analysys mason

Perspective

Small and medium-sized business (SMB) cyber-security challenges and solutions

August 2022

Tom Rebbeck

Contents

List of figures

1. SMBs are coming out of the pandemic ready to grow, but face new security challenges

The impact of the pandemic is receding, and small and medium-sized businesses (SMBs) are looking to invest to improve their chances of growth.[1] SMBs face new challenges in this quest. Compared to 2019, hiring is harder, and a much greater share of the workforce will be working remotely. SMBs are investing increasing amounts in IT to help to solve these problems.

SMBs' cyber-security requirements are changing as part of these broader shifts. The increased volume of threats, use of cloud applications and numbers of employees working from home are all making SMBs more vulnerable.

Therefore, SMBs need to update their cyber-security solutions. However, although spending on security products is increasing, many still do not have sufficient protection.

This report explores how SMBs are emerging from the pandemic, and how their business and technology priorities are changing. It also examines how these changes relate to the threats that SMBs face and provides recommendations for how SMBs can protect themselves.

Data in this paper is taken from our surveys of businesses and also from our forecasts of spending by companies on all IT services, including cyber security.

Extensive surveys support our understanding of the SMB market

An ongoing series of surveys support our understanding of SMBs' activities. These surveys ask IT managers in SMBs about their current technology usage and future requirements, as well as more general questions about business outlook and priorities.

We conducted our most recent survey in Q1 2022. It included 1150 SMBs in the US, Germany, UK and Singapore across a range of vertical industries. Most of the survey data in this report is taken from this survey, but we also incorporate some data from previous studies, which included a wider range of countries.[2]

2. SMBs are adapting for a post-COVID world

Businesses came out of the pandemic looking to invest and expand. SMBs from our sample of countries were typically operating at around 80% of their full capacity in Q1 2022 (Figure 1). They are looking to grow by hiring staff, adding sites and investing more in IT.

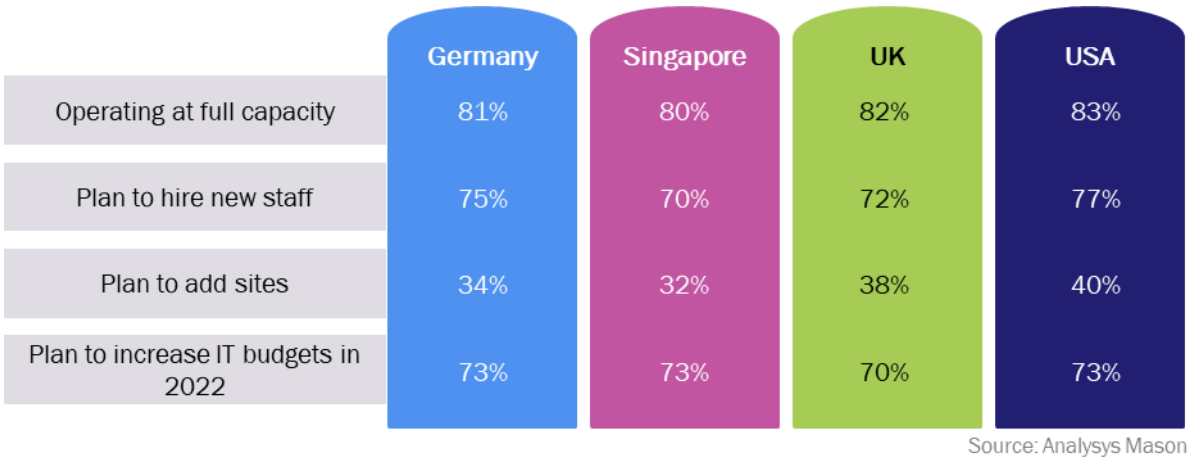
The challenge in hiring and retaining staff, and adapting to new ways of working, are driving spend in IT services, as well as the traditional aims of improved productivity.

---

1 We define SMBs as companies with up to 1000 employees. Within this category, we include small businesses (or SBs) with up to 100 employees, and medium-sized businesses (MBs) with 100–1000 employees.

