WHITE PAPER ● CYBERSECURITY
MARCH 2026

Cybersecurity through the SME lens

Contents

Foreword

Mark Barnett
Global Head of SME, Mastercard

Johan Gerber
Global Head of Security Solutions, Mastercard

Running a business isn't easy. The entrepreneurs who devote themselves to their small and medium enterprises (SMEs) find themselves juggling countless responsibilities and overcoming a constant stream of challenges, from the mundane, to the existential.

As more businesses enter our thriving digital economy, one of the most pressing challenges they face is the growing risk of cyberattacks. No longer the exclusive concern of large corporations, cybercriminals are using increasingly-automated attacks to cast larger nets and catch unwary businesses, hitting companies of every size, in every industry. The consequences of these attacks can be devastating — ranging from financial and reputational damage to bankruptcy or closure. Beyond the business impact, the emotional toll on owners and employees is significant, making it clear that complacency is not an option.

Mastercard's research shows how SMEs are now firmly in the crosshairs of fraudsters and cyber criminals. We spoke with more than 5,000 business leaders representing a broad range of SMEs (see breakout) to find out the biggest risks and impacts cyberthreats have on businesses today.

Confidence is a crucial asset for SMEs as they navigate this landscape. Yet many business leaders report a lack of confidence in their readiness, knowledge, and support when it comes to cybersecurity. This uncertainty can make every challenge feel more daunting and every decision more fraught. Given that SMEs form the backbone of the global economy — accounting for 90% of all businesses, 70% of employment, and around half of global GDP according to the World Bank — their ability to grow and thrive depends on having the tools, information, and help to defend against cyber threats. Empowering SMEs with these resources is essential not just for their success, but for their survival.

The complexity of cybersecurity means that SMEs cannot tackle these challenges alone. As threats evolve, so too does the need for expert guidance. SMEs are increasingly seeking out trusted partners and specialists to help them stay informed, educate their teams, and implement effective protections. There is a clear appetite for support, and a compelling opportunity for organisations like Mastercard and its partners to provide the expertise and solutions that SMEs need to stay protected in the digital economy.

Ultimately, SMEs require practical solutions to address the tangible risks they face. They are more aware than ever of their vulnerabilities and are open to adopting new cybersecurity tools — provided these solutions are accessible, trustworthy, and tailored to their needs. Cost and trust are key factors in decision-making, and providers must be mindful of these realities.

By working together, we can help SMEs access the resources and support they need to overcome cyber threats and focus on what matters most: growing their businesses and achieving their goals.

The survey referenced in this paper was conducted by the Harris Poll on behalf of Mastercard from January 14 to January 28, 2025, among 5,054 small and medium business owners.

Smal businesses are defined as those with 10-49 employees, while medium businesses have 50-250. All respondents are employed full-time, with titles such as Owner, Founder, CEO, or Chairman.

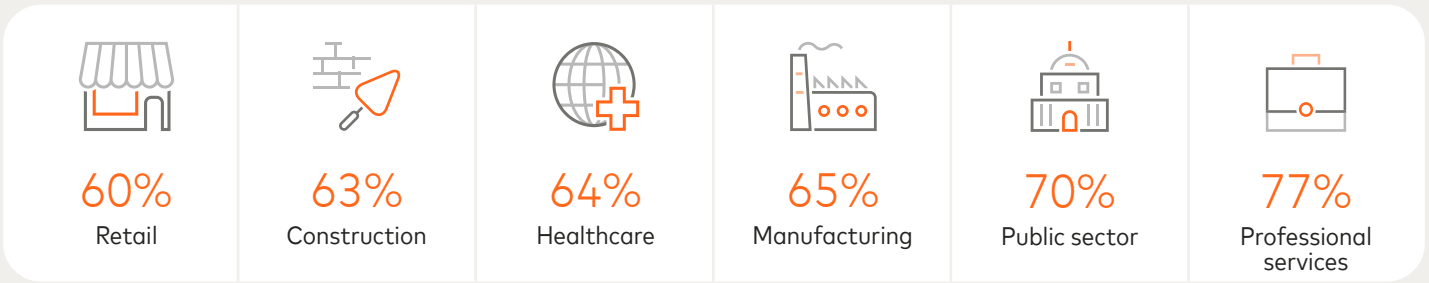
To ensure respondents had experience with cybersecurity to accurately answer survey questions about the topic, they all work for organizations with some sort of digital footprint.

