Report

Cyber security for SMBs: Navigating Complexity and Building Resilience

A global study of SMB's perceptions and experiences of cyber security and how to navigate the changing landscape.

Sage

Table of Contents

Foreword by Ben Aung – Chief Risk Officer at Sage

Collaboration and clear guidance can empower SMBs' cyber security

Small and Medium-sized Businesses (SMBs) should be able to remain focused on profitability and growth while having peace of mind that their cyber defences are strong enough. Collaboration among governments, industry bodies, cyber security firms, and tech companies is crucial to simplify cyber security for SMBs, enabling them to confidently navigate and enhance their cyber resilience in today's complex landscape.

However, the lack of coherent and consistent guidance for SMBs makes protecting themselves, educating employees, and accessing the right tools to successfully manage their cyber risks and thrive in the digital economy, even more difficult.

SMBs are the backbone of our economies and critical to the global supply chain. The technology innovations and interconnectedness which have unleashed the productivity of businesses also pose potential cyber security risks. These risks can be even more acute for SMBs.

If the last decade has taught us anything, it is that doing cyber security properly is hard. Every business with a digital footprint is a target for cybercriminals and the size of an organisation does not shield it from the attention of attackers. Ransomware attacks are no longer the preserve of large enterprises and many SMBs fall victim to them, with potentially devastating consequences. A lack of accurate reporting means it is impossible to quantify the true impact of ransomware on SMBs, but our research shows one in four SMBs experienced multiple cyber security incidents in the last year alone. Therefore, it is not surprising to see SMB decision-makers are taking cyber security seriously. Our research also shows two-thirds are prepared to spend more to ensure better security for their business. Meanwhile, 70% of respondents say cyber threats are a major concern for them.

Yet, despite a desire to secure their business against attacks – as born out in the data in this report and conversations with our SMB customers – there are challenging factors to overcome. Comparatively small budgets compared to larger organisations mean SMBs must prioritise their security and tech investment to get the best value for money.

The insights from this report should spur action across society, government, and businesses. Together, we can work towards simplifying cyber security for SMBs, ensuring a safer digital environment for all.

Executive summary

48%

of SMBs have experienced a cyber security incident in the past year

91%

expect cyber security investments to increase or remain the same in the coming year

69%

of SMBs say cyber security is part of their culture, but most only discuss when something changes or goes wrong internally

This study reveals:

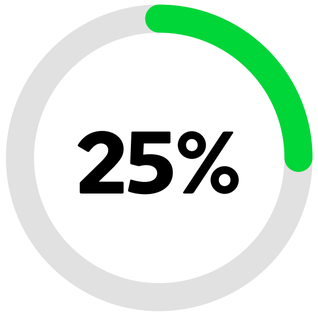
- How SMBs across key global markets are experiencing the evolving cyber security landscape. 48% have experienced a cyber security incident in the past year.
- There is an underlying, possibly misplaced, confidence about managing cyber security. 76% say they regularly review it, although 7 in 10 see threats as a major concern.
- The constantly evolving threat landscape is keeping SMBs up at night. The biggest challenge for over half (51%) is keeping on top of new threats, followed by making sure employees know what's expected of them (45%), educating staff about cyber security (44%), and cost (43%).
- There are mixed messages around cyber security culture. Two-thirds say it is part of their culture but only 4 in 10 discuss it regularly.
- SMBs are prepared to invest more in cyber security. But they require help to fill knowledge and education gaps, and continue to be hindered by ineffective and unclear guidance. 52% want support with education and training.
- They are calling for this education and support to come from cyber security companies (56%), governments (45%), and trusted tech partners (43%). This can reduce the burden on SMBs with limited resources to protect themselves and enables them to improve their cyber security capabilities.

Grappling with the cyber security landscape

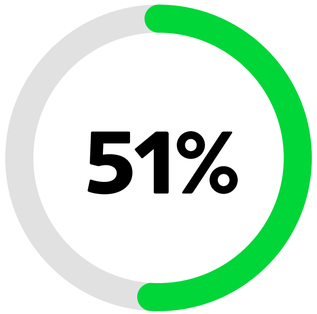
Grappling with the cyber security landscape

Nearly half of the survey participants have faced cyber incidents over the past year, indicating that what is reported is just the tip of the iceberg. While these businesses are acutely aware of the cyber threats they face, they often grapple with a multitude of challenges in safeguarding themselves against what must feel like an avalanche of new vulnerabilities and risks appearing every week.

