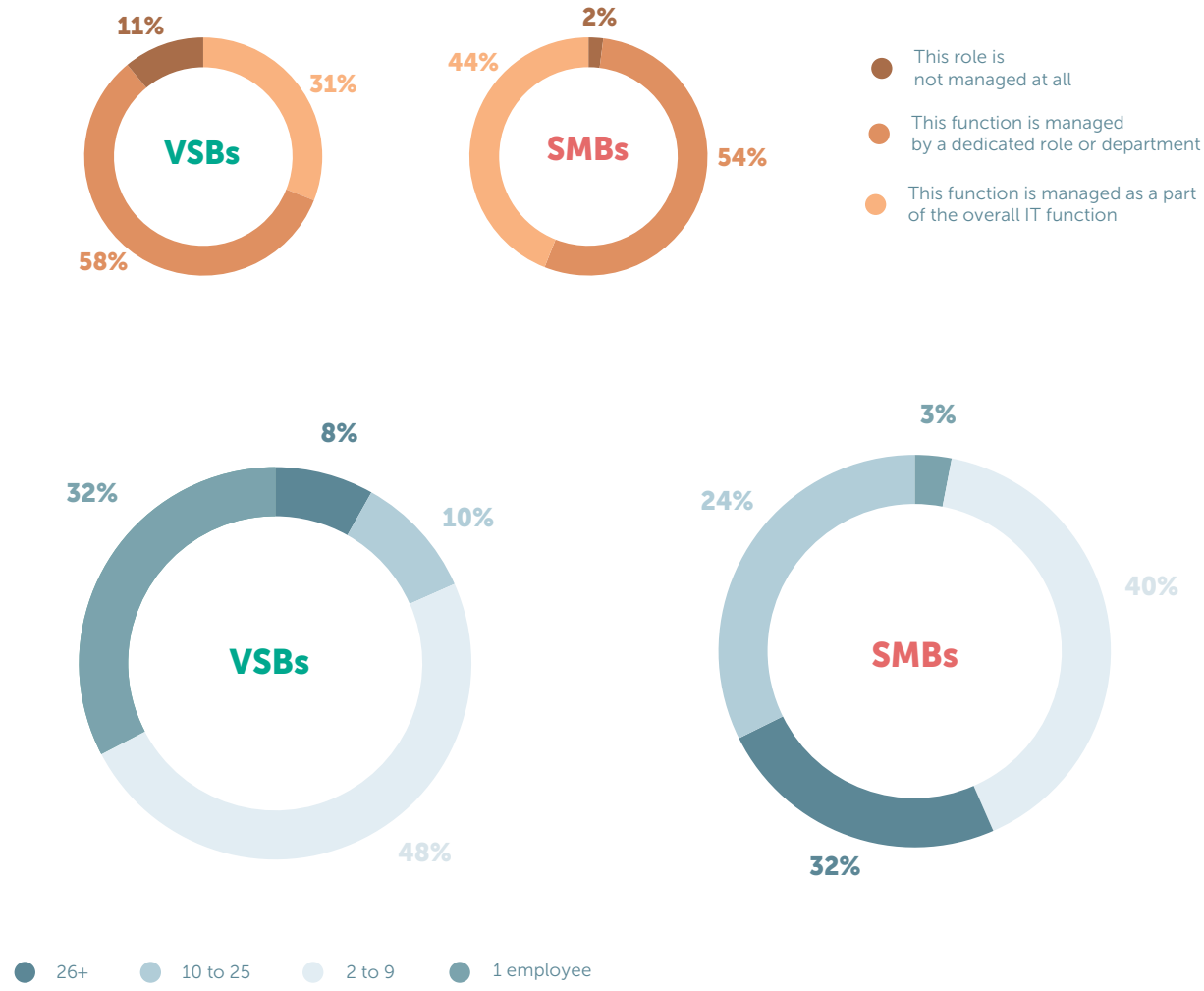


Figure 8: Managing Security

When it comes to the specific people involved in managing IT security, many businesses turn to non-specialists. **Just under a third (32%) of VSBs dedicate the role of security management to non-specialist internal staff, compared to more than one-in-ten (14%) SMBs.**

There is also some indication that smaller businesses are less likely to trust their security function to third-parties. Just **18% of VSBs and 21% of SMBs depend on outsourced IT support companies for their security needs**, which drops even lower for outsourced consultants (7% and 8% respectively) and outsourced managed service providers (4% and 9% respectively).