Cyberattacks are more common than ever

For SMEs, cyberattacks are no longer an out of the ordinary, once-in-a-blue moon event. Cyberattacks are now part of the standard business landscape, an occupational hazard that must be factored into a company's standard operating procedures.

When it comes to cyberattacks, the question to ask is not "if" but "when". For the SME leaders we questioned, nearly half (46%) had experienced an attack at their current business, a figure that rose to nearly two thirds (65%) when they included attacks they'd witnessed at a previous organization. This widespread nature of attacks isn't limited to a single region or industry segment — it's pervasive, worldwide, and posing a unique threat to the backbone of the economy.

Fewer attacks ← **Have experienced an attack by industry** → More attacks



Those working across professional services are the most likely to have suffered an attack, with 77% of respondents saying they'd experienced an attack at their current or previous organization. As heavily digitized businesses working with a wide range of partners, it makes sense that their systems may have particular vulnerabilities that make them a target for fraudsters. But even retail and construction businesses, which are typically less digitized, are being hunted by bad actors, and respondents in those sectors were still more likely to have been the target of an attack than not.

Fewer attacks ← **Have experienced an attack by market** → More attacks

The same is true if we look at the picture by region. While respondents in different countries report varying levels of attacks, nowhere is safe. Even in the U.S., more than half of all respondents report being a victim of a cyberattack at their current or previous workplace, while in India, 71% of respondents have had to deal with the stress of an attack. Wherever they live, whatever they do, SMEs face a constant risk of cyberattack.

The shape of cyberattacks today

Cyberattacks are as diverse as SMEs themselves. Just as businesses grow, develop, adopt new innovations and adapt to new markets, so do the fraudsters behind cyberattacks, constantly testing out new methods and techniques to find weaknesses and exploit vulnerabilities.

The two most common forms of cyberattack are hacking/data breaches and malware, with 32% of those who had experienced an attack having to deal with them. Even these kinds of attacks can come in many different forms, from fraudsters taking advantage of weak security on websites, such as sites that are only protected with single-factor authentication, to employees mistakenly downloading malicious software.

Phishing is similarly common, where fraudsters send plausible looking emails that busy business owners might click on while trying to take care of their admin, only to be taken to a fake site that harvests their details or installs dangerous programs, also known as malware.

Top types of attacks SMEs have experienced

Among those who have experienced an attack

#1 (tied)	Hacking or data breach (32%)
	Malware (32%)
#2	Phishing (31%)
#3	Ransomeware (29%)
#4	Identity theft (28%)

Most concerning cybersecurity threats

Global total: highly concerned (top 3)

#1	Hacking or data breach (67%)
#2 (tied)	Identity theft (66%)
	Malware (66%)
#3 (tied)	Phishing (65%)
	Ransomeware (65%)

Ransomware attacks accounted for 29% of the attacks people have suffered, where a businesses' systems are locked down until a ransom is paid, with huge amounts demanded. Identity theft makes up 28% of attacks. These enable fraudsters to apply for loans and credit, or even take possession of a business' intellectual property, leaving businesses to handle the debts and the reputational damage.

The potential professional embarrassment of identity theft means it's one of the forms of attack that is most concerning to SMEs, with 66% of respondents listing it as their biggest fear, tied with malware. The prevalence of hacking and data breaches, and the potential fallout, makes this the biggest concern for SMEs, with the threats of phishing and ransomware coming in third.

While hacking, malware and phishing are the most commonly experienced kinds of attack in most industries, identify theft is a major cause for concern among retail and construction businesses. In the public sector, account takeover, where fraudsters maliciously access an account and use it to make unauthorized transactions or access data, is the second most common kind of attack.

Hacking:
Unauthorized access to computer systems or networks to steal, alter, or destroy data.

Malware:
Malicious software designed to damage, disrupt, or gain unauthorized access to computer systems.

Phishing:
Fraudulent attempts to obtain sensitive information by sending emails disguised as coming from a trusted source.

Ransomware:
Malicious software that locks or encrypts a victim's data, and then demands payment for it to be released.

Identity theft:
The fraudulent acquisition and use of someone's personal information, which is then used to impersonate the victim.

The impact of cyberattacks on SMEs

If cyberattacks are an everyday reality for SMEs, so are the stresses of dealing with the fallout they cause. The impacts are not just financial – they can range from emotional stress through to legal troubles and reputational damage.

In extreme cases, cyberattacks have even forced businesses to close. While the most common impact among all businesses who have suffered a cyberattack is rising costs (38%), nearly one in five (18%) have had to file for bankruptcy in the wake of a cyberattack, and 17% have had to shut down entirely.

