SIZE DOES MATTER: Small businesses and cybersecurity
WEBROOT | SIZE DOES MATTER: SMALL BUSINESSES AND CYBERSECURITY

FOREWORD BY THEO PAPHITIS

Small businesses are part of the UK’s economic lifeblood. SMBs account for at least 99.5% of businesses in every main industry sector and we need to support and protect them in this challenging climate. Technology is key to helping small businesses grow, reach new customers and thrive. But digital technologies can present challenges and difficulties for any business, the top one is cybersecurity issues.

It’s common for smaller businesses to think they’re too small to be targeted, but this research from Webroot shows that’s simply not the case. Smaller businesses have been and will continue to be targeted by cybercriminals. This puts not only their customers and contracts at risk, but ultimately the future of the business.

However, it’s clear there needs to be a balance. It’s concerning that smaller businesses have had to deprioritise activities that would help their business grow to address security issues. Educating small businesses on cybersecurity and helping them get the right support to address challenges is crucial. Small businesses are in the unique position to act quickly and be more flexible than their larger counterparts. This report is a great education tool providing tangible guidance and advice to UK small businesses to help them use their size as an advantage when it comes to cybersecurity.

“It’s concerning that smaller businesses have had to deprioritise activities that would help them grow in order to address security issues.”

Theo Paphitis
**INTRODUCTION**

With the rise of digital technology, the business environment in the UK is changing rapidly.

But one thing remains the same: small and medium sized businesses (SMBs) are at the core of our economy. Their success will determine the future of the UK in the digital age.

SMBs face a challenging climate. Our smallest organisations must grapple with rapid political, economic and social change.

This uncertainty is looming large in business leaders’ minds, as SMBs point to Brexit as their biggest threat (45%). As well as the many challenges they face as they become established and grow, SMBs must adapt at speed – all with fewer resources than their larger competitors.

It’s in this context that SMBs are tackling the issue of cybersecurity. Since 2017, the threat of cyberattacks has gained more prominence than ever before, with high profile attacks like WannaCry and NotPetya registering on the public consciousness.

This includes SMBs – with 35% perceiving cybersecurity as a significant threat. And these cyber threats can take up a significant proportion of SMBs’ time: nearly a full day per week.

However, cybersecurity is just one consideration as businesses become more established and grow. SMB leaders say that their biggest priorities are attracting new customers (36%) and increasing business growth and profitability (29%).

Moreover, media coverage has tended to focus on the threat of cyberattacks for larger businesses, rather than the risk to their smaller counterparts.

It’s perhaps not surprising that SMB leaders may deprioritise cybersecurity in the face of other business-critical responsibilities – and even be tempted to see themselves as too small to be attacked.

That’s why we set out to understand how over 500 IT leaders at small and medium sized companies in the UK are approaching cybersecurity. This includes how SMBs are defending their businesses on the ground, the greatest security and organisational threats they’re facing and how they can improve their cybersecurity – and business performance.

Our findings point to some concerning vulnerabilities, which SMBs can address.

However, there’s also a fantastic opportunity for SMBs to use cybersecurity to create growth and even competitive differentiation for the business. This will ensure that as we approach our digital future, SMBs are not only safe from threats, but can use their size to thrive.

I hope you enjoy the report.

Paul Barnes
*Senior Director, Webroot*
SMBS’ CYBER DEFENCES

A range of expertise

Looking at how small and medium sized businesses are approaching their cyber defences, it’s clear that security is being balanced with a whole host of other IT – and business – priorities.

At the majority of organisations, responsibility for cybersecurity sits alongside other IT duties, with three quarters (75%) of the IT leaders we surveyed overseeing both. At the remaining businesses, the CEO is usually in charge (44%).

This results in a wide range of cybersecurity expertise within SMBs. Survey respondents rated their knowledge from expert to basic, with many (30%) claiming to have an intermediate understanding of the issue.

SMBS in the finance sector have the highest proportion of ‘experts’ (22%). Meanwhile, retailers have the lowest, which is perhaps concerning given the level of personally identifiable information these businesses usually hold.

Alarming, 11% of SMB IT leaders say that they have basic or ‘no knowledge’ of cybersecurity – leaving 1 in 10 UK businesses at risk.

Getting educated

When it comes to educating themselves on cybersecurity risks, the majority of IT leaders rely on self-teaching and industry news (41%). This rises to 47% of the smallest companies, who have only 1-50 employees.

A lower proportion also rely on dedicated teaching (36%) or their cybersecurity provider (33%) to improve their knowledge.

By contrast, when it comes to teaching other employees about cybersecurity, the most popular approach is dedicated cybersecurity awareness training (38%), and just a quarter (27%) rely on employees teaching themselves.

There’s acknowledgement amongst IT leaders that they could (and maybe should) do more than simply teaching themselves. Three fifths (61%) admit that there’s more they could do to fully understand the right practices for their organisation.