Topping the list of challenges is keeping on top of new threats, with 51% of SMBs providing this response — a figure that increases to 54% for UK-based SMBs. Closely following are other pressing concerns, including ensuring employees understand what is expected of them (45%), educating employees about cyber security (44%), and cost (43%). These statistics underscore that while a significant proportion of SMBs recognise they are under threat they don't necessarily know what to do about it. They need help to cut through the noise about new threats, supported with simple, actionable advice that allows them to focus on what is relevant to their business.



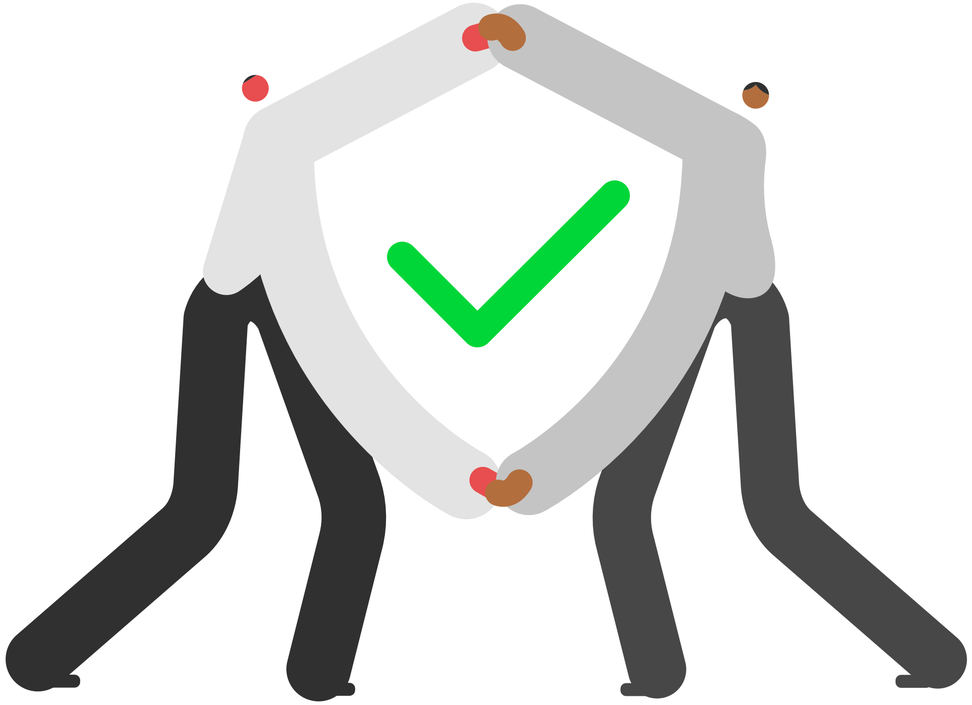
of SMBs have experienced more than one cyber security incident in the past year



say keeping on top of new threats is their biggest challenge

Championing cyber security for SMBs

Championing cyber security for SMBs



> We must bring a human touch to cyber security. Our goal is to simplify, demystify, and remove the fear around what often appears complex and daunting to SMBs. In this way, **we empower them to integrate cyber security into their everyday activity and discussions**, build cyber resilience against cyber threats and futureproof their businesses.

Sophia Adhami
Director Cyber Security Engagement, Sage

SMBs often have limited IT resources and competing demands. Without fit-for-purpose guidance and support, it becomes significantly harder for them to make informed risk management choices about where they invest and what risks they can live with, based on their industry and business context.

It won't be clear for many how a small number of carefully considered cyber security controls can help mitigate the vast majority of attacks they face. We are often told cyber security is about "getting the basics right" but what constitutes the 'basics' is often misunderstood. SMBs need to decide what basic security controls are right for them and this needs to be informed by a blend of internal knowledge and external advice.

Cyber security fundamentals

19% of SMBs depend entirely on what they understand as basic controls. However, even what we dub as “basic” cyber security measures can be complex to set up.

The foundational aspects of cyber security - like system patching, backing up data, access controls, two-factor authentication, asset oversight, and security monitoring - can still require specialist skills and tools to implement and operate.