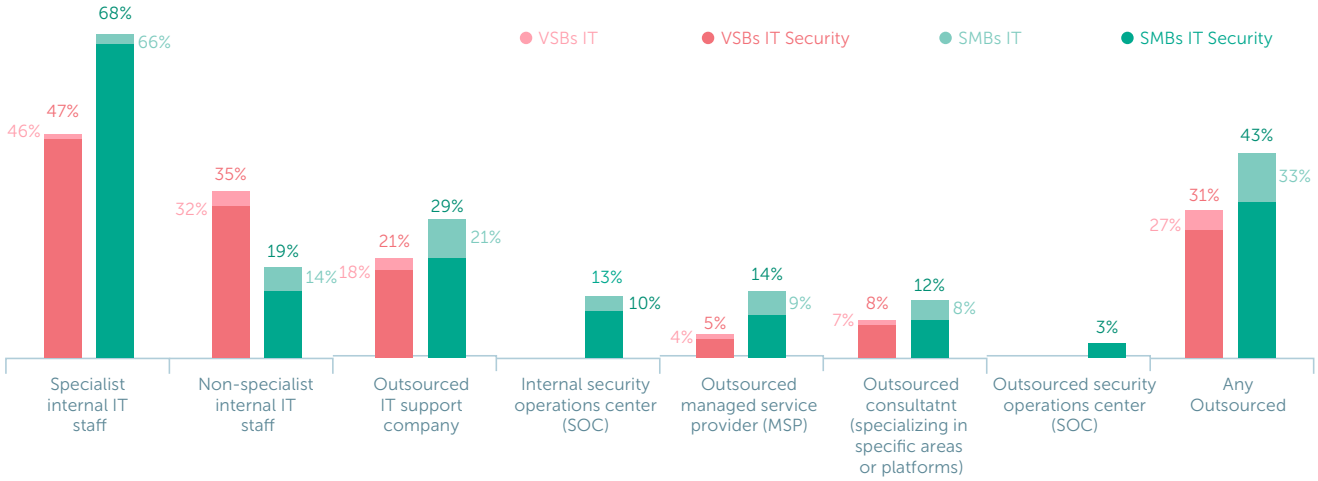


Figure 9: The personnel involved in managing IT and IT security

Interestingly, despite this current reluctance, VSBs and SMBs both see the outsourcing of IT security management increasing in the future. The use of outsourced IT support company shows the biggest increases, with **26% of VSBs and 35% of SMBs predicting that they will rely on them more over the coming years.**

Indeed, the use of any form of outsourcing is expected to increase significantly, irrespective of company size. **Total outsourcing among VSBs is predicted to rise from 27% to 39% in the future and from 33% to 50% among SMBs.**