2 Surveys conducted since 2019 have included SMBs in Australia, Canada, China, France, India, Indonesia, Saudi Arabia, and South Africa, as well as SMBs in Germany, Singapore, the UK and the USA.

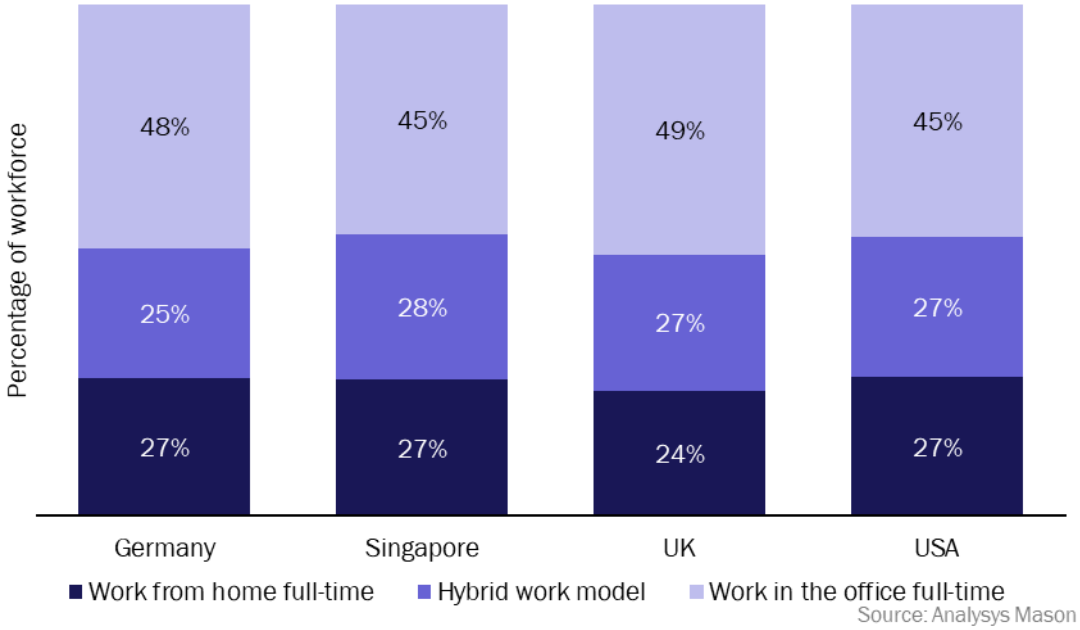
Figure 1: Overview of the key results of our survey, Germany, Singapore, UK and USA, Q1 2022



The levels of remote working will be permanently twice those of the pre-pandemic era

The pandemic has permanently changed the way many SMBs work. In Q1 2022, after restrictions on movement had been lifted in most places, around 50% of employees were working from home at least part of the time (Figure 2).

Figure 2: Work patterns, by type, Germany, Singapore, UK and USA, Q1 2022[3]



In the longer term, that share is expected to drop slightly, but companies expect that 40% of their employees will continue to work remotely for at least some of the time. Remarkably, this level of remote working is similar in all of the countries in our study, despite cultural differences between the four countries. According to the results, the number of employees that will working remotely in 2023 will be more than double that of the pre-pandemic era.

3 Question: "What percentage of your company's employees currently work at home and what proportion of your employees do you expect to work from home vs. work in the office in the next 12–24 months?" n = 1149.

Although remote working has been widespread for over 2 years, SMBs are still adjusting – for example, making new investments in IT – and will continue to do so for the next 12–24 months.