While most businesses survive and continue after an attack, the impacts can still be far reaching. More than three quarters of those experiencing a cyberattack agreed they were more stressed about their security following an attack, while 80% needed to devote time and effort to rebuilding trust with clients.

As well as reaching out externally to reassure partners, SME leaders must refocus internally, working on their own teams and processes to avoid suffering negative impacts again. Business leaders are dedicating more time to learning and researching cybersecurity trends, with 82% feeling the need to become more aware of threats. Another 82% are prioritizing employee training on cybersecurity, taking up valuable business hours and resources.

38%

Increased cost

18%

Filing for bankruptcy

17%

Closing the business

Putting cybersecurity front and center

The day-to-day nature of cyberattacks for SMEs is beginning to be reflected in how they structure their operations. When ranking five common business priorities, 28% of all firms polled put cybersecurity front and center, a figure that rises to over a third of all businesses (34%) in the U.S.

As priorities change, so do budgets. Altogether, 70% of SME leaders told us that if they had additional budget available, they'd funnel it towards their cybersecurity efforts, while 62% agreed that when it comes to allocating budget resources, cybersecurity is currently the top priority.

When asked if cybersecurity is critical to their business operations, 79% of respondents agreed. Cyberattacks aren't an afterthought for today's SMEs — they're something every business needs to think about and prepare for.

Business priorities over the next year (summary of number one ranked issues)

79%

Agree, "effective cybersecurity is **critical to my business operations.**"

62%

Agree, "when it comes to our business' budget, **cybersecurity is a top priority.**"

Cybersecurity is the **top area to which SMEs would allocate additional budget** if they had it (70%)

Perception versus reality

There's no arguing with reality. Whether it's a firm handshake at the end of drawn-out negotiation, or quarterly sales numbers laid out in black and white, these tangible things are what drive our businesses and our decision making.

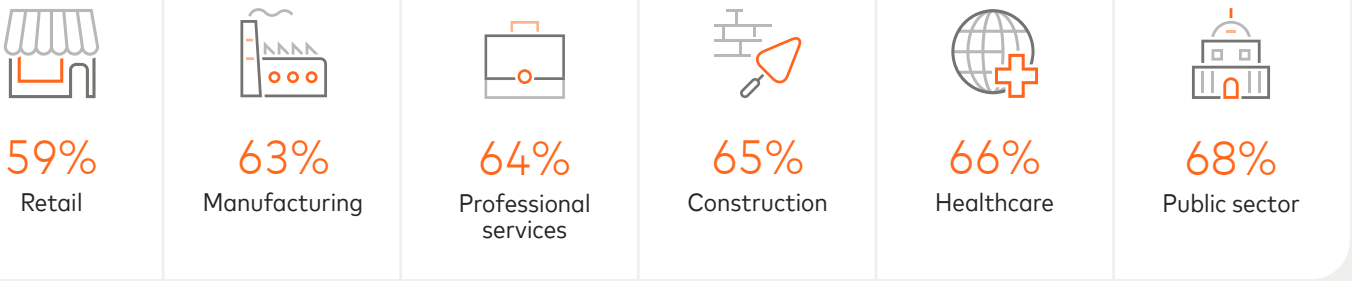
But we can't discount the impact of perception as well. How we think and feel about things can play just as large a part in how we choose to act. A fear of failure can leave us reluctant to take a risk, whereas powerful self-belief can see us taking chances that we might normally choose to ignore.

This tension, between the real and the imagined, plays a large role in cybersecurity and how we approach it. For SMEs, their perception of risk is keeping them on high alert as they try and navigate the reality of cyberattacks.

When asked if the threat of a cyberattack on their business was moderate or high, 63% of all SME leaders agreed. This awareness of risk was higher in certain sectors, such as healthcare, where two thirds (66%) of all SMEs believed themselves to be at high or moderate risk, and the public sector, where 68% of businesses see themselves as vulnerable.

In some notable places, these impressions align closely with the reality. Retail, for example, has the lowest perceived risk, and also reports the fewest attacks (60% of retail business leaders polled had experienced an attack at their current or previous organization, closely matching the 59% perception of risk). In other places, there are stark differences. While the public sector sees itself as uniquely vulnerable and does suffer a comparatively large volume of attacks (70%), it is the professional services sector which is actually the most attack-prone, with 77% of all business leaders reporting attacks at their current or previous place of work. However, only 64% of businesses in the sector perceive their risk as moderate or high — meaning they're underestimating their likelihood of being the target of an attack.