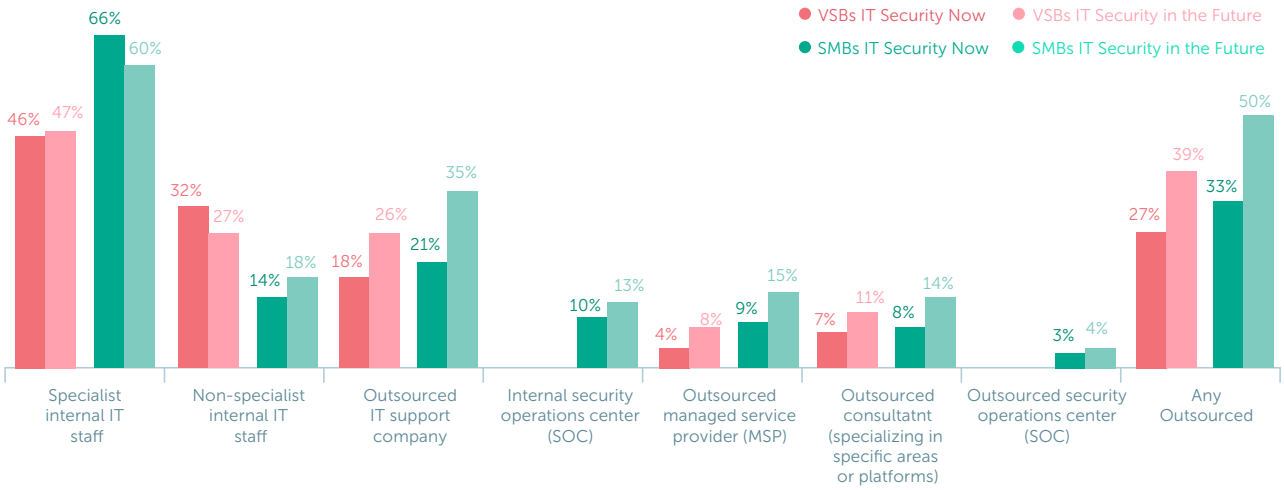


Figure 10: Managing IT security in the future

This trend suggests that businesses are expecting to need more external help in the future as the security demands placed on their IT teams grow over the next few years. Looking back at how much the threat landscape has developed in recent times, businesses would certainly be wise to get ahead of the curve and prepare themselves for what's ahead.

Security growing pains

As businesses grow and embrace new ways of working, their IT infrastructure naturally becomes more complex. Unfortunately, it's an unavoidable reality for any organization and one that can carry significant cybersecurity risks and concerns.

This is shown by the fact that two-thirds **(66%)** of the people responsible for IT in VSBs and SMBs where multiple parties are involved, view managing heterogeneous IT environments as a challenge. Nearly half **(45%)** come across difficulties in securing distributed IT security perimeters, highlighting the growing pains businesses are facing.

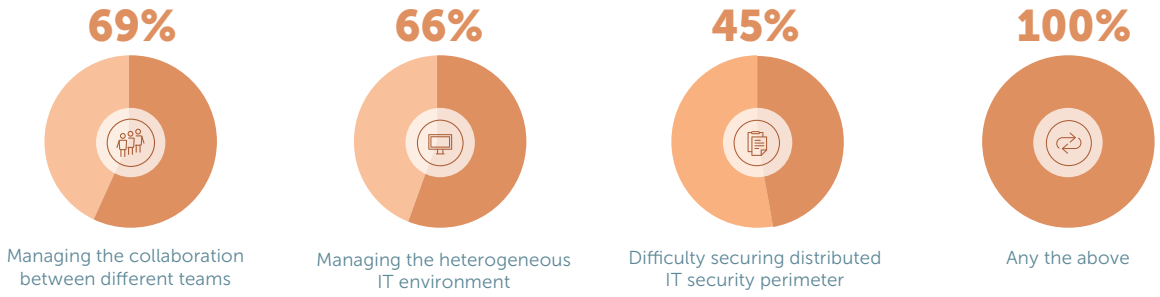
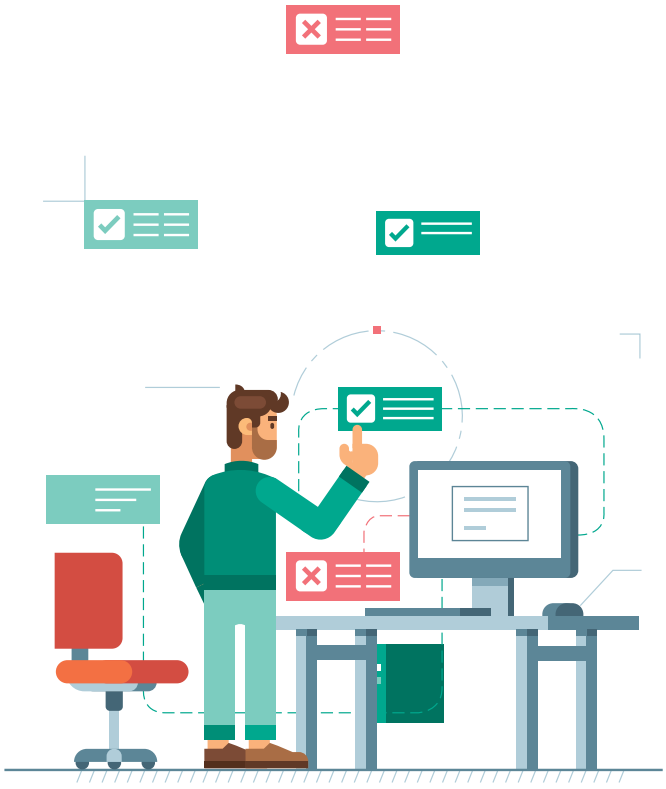