SMBs are again investing for growth

The main priorities for SMBs in 2022 are focused on revenue growth. Most SMBs performed significantly better in 2021 than in 2020 – the majority of firms saw revenue increases. Again, the results for the four countries in our survey was similar, despite the varying severity of the pandemic by country and the different levels of government support available to SMBs. There is some bias in this sample; only firms that had survived the pandemic were able to complete a survey, but it does suggest that for the companies that are still trading, the situation had improved considerably since 2020.[4]

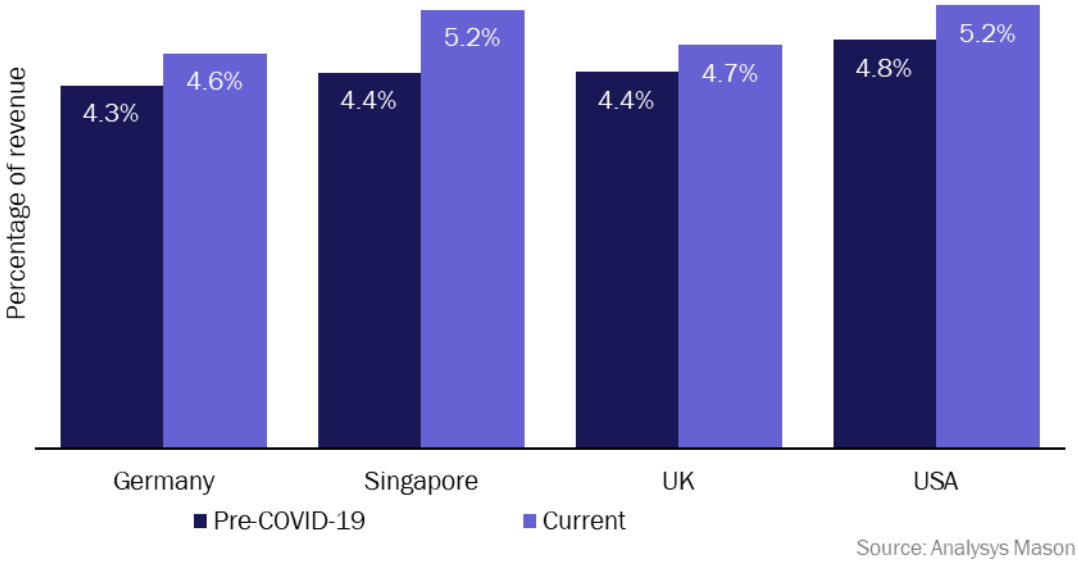
Businesses expect this growth to continue and, to support expansion plans, they are looking to both hire more staff and expand into new locations. Plans do look different by country – SMBs in the USA are looking to grow more rapidly than those in Singapore – but the trend is similar in all countries.

SMBs' investment priorities are changing

The business priorities of SMBs for the future also reflect the key points about growth and new ways of working. The priority areas for businesses do vary by region, but investment in people and in remote working feature prominently. These priorities can also be seen in the technology priorities of SMBs. The highest priority in almost all countries is to ensure that IT can be managed and supported remotely. Businesses are also looking to improve fixed and mobile connectivity for remote workers.

We can see from the survey responses that the changes in SMB priorities appear to be reflected in their IT budgets (Figure 3). Expressed as a percentage of annual revenue, SMBs in all countries in our panel have sharply increased IT spend. Interestingly, that increase is steepest in Singapore (+0.8 percentage points), which compares to around +0.3 percentage points in the other countries. In terms of spend as a percentage of revenue, SMBs in Singapore will match the level of that of their US counterparts.

Figure 3: IT budget as a percentage of annual revenue, Germany, Singapore, UK and USA, Q1 2022[5]