Lower risk ← **Perceived risk by industry** → Higher risk



Lower risk ← **Perceived risk by market** → Higher risk

Brazil	UK	UAE	India	US
50%	64%	66%	68%	69%

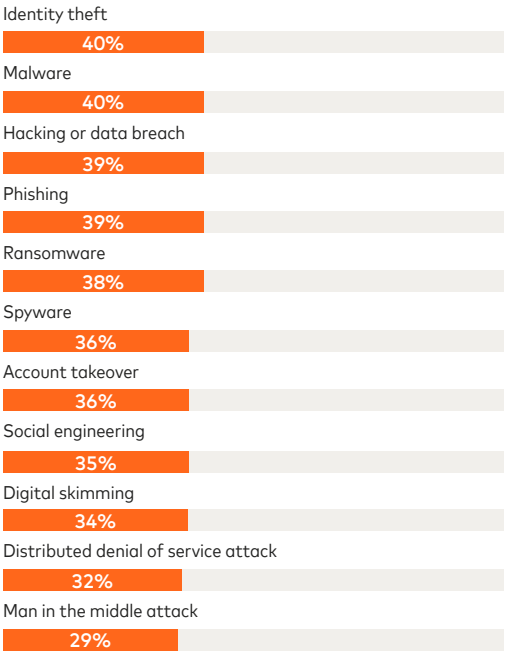
Perceptions of risk also differ from country to country. In Brazil, SMEs we spoke to were generally less concerned about risk, with only 50% of SMEs polled viewing their risk as moderate or high. This is a stark difference from reality, where 64% of small business leaders in the country had experienced an attack.

At the other end of the scale, SMEs in the U.S. view themselves as the most vulnerable, with 69% rating their risk as moderate or high. In actuality, businesses in the U.S. were the least likely to report having suffered an attack, with 55% of those polled having dealt with an attack at a current or previous company. While risk awareness is valuable, paranoia can be damaging in its own way. What is needed is an appropriate awareness of risk, and the tools and knowledge to manage it.

There is also a gap between perception and reality when it comes to the kinds of attacks that SMEs are facing. While the most common forms of attack reported are hacking or data breaches and malware (both 32% of recorded attacks), when it comes to threat familiarity, identity theft ranks as highly as malware, even though it only accounts for 28% of attacks.

Familiarity with threats

Global total



Confidence in short supply

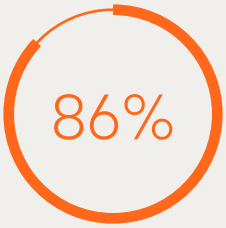
It's clear that SMEs are aware of the threats that challenge their cybersecurity. Whether they've suffered an attack themselves or are just conscious of the potential dangers they face, most SMEs have started to put in the groundwork to keep their businesses safe from attack. In fact, nearly nine out of every ten SMEs we spoke to (86%) have conducted an active cybersecurity risk assessment, and have a cyberattack prevention plan in place, showing that they understand the risks, and are taking steps to minimize them.

But that preparation does not translate to confidence. While SMEs are well aware of the risks and trying to respond, most are deeply unsatisfied with their current strategies. Less than a quarter of all SMEs (23%) say they are very satisfied with their cyberattack prevention plan, and the same percentage report that they're very confident in their ability to identify the cybersecurity threat to their business. While they're trying to mitigate their risk, the process isn't easy, with a full 75% of organizations saying they found evaluating their business' cybersecurity risk to be challenging.

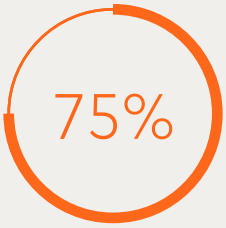
It's not just the threats themselves that are overwhelming. Understanding the cybersecurity world is also a daunting process, with 62% of respondents saying they found navigating the cybersecurity landscape to be intimidating. Keeping pace with the rapidly changing pace of threats also damages confidence, with 75% of business leaders telling us that staying up to date with cybersecurity is challenging. The acceleration of change is another confidence-sapping issue, with 70% agreeing that the emergence of AI makes them more concerned about attacks on their business.

This crisis of confidence exists within businesses as well. Employers are concerned about their staff's familiarity with cybersecurity, with 73% saying that getting employees to take cybersecurity seriously is a challenge, and only 25% feeling very confident in their ability to educate employees on best practices.