Since IT leaders are the gatekeepers for the security of their organisation, perhaps there’s a case for more investment in educating the IT team – as well as employees – on the best cybersecurity practices.

Defence spending

The level of investment that SMBs make in cybersecurity is growing. While businesses invested 5.27% of their turnover in cyber defences two years ago, this has risen to 6.11% at present. By 2021, businesses expect to invest 7.53% each year.

This rising investment is perhaps not surprising in a post-General Data Protection Regulation (GDPR) world, as the penalties of the regulation create a clear incentive for businesses to protect their data.
In every case, IT leaders who are ‘expert’ in cybersecurity spend at least twice as much on cybersecurity than those with ‘basic’ knowledge, 9.44% compared to 4.21% at present.

These investments cover a range of tools, including firewalls (65%), endpoint protection (64%) and email filtering (44%). Interestingly, more than half have also invested in cybersecurity insurance to protect them in the event of a breach.

Money is of course extremely tight for many SMBs, and it’s vital that organisations not only set a cybersecurity budget that aligns with their risk profile, but direct it in the right way. This will ensure that the spend is as cost-effective as possible.

An alarming time-drain

Over half (60%) of SMBs say that their organisation has a complete end-to-end cybersecurity strategy, while 40% don’t. Notably, this rises to 93% of the IT leaders who describe their knowledge as ‘expert.’

But despite this structured approach, it’s clear that cybersecurity is time-consuming for SMBs. In fact, they spend almost a day a week (18%) of their time on cybersecurity-related tasks.

Importantly, it seems that many of these activities are unplanned. Almost half (48%) say that they have had to deprioritise activities that would grow their business to address cybersecurity challenges.

When resources are extremely tight, losing a day a week is a high price. By working with cybersecurity experts – and changing their approach from reactive to proactive – IT teams could regain precious time and ensure that their activities better complement the business’ growth.

Shaped by the media agenda

Mainstream media coverage of cybersecurity issues has risen dramatically since 2017 – and this appears to have shaped many SMBs’ attitudes to the issue.

In fact, more than half of respondents (52%) say that high profile cyberattacks or data breaches in the news have made them change their approach to cybersecurity.

The media focus on consumers’ information seems to have informed SMBs’ approach to investment. The main reason that IT leaders give for investing in cybersecurity is protecting consumer data (25%), alongside reducing risk (25%).

By contrast, many other business critical drivers are overlooked. Despite the fact that non-compliance of GDPR can result in penalties of up to €20 million or 4% of global revenue, meeting compliance requirements was only selected by 11%.

Even fewer SMBs consider protecting their intellectual property (9%) or meeting the requirements set by their customers (4%) as key drivers for cybersecurity investment. As we’ll discuss later, this could suggest smaller businesses are failing to appreciate the very real threats that attacks can pose to their success and survival – as well as opportunities to gain a competitive advantage.
TWO SMALL TO BE A TARGET?

“It won’t happen to me”

Amongst some small and medium sized businesses, there seems to be a shared belief that their size means they are less at risk of a cyberattack than larger enterprises.

Two-fifths (38%) of respondents say that their business is too small to be targeted by cybercriminals, which perhaps surprisingly rose to 43% of the largest SMBs (251-500 employees).

Similarly, more than a third (36%) of respondents say the size of their business means that they do not have to fully understand cybersecurity. Notably, this rose to 46% of the companies with the biggest annual turnover (£500m or more).

One reason appears to be SMBs’ perceptions of the data that they hold. Two-fifths (39%) say that their business does not hold any data that cybercriminals would find useful or valuable.

These views are alarming. All businesses hold information which could be compromised and sold, whether it’s commercially sensitive data or employees’ personal details.

Criminals are adept at finding information that will bring them profit – and will ultimately target any organisation that appears vulnerable. Whatever their size, if a business leaves a door open to cybercriminals, it can become a victim.

A lack of resource

It seems that the lack of cybersecurity resource at SMBs can translate into complacent attitudes.

Almost two-fifths (38%) of IT leaders say that they simply do not have the time needed to fully understand cybersecurity threats to the business, which concerningly rose to 51% of financial services firms.

Similarly, almost a third (31%) say that cybersecurity is too complicated for them to be concerned with it. Again, businesses with higher revenues tend to agree disproportionately with this statement, which is selected by 52% of IT leaders with an annual revenue of £100m to £499m.

It might be that feeling unable to meet cybersecurity challenges makes it easier to use a tick box approach or simply conclude “it won’t happen to me.” After all, a third of SMBs (33%) say they prefer not to think about cybersecurity at all.
A business drain

Perhaps because SMBs view cybercrime as less relevant to smaller organisations, they tend to view investment in cybersecurity as a business drain, rather than a business driver.