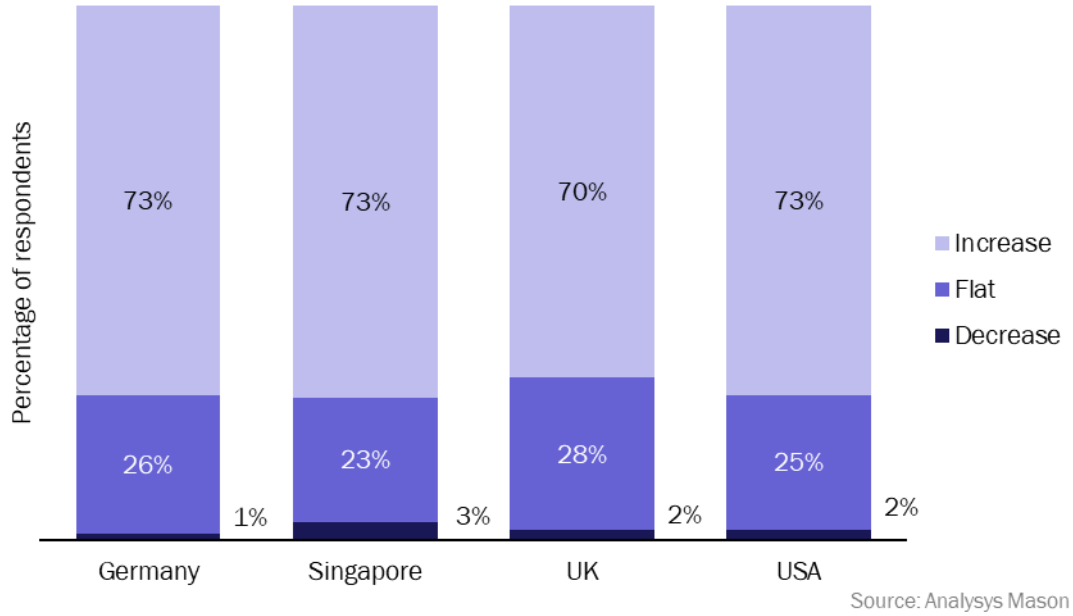


4 The survey was completed when firms were aware of the war in Ukraine and continued supply side challenges. However, any recession or slowdown is likely to be relatively mild compared to the decline during 2020.

5 Question: "What proportion of your company's annual revenue was allocated for your overall IT budget prior to the COVID-19 pandemic, and what proportion is currently allocated?" n = 1149.

Most SMBs expect spend on IT services to increase further (Figure 4). A negligible number expect IT budgets to shrink, while nearly three-quarters expect to have bigger IT budgets.

Figure 4: Expected changes to IT budgets over next 12 months, Germany, Singapore, UK and USA, Q1 2022[6]



3. The threat landscape for SMBs is changing

SMBs are investing in all areas of IT, including cyber security, but many are still not investing enough in security to protect themselves. Since the start of the pandemic, SMBs have faced an increased number of cyber attacks, while the changes to ways of working (such as employees working remotely) may make them more vulnerable. SMBs, the service providers that support them and the vendors that develop security solutions need to explore how more can be done to protect SMBs.

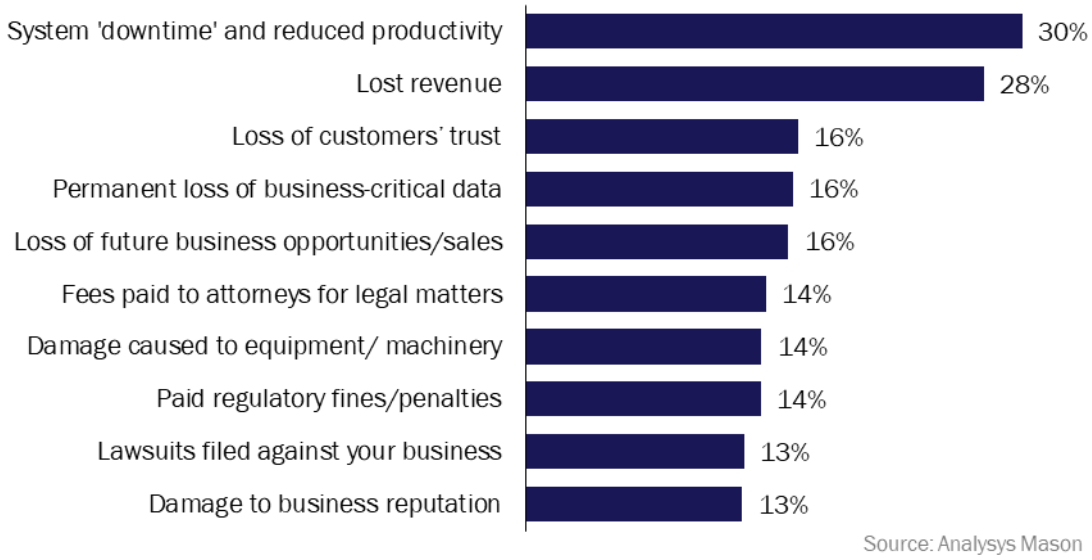
Successful cyber attacks have a disproportionate impact on SMBs