It’s notable that 46% of SMBs don’t employ firewalls, even though 84% claim familiarity with them. On a global scale, 42% neglect to backup critical data. Intriguingly, UK SMBs (62%) are more diligent in this regard compared to their US counterparts (55%).

SMBs exhibit less confidence when confronted with security jargon. Concepts like end-to-end encryption, ransomware, Bring Your Own Device (BYOD), and endpoint detection are the least well understood among the SMB community.

SMBs must grasp how to choose and employ basic measures effectively and know when and how to complement them with more advanced controls, where that makes sense for their organisation.

19%

of SMBs rely solely on basic controls

58%

of SMBs backup their data

Navigating remote work security

In today's landscape where remote and hybrid work models are now commonplace, SMBs recognise the need to safeguard business conducted outside the conventional workplace environment.

73% have implemented systems to facilitate secure work from home, and for 63%, these systems are distinct from their in-office security. However, in the absence of dedicated IT or cyber security experts, there are valid concerns regarding SMBs' ability to tackle specific remote working cyber security risks.

While 82% have adopted some form of security control, only 57% closely monitor remote work security. Among those with a designated plan or process for tackling remote working risks, 25% confess that it's not universally adhered to. It's noteworthy that a considerable 71% of U.S. SMBs monitor remote work security closely, surpassing the global average. Yet, in the UK, only 57% differentiate between office and remote work security — a figure significantly lower than the 78% observed among French SMBs.

82%

of SMBs have a process in place to manage cyber security risks of remote workers

25%

of those with a process in place acknowledge not all adhere to it

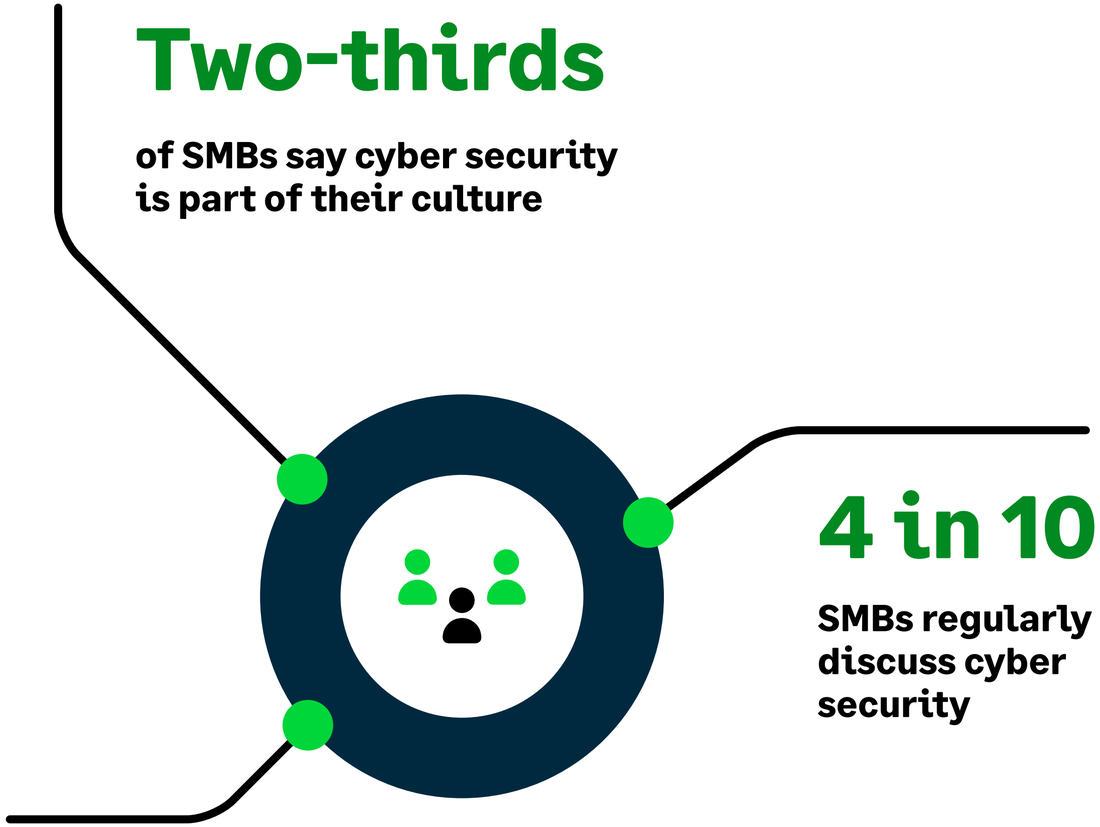
Nurturing a proactive cyber security culture