Figure 11: Challenges facing the people responsible for IT in VSBs and SMBs



In terms of specific challenges, data privacy, financial and IT security risk are the top three concerns for both VSBs and SMBs. Data privacy tops the list for SMBs **(57%)** and is the second-biggest concern for VSBs **(52%).** This is to be expected given the current focus around data protection and compliance, stemming from the recent launch of General Data Protection Regulation (GDPR) that hold businesses accountable for the customer information they collect.

It also links back to the remote working trend, as ensuring the privacy and security of data that is accessed from employees' mobile devices is a challenge facing many businesses that allow their employees to work from outside the office. **The result is that 49% of VSBs and 64% of SMBs now have sensitive customer information stored on employees' mobile devices, while 42% of VSBs and 58% of SMBs store customer data in the public cloud, all of which presents security risks.**

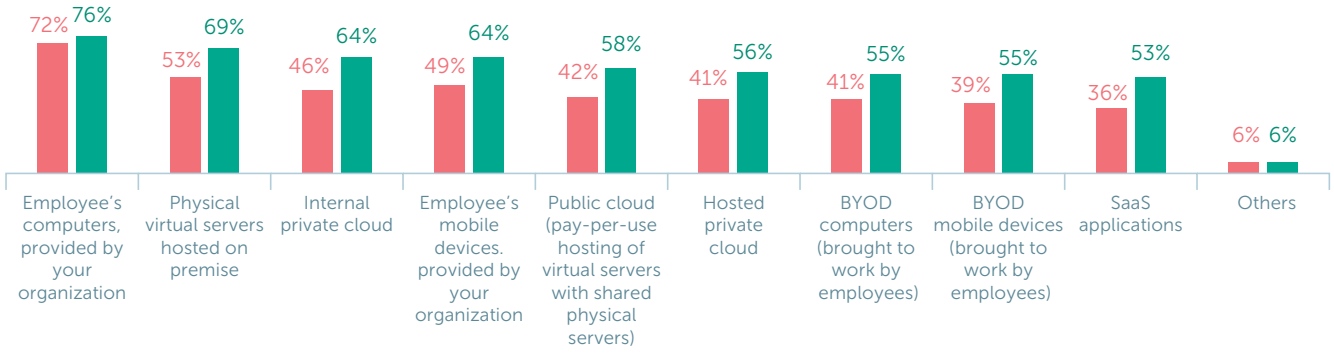


Figure 12: Platforms on which businesses store sensitive customer information

As such, data protection is seen as the number one business challenge faced by both VSBs **(28%)** and SMBs **(26%)**. This is followed by business continuity – the top challenge for **16% of VSBs and 14% of SMBs** – and cloud infrastructure security issues, which one-in-ten VSBs and **13%** of SMBs highlight as their biggest business challenge.

And there are plenty of other risks that are causing businesses concern, **53%** of VSBs are concerned about financial risks and half **(50%)** about IT security risks, while financial risks **(56%)** and IT security risks **(55%)** also round out the top concerns for SMBs.