More than half of SMEs (55%) say their top reason for seeking out cybersecurity information is to help their employees follow best practices. When asked what the key challenge is when it comes to protecting their business, the leading answer was finding the right talent to manage organizational cybersecurity. SMEs need great talent to feel confidence in their security, but they need confidence to find and train great talent.



of SMEs have conducted an active cybersecurity risk assessment and have a cyberattack prevention plan.



of SMEs say evaluating their organization's cybersecurity risk is challenging.

of SMEs are very satisfied with their cyberattack prevention plan.

of SMEs are very confident in their ability to identify cybersecurity threats to their business.

Finding the knowledge

Who do you turn to when you have a problem that needs solving? Ideally, you can find an expert, someone who's familiar with your problem and has experience dealing with them. But that's not all people do. People also seek advice closer to home, asking their peers for their opinions. And sometimes, people just go online and try and find an answer on the internet.

When it comes to cybersecurity, SMEs are largely following the same kinds of processes. While getting help from industry experts is the top priority, many are also turning to social media to try and keep up with trends on cyberattacks.

Very few SMEs are keeping their head in the sand about the threats of cyberattacks. Altogether 93% of SME leaders told us that they actively seek information about cybersecurity and cybersecurity best practices, to stay informed and stay protected.

When they seek out that information, the majority are going to security consultants to try and get either the information (43%), or the solutions (41%) they need. Security consultants, with their deep specialisms in cybersecurity, are perfectly placed to provide accurate and up-to-date advice on protections from cyberattacks, and are a reliable choice of partner.

However, when it comes to cybersecurity information, more than a third of SMEs said that when they were looking for knowledge, they turned to social media. While social media sites with their enormous scale and large user bases can be platforms for useful information, SMEs need to be cautious about the channels they use, and the credentials of those offering advice. As well as social media, 30% of SME leaders said that online groups and forums were places they turned for information. Small business organisations and subject matter experts were the other most popular options that SMEs turn to.

These figures showed a few key differences when broken down into different sectors and regions. For example, those in the public sector said that they particularly valued subject matter experts (44% used it as a source, compared to 31% of SMEs in general), while they also looked to financial institutions for accurate information (34% of public sector respondents, compared to 26% overall). Meanwhile, those in the healthcare sector said that newsletters were one of their preferred ways to learn about cybersecurity, with 29% using them compared to 23% of SMEs in general.

There were geographical differences as well. Businesses in India rated social media higher as a source of information than any other nation polled (41% compared to 35% total), while in the U.S., small business organisations are more trusted (39% against 32% overall). In Brazil, there is a strong preference for subject matter experts, with 42% of SMEs using them as a source of information, compared to 31% of SMEs in all regions.

Top sources for cybersecurity information

#1	Security consultant	43%
#2	Social media	35%
#3	Small business orgs	32%
#4	Subject matter experts	31%
#5	Online groups / forums	30%

Top sources for cybersecurity solutions

#1	Security consultant	41%
#2	Social media	29%
#3	Small business orgs	29%
#4	Subject matter experts	28%
#5	Online groups / forums	25%

Where SMEs turn for help

When the worst happens, and SMEs find themselves as the target of a cyberattack, it is usually outside experts who are the first to get a call.

Speaking to SMEs who had found themselves on the receiving end of an attack, the first step taken by 40% of all respondents was either to engage their cybersecurity solutions partners, or to engage a cybersecurity professional such as a security consultant.

Seeking expert assistance took priority even over steps such as shutting down all computer systems, or identifying the cause of an attack. The prioritization of consulting with an expert shows the deep reliance that SMEs have on their cybersecurity partners. Before they can take active steps to minimize the impact of the attack, or inform their staff or other affected partners, they need the reassurance and support of experts who can guide them through the process and help them handle the fallout.

First step they took after an attack

Among those who have experienced an attack

#1	Engage their cybersecurity solutions partners	21%
#2	Engage their cybersecurity professionals (e.g., security consultant)	19%
#3	Identified the cause of the attack	13%
#4	Recovered lost data	12%
#5	Informed everyone in the company	11%
#6	Shut down all computer systems	9%
#7	Contacted lawyers or getting legal advice	9%
#8	Notified affected parties	6%

When asked more generally about who they would opt to turn to if they were targeted in an attack, it was again cyber solutions providers who were the most sought after. More than a third of SMEs (35%) said that dedicated cyber solutions providers would be their top choice for helping in the wake of a cyberattack, ahead of general IT consultants (21%), government cybersecurity agencies (10%), or financial technology companies (7%).

There is clearly a strong desire among SMEs to have access to credible cybersecurity professionals, who have deep experience and knowledge of the sector and the practical tools to help with the impact of a cyberattack.