Nurturing a proactive cyber security culture

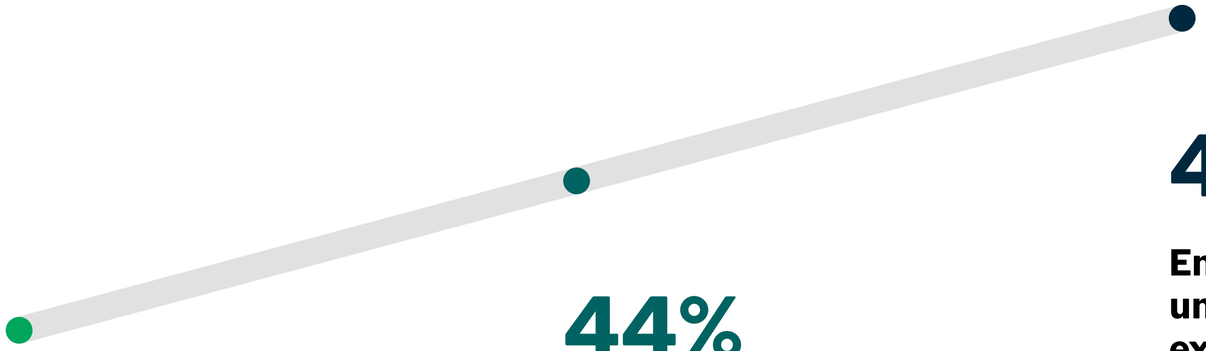
Major enterprises have long understood that securing a business requires a robust cyber security culture to complement their technical controls. When executed well, adopting a people-centric cyber security strategy — where businesses empower and trust employees to consistently make the right security decisions — can actually offset the need for expensive or burdensome security controls. However, for SMBs, there seems to be a disconnect between their perception of what a good security culture is and the actual practices within their organisations.

Two-thirds of SMBs believe cyber security is woven into their company culture. This is particularly evident among South African, Australian, and U.S. SMBs. However, only 4 in 10 SMBs routinely discuss cyber security, with 16% addressing it only after something has gone wrong. 11% of micro enterprises admit to never discussing cyber security at all.

There are numerous budget-friendly ways SMBs can improve their cyber security culture. Practices such as managers leading by example, using educational tools to increase knowledge, making things as easy and intuitive as possible for employees (especially reporting anything suspicious, such as phishing emails) and just talking about cyber security regularly will all make a big difference and reduce the stigma of complexity around cyber security topics.



Most common cyber security challenges



43%

Understanding what security is needed

44%

Educating employees about cyber security

45%

Ensuring employees understand what is expected of them

In today's digital realm, cyber security hurdles are a constant reality for businesses like ours. We face daily data breaches, phishing attempts, ransomware attacks – it's a maze out there. As a small business, juggling protection and growth is a real challenge. The cyber world is a puzzle we can't ignore. Safeguarding while advancing is the name of the game, and finding solutions that fit our size is a must. In this journey, a helping hand from tech companies and government support is crucial. With their help, we can navigate this intricate landscape with more confidence.

Lynne Pace
CFO & VP of Finance for Danson Construction

Pioneering cyber security preparedness

Pioneering cyber security preparedness

Cyber security requires ongoing investment — there aren't any silver bullets or miracle solutions. Increasingly, cyber security is ‘built in’ natively to technology, such as cloud hosting or operating systems, and emerging technologies, such as AI tools, show great promise, but also potentially introduce new risks and new costs. To be effective and stay ahead of cyber threats, organisations of all sizes need to plan their investments carefully, often maintaining or increasing their spending levels, while looking for opportunities to achieve good security outcomes more efficiently.

This is reflected in our research, which reveals an overwhelming 91% of SMBs anticipate their investment in cyber security will increase or remain the same in the next year. Notably, SMBs favour suppliers who prioritise security. A significant 68% would use a more expensive supplier if that supplier demonstrates superior security and transparently communicates the privacy and security aspects of their offerings.