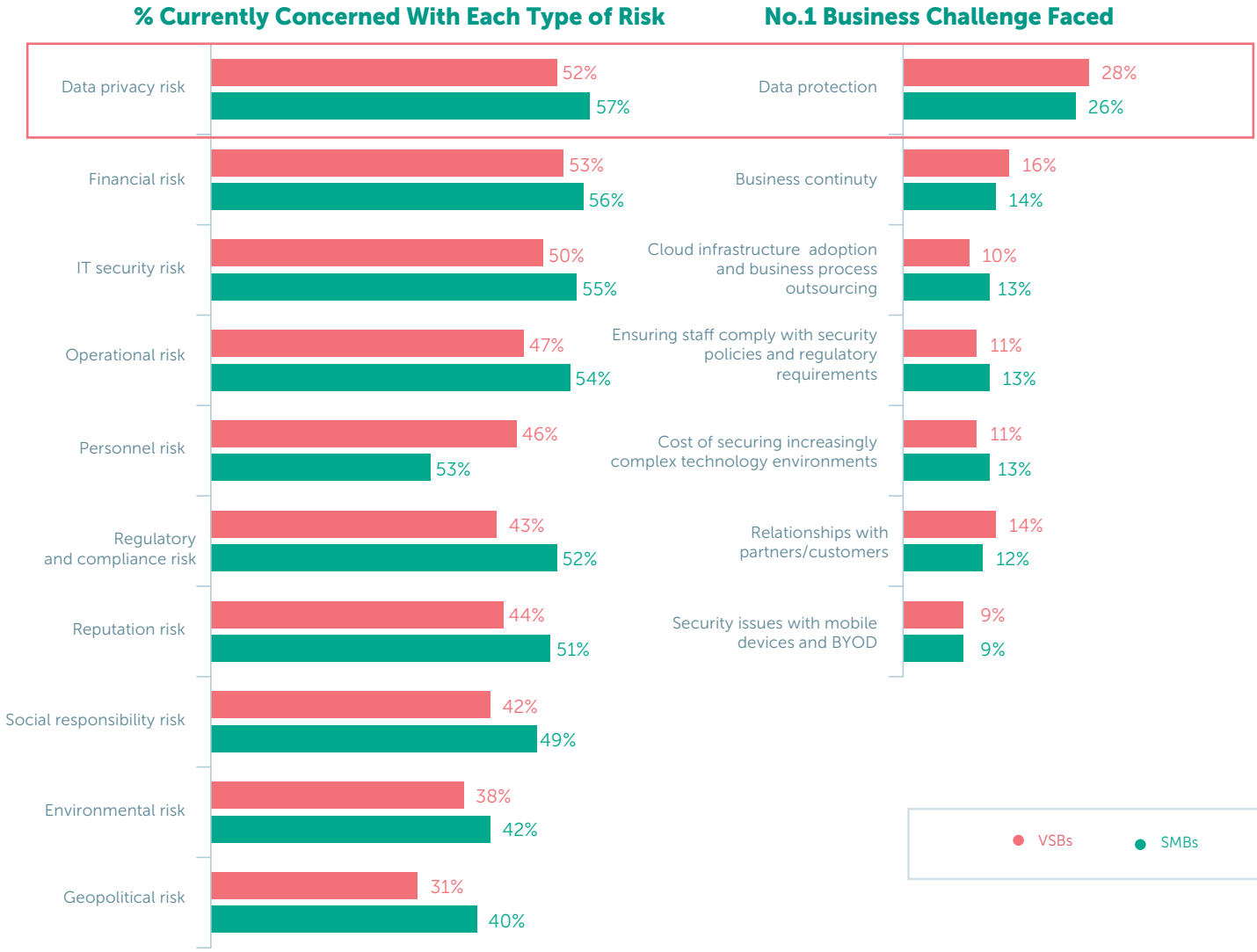


Figure 13: The biggest concerns and challenges facing VSBs and SMBs

Part of the reason for these concerns is a lack of understanding around who is responsible for the security of business services and applications – the organization or its service provider - which can lead to security risks. For example, in businesses with less than 50 employees, the biggest disparities can be seen in office productivity software and team document sharing sites. Nearly two-thirds **(64%)** of VSBs think they are responsible for the security of their productivity software, while just **44%** believe that responsibility lies with the application provider. When it comes to ensuring security for team document sharing sites, just **49%** of VSBs think they are responsible, with **64%** believing it is the responsibility of their provider.