Half (50%) say that their profits will take a hit from investing in cybersecurity, while a quarter (24%) say they see no returns from their cybersecurity spend.

Importantly, two-fifths of respondents (40%) believe that cybersecurity policies and threats restrict their business’ growth more than larger enterprises – meaning that protecting the business is actually placing them at a competitive disadvantage.

However unlikely they believe it to be, SMBs nonetheless understand the damage that a cyberattack could do.

Three-fifths of respondents say that their productivity (60%) and profits (59%) would take a hit as a result of cybersecurity incidents.

Cybersecurity can even shape the business strategy, with nearly half of businesses (46%) admitting to changing their business plan as a result of cybersecurity issues.

SMBs certainly aren’t at lower risk of cyberattack than their larger competitors, and it’s clear that they understand the potentially devastating consequences of a successful hack. But with the right strategy, it’s possible to change cybersecurity from a business drain into a business driver, as we’ll discuss in Chapter 4.
THE THREATS

The scale of the challenge

Far from being a ‘big company’ problem, the experiences of small and medium sized businesses underline that cyberbreaches are a real and likely threat.

Almost half of all IT leaders (48%) say that their business has suffered a cyberattack or data breach. In fact, one in seven (15%) say that it has happened more than once.

Financial services businesses are the most likely to have been targeted, with one in four (24%) being attacked on multiple occasions. Alarminly, a third (35%) say that they have experienced a breach in the last twelve months alone.

Although these rates are high, they are relatively conservative compared to most cybersecurity research – suggesting that many businesses may have experienced an attack but are not aware of it.

Today cybercriminals want to remain undetected, so that they can keep collecting data, gain further access to the network or even breach partner networks, like suppliers or customers.

Stealthy malware can often remain unnoticed for long periods, meaning that SMBs must remain vigilant, however immune they may think they have been to this point.

Types of attack

Cyberattacks come in many shapes and sizes. Perhaps again indicating the influence of the media agenda, SMBs are most concerned about the attack vectors that have been most prominent in the news.

Malware infections (19%), IT system failures (16%) and ransomware attacks (16%) top the list of IT leaders’ biggest concerns, followed by phishing (10%) and employees (9%).

It may be telling that healthcare SMBs pointed particularly to malware (26%) and ransomware (19%), which were the main methods deployed in the WannaCry attack against the NHS.

Just 1 in 20 respondents point to DDoS attacks (6%), insider threats (5%) or cryptojacking (5%).

Notably these fears don’t reflect the real frequency of attacks, as cryptojacking was actually the second most popular attack vector in 2018.

A lack of awareness of some cyberattacks may be shaping SMBs’ concerns. For example, although only 5% of IT leaders highlight insider threats as a key risk, almost half (45%) believe that disgruntled employees committing deliberate sabotage in their organisation could contribute to insider threats – suggesting a far higher threat.
Understanding more about each attack vector, and the risk it presents to the organisation, will help IT leaders more accurately assess the biggest threats to the business.

**A lack of awareness**

Employees are often described as the first line of defence against cyberattacks, and it’s clear that working practices and behaviours could be putting businesses at higher risk.

Lack of awareness is an important issue. Two-thirds (69%) of IT leaders believe their business is at risk due to employees inadvertently creating security threats due to lack of knowledge.

The often-demanding working environments at growing businesses can present a risk too, as nearly two-thirds (64%) say that high workloads can cause employees to make cybersecurity mistakes.

This lack of awareness is placing SMBs at risk of attacks specifically designed to target them, such as Remote Desktop Protocol (RDP) attacks. In these cases, hackers use unsecured RDP protocols as a port of entry into a network, before deploying either ransomware or cryptojacking.

Cybercriminals may execute RDP attacks because default ports are left open or the organisation has lax password policies. However, another critical point of entry is phishing attacks on employees which compromise the network’s credentials.

Boosting awareness of hackers’ tactics can help SMBs ensure that their employees are a security strength, rather than a weakness.

**The risk of closure**

SMBs are also well-aware of the ways that a cyberattack could inflict damage on the business, and customer relationships are critical.

Over two-fifths of respondents (44%) say that their business could be used as an entry point to one of their large enterprise customers.

Nearly half (48%) of the cases negatively impacted relationships, and almost a quarter (22%) admit they are no longer a supplier as a result.

This is striking, especially since only 4% of SMBs say that meeting their supplier requirements is a key driver for cybersecurity investment.

When uncertainty is high and the landscape is highly competitive, SMBs absolutely can’t afford to risk losing customers because of cybersecurity failures.

Meanwhile, IT leaders acknowledge the impact that falling foul of data protection regulation could have on the business. Three-fifths say that industry regulation like GDPR has made them prioritise cybersecurity.