In a bid to narrow the knowledge gap and boost confidence, SMBs are actively asking for support — most notably from governmental bodies — in cyber security education and training. Only 6% of SMBs foresee a decline in their cyber security investments. For 44% of these businesses, economic uncertainty and rising living costs are a factor in their cyber security spending. Intriguingly, 29% perceive a dip in threat levels this year. France, Spain and Canada are the countries where the most SMBs expect to decrease their investment in cyber security.

a **91% of SMBs expect cyber security investment to increase or remain the same in the next year**

b **68% would use a more expensive supplier if that supplier demonstrates superior security**

c **64% of SMBs use cyber insurance – 74% plan to use it next year**

d **52% want more support with cyber security education and training**

e **44% say economic uncertainty/cost of living has reduced cyber security budgets**

> **Cyber crime is now a real threat to small and medium businesses, irrespective of their scale.** Their digital presence can turn into a potential weak link within the supply chain. Dependence on major suppliers and government authorities requires collective action. At the same time, tackling this looming challenge also presents a unique opportunity to carve out a distinct competitive edge - enhancing an organisation’s reputation and building trust.

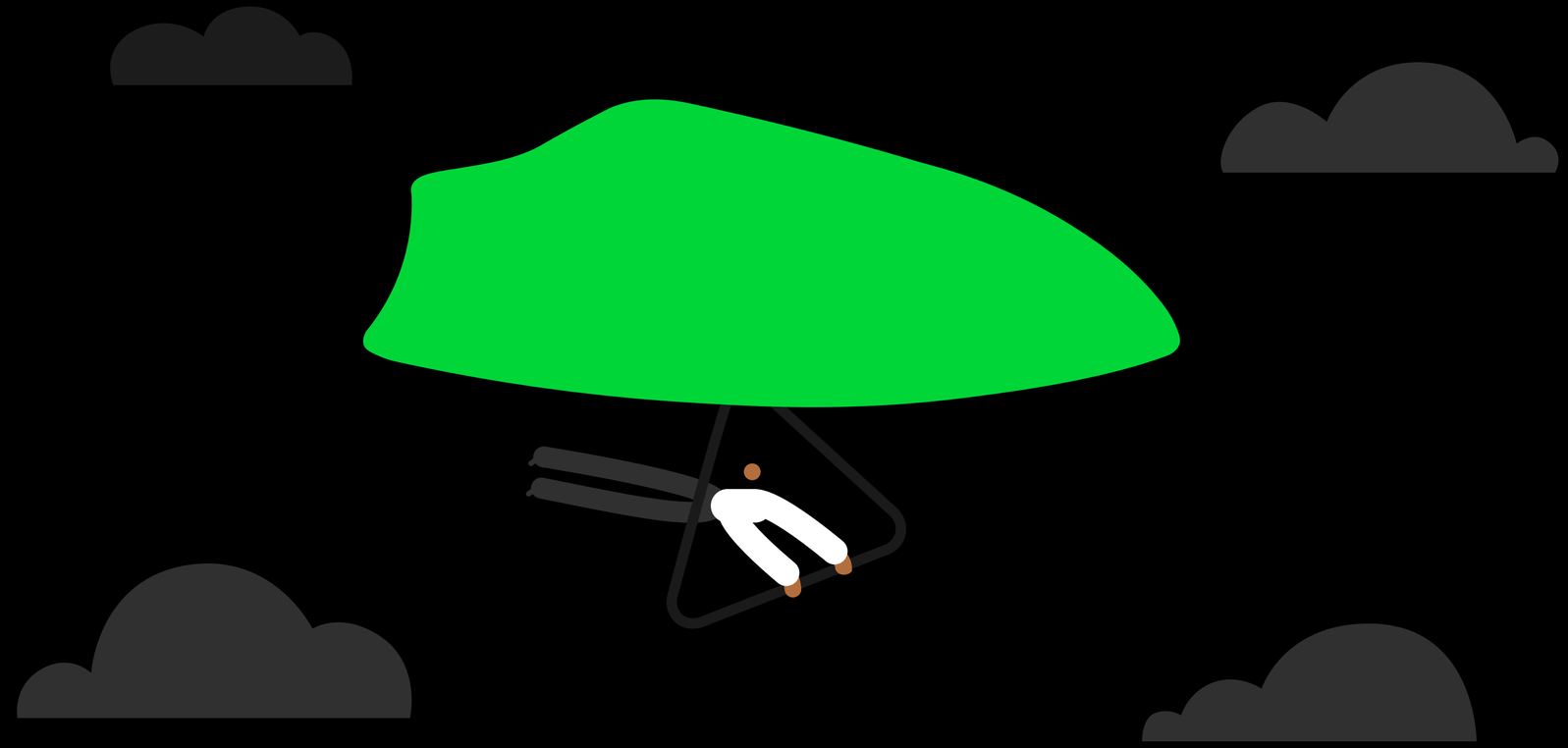
Simon Borwick
Cyber Security Partner at PwC UK