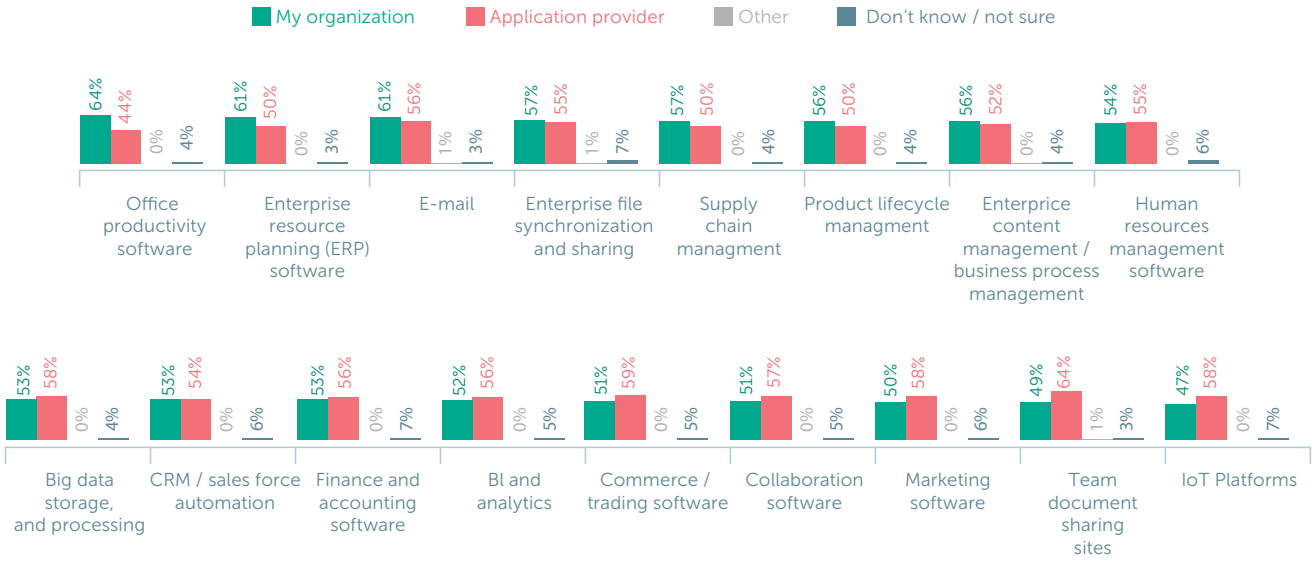


Figure 14: VSBs and the perceived division of responsibility for application security

The pattern is very similar among businesses with 50 to 249 employees, with office productivity software again showing the biggest split regarding who is responsible for security – **74%** of SMBs believe it lies with their organisation, while just **43%** think it lies with the application provider. But there are also some other notable disparities, such as email **(71% vs 49%)**, BI and analytics **(68% vs 41%)** and finance and accounting software **(65% vs 49%)**.

Interestingly, across all business applications, VSBs tend to assign the responsibility of managing security to their provider. In comparison, SMBs believe that this responsibility lies with them in virtually all cases, suggesting that larger businesses are more willing to take accountability for their data security.