The impact of a cyber attack is potentially more damaging to an SMB than it is to a large business. High-profile breaches in large enterprises may make headlines, but rarely affect the long-term viability of the business. In contrast, an attack on a small business can threaten its very existence. This was true before the pandemic, but changes working patterns since the start of 2020 plus the rise in the number of cyber attacks, increase the risks for SMBs.

Even if an SMB can survive the short-term impact of a security attack, other consequences can have a negative impact on the company's ability to do business in the longer term. Figure 5 provides data from companies that had suffered a security breach in the past 12 months but managed to remain in business. Businesses were hit by a loss of customer trust and reputational damage in addition to the direct financial impact.

6 Question "Over the next 12 months, how do you anticipate your company's IT budget will change?" n = 1149.

Figure 5: Impacts on SMBs suffering a security attack in the last 12 months



4. Most SMBs are not doing enough to protect their business

SMBs are aware of the changing nature of threats to their companies. Investment in security has increased – for example, more than a third of SMBs have deployed additional security solutions in the last year (Figure 6), making it one of the most popular areas for investment due to the pandemic.

Figure 6: Measures taken by SMBs to support remote employees, Germany, Singapore, UK and USA, Q1 2022[7]

	Germany	Singapore	UK	USA
Deployed additional security solutions	42%	33%	36%	36%
Increased mobile data allowances for company-provided mobile plans	32%	34%	41%	46%
Purchased new laptops	59%	44%	50%	45%
Held regular well-being check-ins with employees	37%	45%	48%	42%
Offered financial support for home broadband	31%	32%	36%	40%
Increased VPN capacity/seats	36%	34%	28%	35%
Purchased mobile phones	39%	32%	36%	34%
Enforced added security training measures	38%	34%	32%	31%

7 Question: "What measures has your company taken to help support your employees working from home?" n = 1149.

Despite this additional investment, IT managers still do not feel that they have adequate security. Only 22% of those surveyed felt they were 'extremely well protected' against cyber-security attacks and threats from external parties.

SMBs are also open to receiving more help with security from service providers. Around a third would like additional help from their service providers in upgrading security (Figure 7). In Germany and the USA, upgrading security is the mostly commonly cited area with which services providers could offer assistance.

Figure 7: Services cited as the most helpful by SMBs, Germany, Singapore, UK and USA, Q1 2022[8]

	Germany	Singapore	UK	USA
Upgrade security	27%	31%	31%	38%
Provide remote IT support	22%	37%	34%	37%
Offer flexible payment terms	24%	27%	31%	37%
Offer complimentary subscriptions	16%	28%	32%	32%
Suggest IT solutions	24%	31%	32%	35%
Business continuity planning	25%	31%	35%	34%

Many SMBs do not have basic security products in place

Looking at the security solutions that businesses have in place supports the view that additional investment is required. The take-up rate of even basic security products is low (Figure 8). The most commonly adopted service, endpoint protection, is only used by 67% of SMBs. Less than half of SMBs have any form of mobile security.

The figures do improve as business size increases. For example, for medium-sized businesses (that is, firms with 100–1000 employees), three-quarters of firms are using endpoint production and two-thirds are using email security.