Conclusion

SMBs are actively trying to ensure their organisations are cyber secure. But they face challenges at virtually every turn. These hurdles range from complex advice which isn't tailored to their risks and needs, to a lack of support from governments and tech partners leaving them unaware of what solutions are right for them, or unable to implement them due to limited knowledge and resources.

Bigger companies and governing bodies must make it easier for SMBs to leverage great cyber security 'out of the box' and help demystify it as a business issue for their employees.

Understanding how to optimise, and go beyond, "basic" controls by using the right technology services, such as cloud adoption, can ease the burden on resource-tight businesses. By providing secure software, cutting through the noise with targeted advice, and empowering them with knowledge, SMBs can integrate cyber security into business as usual and focus on growth.



Country-Specific Information

Covering: United Kingdom, United States, Canada, France, Spain, Germany, Portugal, South Africa and Australia

United Kingdom

A job to be done to boost culture and coverage

UK SMBs reported the fewest cyber security incidents in the past 12 months (42% reported one). This contrasts dramatically to France (60%) and Germany (55%).

However, they appear to be lagging behind other nations when it comes to implementing measures to secure remote workers. Only 57% have different policies in place depending on home and office work, compared to 78% in France, for instance. This leaves them vulnerable to the unique threats posed by remote work, such as unprotected WiFi connection.

Perhaps this is one reason why more UK SMBs (54%) see keeping on top of new threats as a bigger challenge than the global average (51%). Why more want support with education and training (57% vs. 52% globally). And why slightly fewer see cyber security as part of their culture (67% vs. 69% globally).

57%

of UK SMBs have different policies for office and home working

United States

Room to build on cyber engagement rates

More than three-quarters of SMBs in the United States believe cyber security is a part of their culture – significantly above the global average of 69% - and they are most likely to be using cyber insurance (67%). This aligns with 77% saying they actively invest in cyber security measures for their businesses and explains why this group has the greatest confidence that small businesses are taking cyber security seriously.

However, although more SMBs discuss cyber security regularly than the global average (45% vs. 40%), this leaves room for improvement to ensure employees are engaged and educated to combat attacks.

When it comes to specific cyber security challenges, keeping on top of new threats (49%) and educating employees on cyber security (43%) are identified as the biggest challenges in the U.S – in line with the global perspective.

76%

of US SMBs agree that cyber security is part of their culture

Canada

Threat identification a top priority

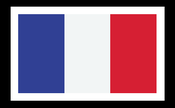
Fewer SMBs in Canada reported having different security in place for those working from the office versus at home than the global average. And Canada – alongside France and Spain – is one of the countries where the highest percentage of SMBs expect to decrease cyber security investment in the next 12 months.

Yet, only 48% want more support with cyber security education – suggesting a disconnect between challenge and potential solution.

Canada also ranks marginally below the global average when it comes to SMBs who see cyber security as part of their current culture. 63% of Canadian businesses agree, compared to 69% globally.

59%

of Canadian SMBs have different policies for office and home working



France

Lack of investment explains lack of concern?

SMBs in France are the most confident group (82%), alongside Spain, in managing their cyber security. And they have taken steps to address working from home, with 72% having different policies for remote vs. office work.

However, they are also the least likely to see keeping on top of new threats as a challenge (39%), compared to global counterparts (51%) and utilise basic controls less than SMBs in other countries. Only 50% say they use cyber security insurance, with 8% citing cost as the prohibitive factor.

This is a concerning trend given 60% of French SMBs reported incidents in the past year and more SMBs in France than in any other country except Spain are expecting to decrease their investment in cyber security moving forward.

39%

of French SMBs said keeping on top of new cyber security threats is a challenge

Spain

Least likely to be talking cyber security

Just under three quarters (73%) of SMBs in Spain say they do not discuss cyber security regularly, making them the least likely to do so across all regions. This conflicts with their strong belief (71%) that cyber security is part of their culture.