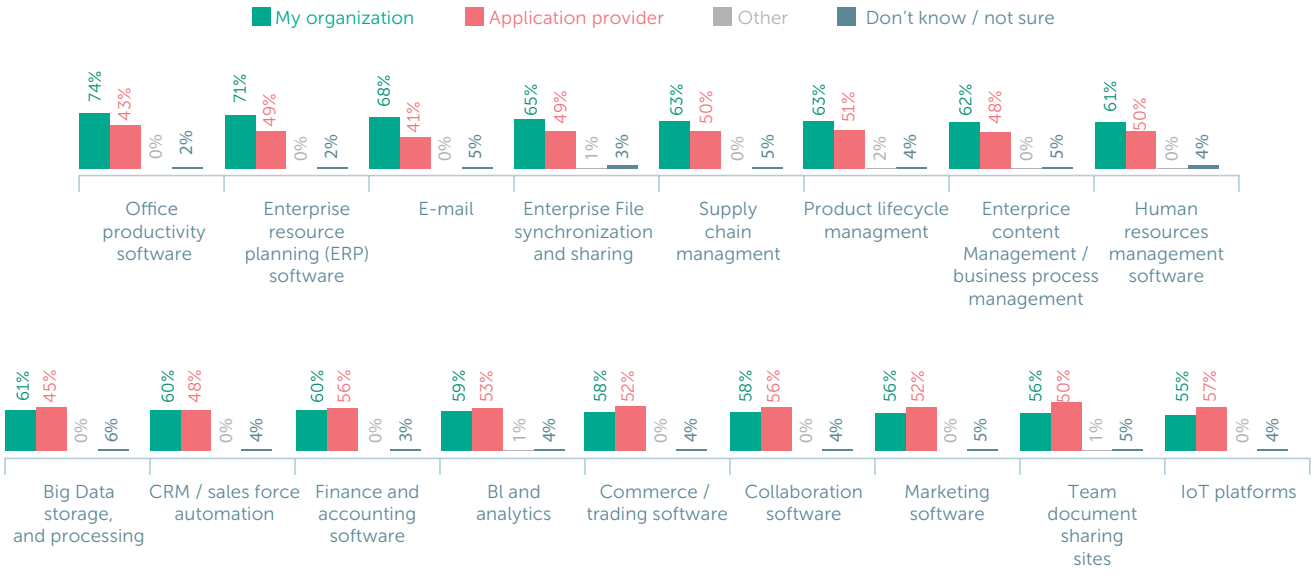


Figure 15: SMBs and the perceived division of responsibility for application security

The bad news for businesses is that security concerns appear to be well-founded. Those making use of cloud solutions (particularly hybrid cloud), have a broader surface area to protect from cyberthreats and so report a larger number of attacks. This is especially true for SMBs, which reported an average 10 security incidents over the last twelve months across any cloud platform, compared to an average of seven incidents among VSBs.

In comparison, those businesses with no cloud only reported seven (SMBs) and six (VSBs) security incidents over the same period. This represents a challenge and a risk for businesses wanting to use cloud as a means of growing or making the transition from VSB to SMB.

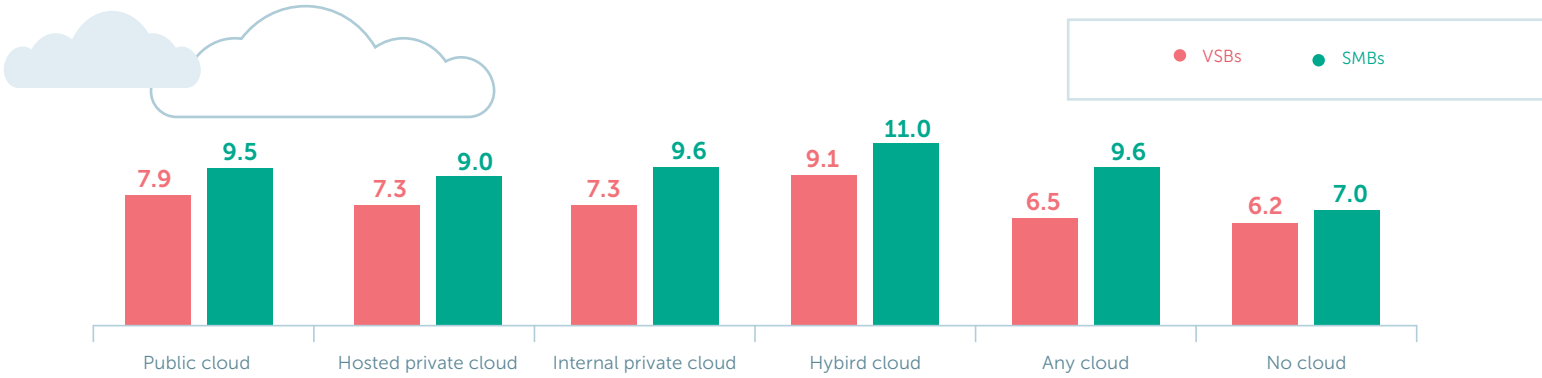


Figure 16: Average number of incidents reported over the last 12 month among users of different cloud types

Cyberattacks related to virtual and cloud infrastructure have also been prominent over the last 12 months, putting businesses at risk as they continue to turn to cloud platforms to support their growth and development.

A large proportion of businesses have experienced these types of attacks in the past year, especially SMBs. Over two-fifths **(42%)** of SMBs have experienced a security incident affecting virtualized environments, while **36%** have experienced an incident affecting third-party cloud services, and **33%** have faced some kind of cyberattack affecting infrastructure hosted by a third-party.