Ultimately, SMBs understand that the financial – and reputational – damage of a cyberattack could be devastating. Almost half (46%) of respondents say that if their organisation suffered a data breach, it would put their business at risk of closure.

But it is possible to turn cybersecurity from potential weakness to strength, by making it core to business productivity and innovation.
THE COMPETITIVE DIFFERENTIATOR

From business drain to business driver

Many small and medium sized businesses view cybersecurity as a business drain: a tickbox exercise and necessary evil to keep the organisation safe.

However, far from being an impediment, cybersecurity can act as a differentiator for SMBs. Organisations can not only shore up their customer relationships but also support wider improvements to their productivity and innovation.

Powering productivity

Technology improvements will be key to the future of both large and small businesses in the UK.

Promisingly, many smaller organisations are investing – or planning to invest – in a wide range of digital technologies that will improve their productivity and performance.

The cloud (61%), improving connectivity (49%) and bring your own device policies (39%) are the most popular strategies currently in use.

Meanwhile, new devices and the Internet of Things (37%), agile and remote working (34%) and improving connectivity (34%) top SMBs' plans for the future.

While this is positive, it's important to acknowledge that adopting new technologies will inevitably increase SMBs' attack surface, making them a bigger target for hackers. In fact, concerns about the security of these technologies are mentioned frequently as reasons that SMBs won't invest in them.

IT leaders explain why they won't invest in areas like cloud and agile working with comments including “it's insecure”, “I don't trust it”, “it worries me” and “there's not enough security”, as well as the “risk is too high of virus on the network” and “it could not be protected.”

While it is possible to protect these technologies, it requires a holistic cybersecurity strategy – and it's here that specialist support can help.

Adopting an approach that can not only protect the whole network, but also adapt as new technologies are introduced, will enable SMBs to keep themselves secure.

Meanwhile, tools that automate many cybersecurity tasks can help to free up IT managers' valuable time from the day a week currently lost to security activities. This will enable them to focus on the technologies that will improve the business' overall performance.
Happier employees and happier customers

Overworked employees can increase the risk of cyberbreaches. Nearly two-thirds (64%) of SMBs say that stressed workers put their organisation at more risk, as discussed earlier.

Digital tools could help employees to speed up or automate many routine tasks, making their working days more enjoyable and more productive – and ultimately making workloads more manageable.

In turn, these workers will be able to focus more on the creative, innovative thinking that will help their businesses to succeed in a landscape of rapid change.

This will not only improve businesses’ performance, but reduce risks from cyberattacks, keeping them safe.

This link between cybersecurity and performance is recognised by many IT leaders, as half of respondents (58%) say that cybersecurity policies could increase productivity in their business.

Meanwhile, a proactive and dynamic approach to cybersecurity can help to protect vital customers, whether it’s consumers or larger businesses.

By actively meeting and exceeding supplier requirements, SMBs can present themselves as true partners to big businesses, not only avoiding the loss of customers, but actively setting themselves apart to attract new ones.

Perhaps as a result, nearly three-tenths (28%) of SMBs say cybersecurity could increase their revenues and attract new customers.
CONCLUSION:
SIZE DOES MATTER: AGILITY IN AN AGE OF CHANGE

Small and medium sized businesses are well-placed to succeed in this uncertain climate. Their agility means that they can adapt to developments in the cybersecurity landscape and the business environment.

This is something that businesses themselves appreciate; nearly two-thirds (64%) believe that being smaller enables their business to react more quickly to industry or political change than larger enterprises. Technology will be critical here, and it’s encouraging to see the numbers showing plans of ambitious digital investments.

And although resource can be a challenge, it’s not everything, as more than half (64%) believe their size means it’s easier to find the means to react to industry or political change.

This agility also applies to cybersecurity. Cybercriminals are constantly developing new attack vectors and seeking ways to profit from businesses of all sizes, but with the right cybersecurity strategy, SMBs can adapt.

Nearly two-thirds (63%) of respondents say that being smaller means they can more quickly implement new measures in response to an evolving cybersecurity landscape.

People are small businesses’ biggest asset, and they can also be a vital ally in the battle against cyberthreats. Three-fifths (61%) of IT leaders say that their employees are quicker to flag potential cybersecurity issues than at larger enterprises.

Importantly, two-thirds believe their employees are more open to embracing change, in technology and in security. But to succeed, small and medium sized businesses must be realistic about the threats that they are facing – and embed an agile cybersecurity strategy into everything that they do.

With confidence that their business is protected, smaller businesses can digitally transform, improve their experiences of their customers and employees and ultimately secure their success.

Size does matter when it comes to cybersecurity. It can be SMBs’ biggest asset in these times of change.

METHODOLOGY

This survey of 501 IT decision makers in companies with 1-500 employees was conducted by Censuswide in January 2019. Respondents included businesses in the financial services, retail, healthcare and public sectors.