This is borne out when SMEs were asked about if they have already invested in their cybersecurity, or where they would invest in future. For those who have already purchased cybersecurity solutions, half of all SMEs we polled said they bought them from a dedicated cyber solutions provider. General IT consultants were the follow-up choice, with 43% buying their cybersecurity tools from one. Between 25% and 28% of SMEs had sourced their solutions from fintechs, e-commerce businesses, payment networks or financial institutions.

For those who are considering finding a partner for their cybersecurity solutions, dedicated cybersecurity providers were the most popular choice, with more than a third of businesses (35%) listing them as their preferred option. IT consultants came in second preference, with 16% of SMEs willing to partner with them, and no other option was as popular. In third place was government cybersecurity agencies, at 10%, showing there is some level of trust for government-backed tools over commercially available options.

Who they would turn to for help after an attack

Global total

#1	Cyber solutions provider	35%
#2	IT consultant	21%
#3	Government cybersecurity agencies	10%
#4	Financial technology companies	7%
#5	Banks / financial institutions	6%
#6	E-commerce businesses	5%
#7	Telecommunications companies	5%
#8	Local software sales rep	5%
#9	Payment networks	5%

Where SMEs have purchased / would purchase cybersecurity solutions

The tools SMEs want

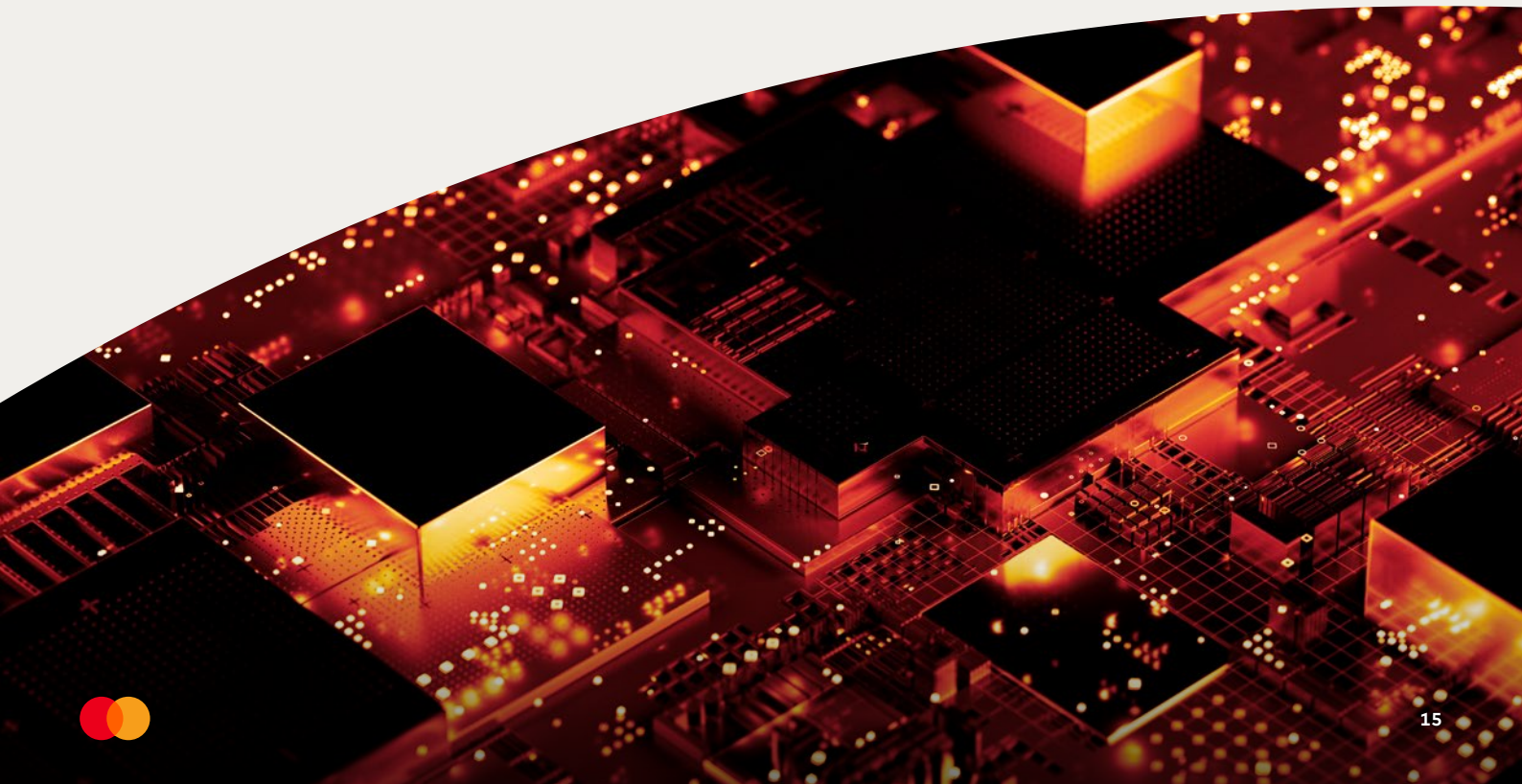
SMEs don't come in a single shape or size, and the cybersecurity solutions they're looking for are as diverse as they are. Businesses understand the threats they face come in different shapes and sizes too, and the tools they need reflect that complicated landscape.