The figures are slightly lower for VSBs – 30%, 23% and 23% respectively – possibly suggesting that smaller businesses are either not at risk, or have a smaller attack surface for hackers to exploit.

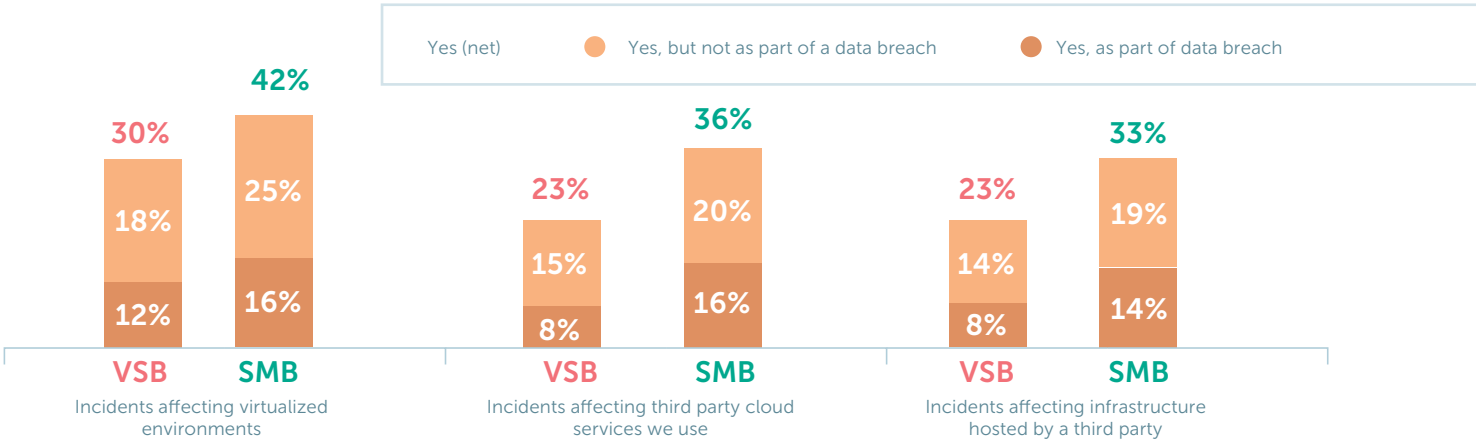


Figure 17: Security incidents affecting cloud and virtual infrastructure

There can be no arguing that the adoption of cloud platforms brings with it some security risks, particularly as a result of increasing infrastructure complexity. Outsourcing security can be one solution, but businesses have to be prepared to view security as a priority, rather than an afterthought.

Conclusion

Clearly, cloud platforms and services are an essential component of any modern business. They give organizations of all sizes the ability to scale and grow their operations without having to spend excessive amounts of money on infrastructure.

Through SaaS-based apps, employees can access important information from wherever they are, significantly increasing the productivity of individuals as well as the company as a whole.

However, for both VSBs and SMBs, there will come a point during their growth when they will be faced with the following dilemma: do they either try to react to security issues as they emerge (often as a result of their growing and increasingly complex infrastructure), or do they make security part of their technology adoption plan at an early stage. Take option one, and businesses face the risk of their security being too slow to keep up.

The latter option can enable businesses to become 'secure by design,' either by establishing an internal ecosystem of experienced personnel, or by outsourcing security to a reliable partner.

Of course, outsourcing still comes with its own risks. However, giving a third-party responsibility for maintaining security can take a huge amount of pressure off businesses, especially those with small and potentially inexperienced IT teams.

Failing to adapt, and continuing to manage IT security in the same way, will present in increased amount of cybersecurity risks. Today's threat landscape is constantly evolving and businesses have to be prepared to do the same.

Whichever approach businesses take, they need appropriate solutions that empower them to maintain the necessary levels of security as they grow. Kaspersky Lab has a range of solutions that can accompany businesses all the way through their development – from start-ups or small companies to more mature medium-sized businesses – and protect them against today's cyberthreats.

KASPERSKY lab