Figure 8: Top 5 security solutions deployed by SMBs[9]

	Germany	Singapore	UK	USA
Endpoint protection – including anti-virus, anti-spyware, anti-malware	62%	70%	69%	67%
Email security – including anti-phishing, secure email gateways, email encryption	61%	67%	64%	61%
Firewalls and unified threat management (UTM) solutions – devices/software	48%	54%	50%	48%
Web security – including URL filtering, DNS protection, company policies enforcement	50%	45%	48%	39%

8 Question: "Please rate the following services from IT or telecoms suppliers in terms of how helpful they would be to your business during the next 12 months?" n = 1149

9 Question: "Which of the following security solutions does your company currently use or plan to start using or upgrade in the next 12 months?"; n = 1149.

	Germany	Singapore	UK	USA
Mobile threat defense (MTD) – prevents app-, network- and device-based malicious attacks	42%	41%	47%	45%

However, the overall figures are concerning because they suggest that many firms do not have even the simple security products in place.

Many SMBs are not correctly managing the security products they are using

Having the correct mix of security products is only part of a protection strategy. These products also need to be managed by people with the right skills. Again, the data on SMBs is troubling.

Only a minority of SMBs have either internal security specialists or are working with a third party to manage security. This means that a large number of SMBs either have no security products in place, or these products are managed by non-specialist staff.

Few SMBs perform basic security testing or vulnerability assessments or have a plan in case their business is attacked. More than 30% of businesses admit to having only informal processes in place to manage security. We suspect the actual figure is higher as the IT managers who completed the survey may be unwilling to admit they do not have formal processes in place.

The results are better for medium-sized businesses (100–1000 employees) than for smaller firms. However, these results give plenty of cause for concern. **Overall, we would estimate that only around a third of SMBs have adequate cyber-security protection.**

There are reasons for this lack of protection – survey respondents point to a lack of adequate cyber-security expertise and understanding of security options, limited budgets and informal security management as roadblocks. Given what is at stake though – and for SMBs this literally means the survival of the business – more attention should be directed at resolving these issues.

5. Spend on security by SMBs is on the rise

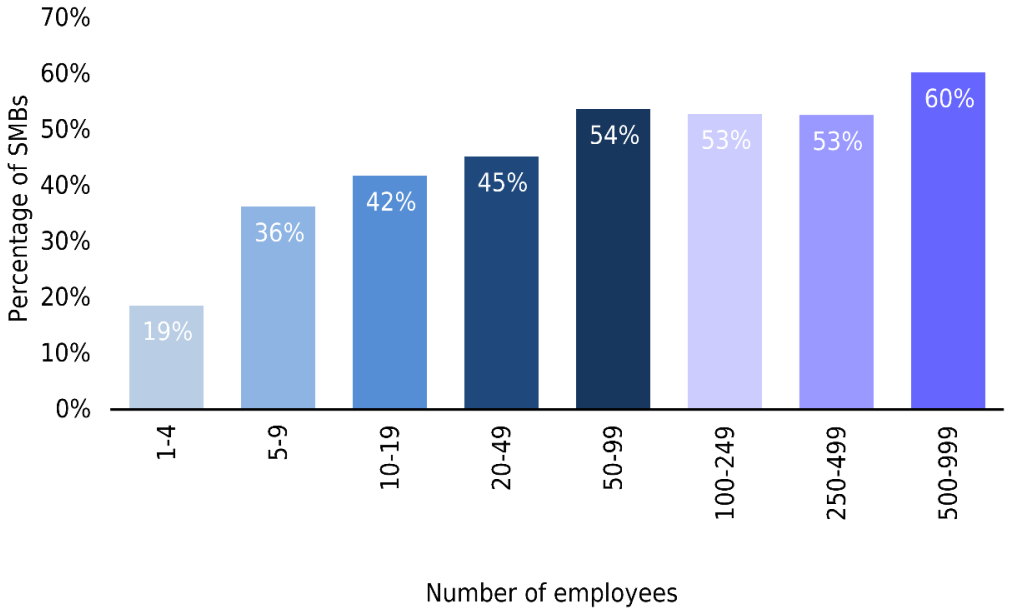
In 2021, SMBs worldwide spent USD68 billion on security solutions and that figure is expected to increase to USD105 billion in 2026.