What they do have in common is a general need for solutions that keep them safe. The vast majority of businesses across all sectors (88%) said they were very or somewhat open to implementing new cybersecurity solutions, with 91% of retail businesses open to the idea. In general, most SMEs (57%) said they would prefer to purchase cybersecurity solutions in a bundle or package, aiming to cover as many eventualities as possible, while 43% would prefer a la carte options, picking and choosing the tools they need for specific use cases.

When asked about specific solutions, there were a number that businesses sought out. The most popular choice was vulnerability assessment tools — businesses are keen to understand their own risk profile, fy any weaknesses in their systems or practices, and start taking steps to mitigate them. Services that monitor vendor and third-party cybersecurity risk were the second-most popular option, as businesses look to expand their visibility not just of their own risk profiles, but of those they do business with, which can have direct impact on themselves. Securing the help of a third-party IT and security team was the third most popular option.

Cybersecurity solutions most likely to consider

#1	Vulnerability assessment tools
#2	Service to monitor vendor / third-party cybersecurity risk
#3	Third-party IT and security team
#4	ID theft protection
#5	Phishing solutions
#6	Internal cybersecurity team



The most popular solution varied widely by industry, in line with the different kinds of challenges and threats faced in different sectors. While retail matched with the overall preference for vulnerability assessment tools, healthcare businesses are more preoccupied with ID theft as a risk, and their need is for ID theft protection tools. The public sector's top ask was more fraud protection, while the construction sector priorities are phishing solutions.

When it comes to how much SMEs are willing to spend on these solutions, the totals vary according to a range of factors, including the type of industry, the size and age of the business, and an executive's particular experiences with cybersecurity.

As may be expected, the larger a business is, the more it expects to spend on cybersecurity solutions — 61% of medium businesses are spending more than $2,000 a month: conversely, 58% of small businesses are spending less than $2,000 each month. The age of a business is another key factor. Those who have been in business between five and nine years spend on average $1,000-$2,999 each month, while those who have been operating for over a decade spend on average more than $3,000 each month. At the other end of the scale, businesses which are still in the early stages, and have been running for less than five years, are only spending on average less than $1,000 a month on their cybersecurity.

The type of industry plays a large factor in typical spending. Retail and construction are some the sectors which record the lowest numbers of cyberattacks, and their spending correlates, typically less than $1,000 a month. Professional services and the public sector, which experience cyberattacks at a higher rate, are more likely to spend $3,000 and above each month on their protection.

Experience also plays a key role, as 56% of those who have conducted a cybersecurity risk assessment are likely to pay more than $2,000 a month for their solutions, compared to just 25% of businesses who have not conducted an assessment.

Top considered solution by industry

#1	Vulnerability assessment tools
#2	Service to monitor vendor / third-party cybersecurity risk
#3	Third-party IT and security team
#4	ID theft protection
#5	Phishing solutions
#6	Internal cybersecurity team

Cybersecurity decision drivers

SMEs are increasingly aware of the threats they face and know the kind of tools they need to protect themselves. But there are several factors that affect how they make the decision to purchase those solutions. They are motivated by different goals, held back by a few concerns, and, like all consumers, swayed by influences such as price, familiarity and trust.

The chief motivator for SMEs when looking to purchase cybersecurity solutions is ensuring operational resilience and combatting growing threats. As SME leaders become more familiar with increase in threats, they understand the potential risks to the smooth running of their business, and it's natural that ensuring resilience would be their key concern.

It's also worth noting that businesses are largely proactive when it comes to their choices. In general, they're driven by their concerns and desires to make an active choice, rather than making the choice because its mandated or comes bundled with something else.