The Spanish are also more comfortable with the levels of cyber security support provided than other countries, with 45% of respondents wanting more support compared to 52% globally. However, alongside France, they have more SMBs than anywhere else expecting to decrease cyber security investment. Doing so will make it more difficult to keep on top of new threats and educating employees – the top two challenges identified in the region.

27%

of Spanish SMBs are discussing cyber security regularly

Germany

Contrast between incident rate and knowledge, concern

55% of SMBs in Germany reported at least one cyber security incident in the past year. Only French SMBs reported more. The statistics point to a general need to improve education and support to help reduce this real threat.

German SMBs review their cyber security the least (68% vs. 76% global average), are least concerned (54%), and 20% have no plans to use cyber insurance. They also have a lower level of understanding of cyber terms such as ransomware (60% do not know what it means).

This perhaps explains why only 41% see keeping on top of new threats as a challenge.

68%

of German SMBs review cyber security regularly

Portugal

Seeking support with education, recruitment

Over half of Portugal's SMBs believe educating employees on cyber security issues is their biggest challenge – far higher than the 44% global average.

They also identified various skills and operational gaps in the region. 40% admit struggling to recruit people with cyber security skills, 56% are uncertain that suppliers operate securely, and Portugal has the least confidence (46%) that small businesses are taking cyber security seriously.

Given that only approximately two-thirds of SMBs in Portugal are investing in cyber security measures themselves, this support may have to come from external sources and guidance. With 71% of Portuguese SMBs seeing cyber security as part of their culture currently, there is appetite for this.

55%

of Portuguese respondents said that educating employees on cyber security is the biggest challenge

South Africa

Education and training a top priority

Despite, or because of, high levels of investment in cyber security measures, there is a clamour for better education and training around cyber security among South African SMBs – reflecting the complex nature of current guidance as well as a need to raise awareness around training options. The number seeking more support (69%) is a dramatic outlier compared to the 52% global average.

So, it is no surprise that 55% of respondents see educating employees as the biggest challenge – again significantly higher than the global average of 44%.

Interestingly, the most common cyber security incident reported in South Africa was stolen laptops. Ransomware attacks were reported less (9%) than the global average (13%).

69%

of South African SMBs want more support with education and training

Australia

Cyber security culture is commonplace

Three-quarters of Australian small and medium-sized businesses believe that cyber security forms part of their culture, compared to 69% globally.

Despite, or because of this, they are keen to seek out more support with education and training. 57% of respondents want more of this, ranking second globally and above the 52% global average. And it may also explain why more (57%) see keeping on top of challenges as a bigger challenge than the global average (51%).

Educating employees is also a concern for more Australian SMBs (48%) than the 44% global average.

75%

of Australian SMBs agree cyber security is part of their culture

Summary of methodology

Sage's research was conducted by independent market research company, Danebury Research, between 4th April and 15th April, via 2,100 online interviews with decision-makers in small and medium-sized businesses ranging in size from up-to 9 employees and 499 employees. The 2,100 interviews were split across nine markets: UK, U.S., France, Germany, Portugal, Spain, South Africa, Canada, and Australia.

Country	Sample size
UK	500
U.S.	500
France	100
Germany	100
Portugal	100
Spain	100
South Africa	100
Canada	500
Australia	100

About Sage

Sage exists to knock down barriers so everyone can thrive, starting with the millions of small and medium-sized businesses served by us, our partners, and accountants. Customers trust our finance, HR, and payroll software to make work and money flow. By digitising business processes and relationships with customers, suppliers, employees, banks and governments, our digital network connects SMBs, removing friction and delivering insights. Knocking down barriers also means we use our time, technology, and experience to tackle digital inequality, economic inequality and the climate crisis.

About Danebury Research

Danebury Research is a global full-service market research company based in Stockbridge, Hampshire. It works with both agencies and clients on a global level. With access to a panel of over 200 million respondents, Danebury Research is dedicated to empowering brave decisions through the provision of reliable, accurate, and representative data. Services offered by Danebury Research include market research, brand research, customer satisfaction surveys, employee surveys, and PR surveys.

For more information about Danebury Research and its market research services, please visit the company's website at **www.daneburyresearch.com**.

sage.com