More than **40% of the businesses in our recent survey plan to increase their spending on security solutions** year-on-year in 2022. Nearly a fifth of them are budgeting increases of more than 20%.

Much of this increase in spend will be made through service providers

We also see a significant rise in the share of SMBs that are working with managed service providers to help address IT issues (Figure 9). The pandemic caused many changes to the IT requirements of SMBs, and many firms could not manage these themselves. However, it is notable that the smallest firms were still unlikely to work with MSPs. In part, this is because smaller firms have less complex IT requirements, but we suspect that many of these smaller firms are not taking advantage of services that are available to them.

Figure 9: Percentage of SMBs that started/increased their use of managed services in response to the COVID-19 pandemic, all countries surveyed



6. Recommendations for SMBs

SMBs, even the smallest of businesses, can take a variety of measures to improve their data security, including the following.

- **Increase spending on security.** The financial damage of a security breach can be disastrous for a small firm, and yet many SMBs only assign only a limited budget to IT security. 35% of firms cited inadequate security budgets/security vendor solutions priced beyond their budgets as a key challenge to having effective cyber-security capabilities. Firms should consider whether they are spending enough on cyber security.

- **Create formal processes for managing security.** Too many SMBs (63%) do not have documented procedures in place to act quickly in case of an IT security breach, 70% do not conduct regular security assessments, and 67% rely on informal, ad hoc processes to manage their security. In addition, the lack of formal processes is more commonplace for smaller businesses who often have more difficulty managing a breach. An SMB needs to develop and follow formal processes for assessing and managing its security systems.

- **Work with third parties, such as MSPs, to provide their security**. One-third of SMBs already have security managed by a third-party provider. SMBs have increased their usage of third parties to provide security in the past few years and are open to buying additional security services from their IT, telecoms or technology suppliers. 74% of SMBs reported they would find it very helpful if their technology providers would help them upgrade security to cover new problems (for example, working from home, collaboration, BYOD). Obtaining support from third parties is a good idea for many firms for various reasons, but most importantly it provides them access to experienced cyber-security professionals which they otherwise would not be able to afford, as well as expert advice on which solutions would best suit their business and ongoing support and training which is critical. SMBs can benefit from a professional assessment of their

cyber-security situation. Security vendors and solution providers can offer strategic recommendations on security solutions that are the best fit for SMBs based on their size, type of operations and business objectives.

- **Consider how security needs have changed since the start of 2020 when making deployment decisions.** Many businesses have employees that work from home and will continue to do so post-Covid. Many businesses have changed how they sell or deliver services. These changes have altered the potential threats that a business faces – security solutions and policies should be reviewed and potentially updated.

- **Consider how future business growth plans will affect security needs.** 90% of SMBs interviewed in our most recent study are reporting a more optimistic outlook for their company's prospects and are focusing on growing their business. SMBs' business priorities for the next 12 months revolve around supporting remote workers, rehiring/retaining employees, funding more digital transformation projects and increasing their customer share of wallet. The majority of businesses (74%) reported they are planning to hire new employees. New security deployments must be scalable and SMBs should look for solutions packaged with onboarding and training services.

- **SMBs should consider whether customer data is sufficiently protected.** Security is not only about protecting an SMB's data, but also about protecting customers' data. Many businesses collect information on their customers in the course of doing business. Some of this data is financial (for example, credit card information) but much is not (for example, details of past orders or preferences). SMBs are highly cognizant of the fact that a data breach against their customer data can be catastrophic. Indeed, 70% of SMBs felt that "protecting customers' privacy and financial data" was the most important goal impacting their cyber-security plans. Companies have a duty to protect all of this information and need to consider if they are sufficiently well protected to do this.

7. Check Point's security solutions for small and medium-sized businesses

Check Point Software Technologies provides governments and enterprises with cyber-security solutions that are designed to prevent malware, ransomware, phishing and much more. The solutions span network security, IoT security, endpoint security, cloud security, mobile security, data security and security management.