As well as internal pressures, there are external drivers. Complying with regulations and data protection laws is a key motivator to adopt new cybersecurity solutions, as are mandates from insurance firms. Organizational growth is also a key factor in investing in greater cybersecurity, while many are simply pushed into action by being on the receiving end of an attack.

Top motivators for purchasing cybersecurity solutions

Cybersecurity solutions users (summary of top 3 rankings)

#1	Ensuring operational resilience of the business	47%
#2	Increased prevalence of threats	46%
#3	Regulation / compliance with new data protection laws	44%
#4	Organizational growth required it	44%
#5	Security issue / attack triggered the purchase	44%
#6	Bundled with other software and / or default setting	38%
#7	Insurance company mandated or requested it	38%

At the other end of the scale, there are numerous factors that stand in the way of businesses adopting new cybersecurity tools. Many SMEs are still unsure of which types of solutions they should prioritize, or find there are too many options to choose from. Lots of businesses are simply held back by the issue of costs — the solutions they want are seen as too expensive.

When it comes to choosing a cybersecurity partner, a lot of the drivers behind decision making are practical issues of adoption. How easy are the solutions to integrate into our own systems? Are they suitable for the size of our business? They're also pushed by common factors that lots of customers have when making a purchase: does this provider have a good reputation? Am I familiar with the brand? How much relevant experience to they have? Do they have a local footprint? And once again, how much does the service cost?

Reaching SMEs with useful solutions means navigating these drivers and answering these questions.

Top barriers to purchasing cybersecurity solutions

Cybersecurity solutions non-users (Multi-select)

#1	Unsure what types of solutions to prioritize	33%
#2	It is too expensive	31%
#3	Too many products to choose from	29%
#4	Haven't had time to look into it	29%
#5	Not necessary for type of organization I run	29%
#6	Haven't had a need to look into it	28%
#7	Not necessary for my business	25%
#8	Don't know whot to trust or go to for solutions	8%

Top influencers on cybersecurity solution partner selection

Global total (summary of top 3 rankings)

Ease of use / integration (33%)

Provider has range of solutions / can tailor (32%)

Experience specific to org's industry (31%)

Price (31%)

Provider has local footprint (30%)

Well-established trust in provider (29%)

Provider has solutions for small- to medium (29%)

Long tenure / experience with cybersecurity (29%)

Adherence to compliance required by industry (28%)

Familiarity with brand (27%)

Conclusion

Cybersecurity isn't an afterthought for SMEs — it's an essential, everyday safeguard against increasingly sophisticated and pervasive threats. The stakes are high: SMEs are vital to the people they employ, the communities they serve, and the broader economy they help drive.

Fortunately, SMEs do not have to face these threats alone. The climate of fear and doubt that can accompany cyber risk does not need to define their experience in the digital economy. Instead, with the right support, SMEs can build the confidence they need to participate fully and securely. Organisations like Mastercard, with deep expertise in monitoring fraud and cyber threats, are uniquely positioned to help SMEs protect themselves from these threats, alongside trusted partners that are ready to stand beside them, offering knowledge, support, and practical solutions to empower business owners and their teams.

A key insight from our research is that SMEs do not want to become cybersecurity experts — they want solutions that keep their businesses safe without requiring deep technical knowledge. The appetite for high-quality assistance is clear, whether from dedicated cybersecurity providers or from partners like Mastercard. Tools such as the Mastercard Trust Center, My Cyber Risk and ID Theft Protection are designed to provide accessible, actionable resources and personalised risk assessments, helping SMEs understand their vulnerabilities, prioritise remediation and protect against identity theft. These initiatives, alongside a growing network of partnerships, are making it easier for SMEs to access the support they need. Millions of merchants worldwide can also access Mastercard's risk scoring and evaluation capabilities combined with VikingCloud's cybersecurity remediation solutions.

However, barriers remain. Cost, trust, and a lack of clarity about which tools are most effective can prevent SMEs from accessing the help they require. It is essential for solution providers to find new ways to reach and support SMEs, demonstrating expertise and offering practical, tailored guidance.

By working together — businesses, partners, and solution providers — we can ensure that SMEs are not only protected from cyber threats, but are also empowered to achieve long-term success in an increasingly digital world.

Let's strengthen SME cyber resilience, together

If you want to know more about how you can be a trusted partner for SMEs, supporting their growth and empowering them to reach their goals, Mastercard is ready to help.

Get in touch today to learn more about how we can work together, through insights, collaboration, and scalable solutions, to help SMEs stay secure and succeed in our digital economy.

Contact Mastercard