Check Point Software offers a unique, comprehensive security solution suite specifically built to aid SMBs and MSSPs in their fight to protect networks and devices against cyber attacks The Check Point SMB Security Suite delivers security in a series of simple and affordable solutions that protect SMB employees, networks and data from cyber attacks.

SMB Security Suite is designed to provide SMBs with the security that they need, right out of the box. This spans network security, cloud security, as well as mobile and endpoint security, including market-leading technology to help to protect SMBs from security risks.

Check Point SMB Security Suite combines the following best-of-breed security technologies from Check Point into a single offering.

The **Quantum Spark Next Generation Firewalls for SMBs** feature best-in-class threat protection, are easy to deploy and manage, and integrate communication and security into an 'all-in-one' security gateway solution.

They also offer:

- threat prevention performance up to 2 Gbps
- flexible connectivity options: Wi-Fi, Gigabit Ethernet, DSL, Fiber and 4G LTE
- automated easy installation in 60 seconds or less with no onsite technician
- simple Web UI for automated threat management from a single screen
- mobile app for management on-the-go.

The **Harmony Email & Collaboration** security solutions provide complete protection for SMBs' collaboration and file-sharing apps and:

- block advanced phishing, malware and ransomware attacks before the inbox
- protect sensitive business data (DLP) from leaving the organization
- prevents account takeover and keep users safe
- secure all lines of business communication, including Slack and Teams
- are the first solution to implement API, machine learning and AI for email security.

Today more than ever, endpoint security plays a critical role in enabling a remote workforce. **Harmony Endpoint** provides comprehensive endpoint protection at the highest security level, crucial to avoid security breaches and data compromise. The solution offers:

- complete endpoint protection preventing the most imminent threats to the endpoint
- automates 90% of attack detection, investigation and remediation tasks
- efficient, cost-effective and fully flexible to meet security and compliance requirements.

While employees are increasingly accessing corporate data from their smartphones, businesses are exposed to breaches more than ever. **Harmony Mobile** delivers complete protection for a mobile workforce and is simple to deploy, manage and scale. The solution:

- protects corporate data across the mobile attack surface: apps, networks, and OS
- offers scalable and easy-to-manage security for any type of mobile workforce
- enables users to adopt it quickly with zero impact on user experience or privacy.

Summary

Check Point understands that running a small business requires dealing with an immense number of issues from competition to scheduling, payroll, banking, and much more. The Check Point SMB Security Suite leverages industry leading threat prevention, automation and ease of use, to deliver simple and affordable security solutions that protect SMB employees, networks and data from cyber attacks. This enables you to focus on making your business successful by leveraging the security expertise of Check Point and your managed service provider.

For more information on Check Point and its SMB security solution, visit www.checkpoint.com/solutions/small-medium-business-security/.

About the author

Tom Rebbeck (Partner) leads Analysys Mason's *Operator Business Services and IoT* research practice drawing on more than 20 years of experience in the telecoms sector. He is based in our London office, but works for clients worldwide. Tom is a specialist on the Internet of Things (IoT) and other enterprise services and has written widely on the role for operators as telecoms markets develop. As well as published research, he has worked on projects for a range of clients – including operators, regulators, industry bodies and vendors. Many of these projects have been supported by original research, such as expert interviews and customer surveys.

MESSAGE FROM THE SPONSOR

About Check Point Software

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber-security solutions to governments and corporate enterprises globally. Its solutions protect customers from sophisticated 5th-generation cyber attacks with an industry-leading catch rate of malware, ransomware, and other types of attacks. Check Point offers its multi-level security architecture, Infinity Total Protection with Gen V advanced threat prevention, which defends enterprises' cloud, network and mobile device held information. Check Point provides the most comprehensive and intuitive one point of control security management system. Check Point protects over 100 000 organisations of all sizes.

Schedule a demo to learn how Check Point can help you to protect SMBs from any threat, anywhere, with innovative and effective network security. Sign up today at www.checkpoint.com/quantum/next-generation-firewall/small-business-firewall/