

Big Security in a Small Business World

10 myth busters for SMB cybersecurity



Contents

Is your cybersecurity protecting your organization as intended?	3
Exploring 10 myths.	5
SMB vs. large enterprise security postures	5
Myth 1: Only large organizations face public scrutiny – in all its forms	5
Myth 2: Larger businesses suffer less downtime and recover faster from attacks.	7
Myth 3: SMBs lack personnel dedicated to security	8
Myth 4: Large businesses have more updated infrastructures	9
Myth 5: SMBs face different threats than larger businesses	10
Myth 6: SMBs don't proactively perform threat hunting	12
Myth 7: Smaller businesses don't test their incident response plans with drills/exercises	13
Myth 8: For whatever reasons, SMB leadership doesn't take security and data privacy seriously	14
Myth 9: Smaller organizations don't regularly patch vulnerabilities	17
Myth 10: SMBs can't measure the efficacy of their security programs	18
Seizing opportunities to optimize your security	19
Cybersecurity fatigue	19
Employees' adoption of cybersecurity awareness	19
Reducing downtime	21
Vendor complexity	22
Resources to secure your journey forward.	23
Securing your remote workforce	24
About our experts	25
About the Cisco Cybersecurity Report Series	25

Is your cybersecurity protecting your organization as intended?

If you own or work for a small or medium-sized business (also referred to as SMBs), you've already overcome significant challenges. From raising seed money and knowing when to hire, to managing operational costs and strategizing to scale... it's tough. Exhilarating, meaningful, and personal... but tough.

And when you're faced with an unprecedented situation, like trying to keep your operations afloat through a pandemic or recession, how do you manage? What should you focus on to stay secure? How do you cover your organization from cyberattacks if you're operating with a reduced staff?

Those entrepreneurial instincts kick in. In times of crisis, by necessity, fresh ideas emerge while you adapt to new approaches to working. You come up with ways to stay productive and competitive, against all odds.

Does cybersecurity play a major part in this when there are so many other emergent issues to consider?

You bet it does! This report is designed to give you insights into exactly how cybersecurity can play a crucial role in empowering small and medium-sized organizations to not only survive, but thrive and accelerate success. How are we doing this? By using data to debunk the pervasive myths that are misguiding SMB security assumptions.

The security industry has often been unjustly harsh towards small and medium businesses when it comes to recognizing how you prioritize cybersecurity. It may have seemed as though vendors pandered to you, assuming you don't take security seriously, and proceeded to explain it to you ("cybersplaining," if you will).

This report – based on a survey of almost 500 SMBs (defined here as organizations with 250–499 employees) – reveals that not only do you take security very seriously, but that your innovative and entrepreneurial approach to security is also paying dividends. It's time to bust some myths about the way in which SMBs are using their cybersecurity resources.

We'll be using our annual [CISO Benchmark survey](#) findings and our outcomes from conversations with small and medium-sized businesses to debunk myths – on topics such as how many SMBs have departments dedicated to proactive threat hunting, and the types of cyber threats that you face.

In other words, we'll be putting the magnifying glass on the key factors that are impacting your cybersecurity. For example, we learned about the consequences that an outdated infrastructure can have on a breach, and how long it lasts. We also learned that the more vendors you use, the longer your downtime from your most severe breach. We'll explore your most impactful strategies, and we'll present data demonstrating that your businesses are rebounding more quickly after a data breach than the industry previously expected.

If all the pressures of being a small business are not enough, it's now apparent that external pressures can force some or all of your workforce to be remote at any time. As [Graham Cluley](#), independent cybersecurity analyst and blogger recently stated in his newsletter, “We may be working from home, but the hacks keep on coming.” We might be having to adjust to different ways of working than we're used to, and when times are hard, prioritizing is essential.

What this report aims to do is highlight which strategies are working. We hope this helps with the decisions you're making about how you and your workforce manage security in the future, and how cybersecurity can help empower you to accelerate your success.

“Security plays an important part in our organization. We perform backend functions for three credit unions in the USA, as well as a combined call center. Security helps us bring key aspects of our business together for operational efficiency.”

Kevin Hatch, Network Engineer,
Open Technology Solutions

Exploring 10 myths

SMB vs. large enterprise security postures

To evaluate common myths held about SMB security postures, we compared survey responses across various cybersecurity capabilities for SMB (250–499 employees) versus larger organizations (500 employees or more).

What we uncovered in our research data debunked several myths. Here, we investigate those myths and provide data to disprove them – leaving SMBs in better security shape than anyone perceived.

Notes:

1. For the purposes of this research, we defined small to medium-sized businesses, or “SMBs,” as employing 250–499 employees. Keep in mind that survey data may very well be different in organizations with less than 250 employees.
2. All percentages are rounded, and we’ve omitted the small percentage of “Don’t Know” responses to survey questions. For these reasons, accounting may not always total 100% in the graphs provided. Survey data source: [Cisco 2020 CISO Benchmark Study](#).

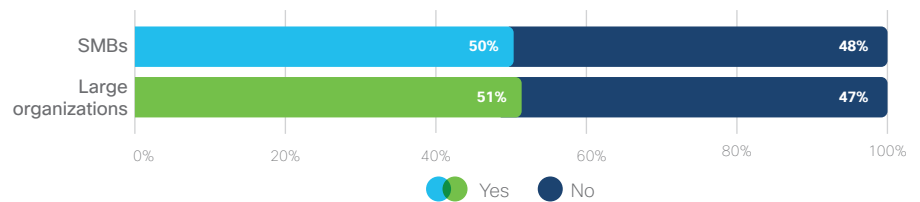
Myth 1: Only large organizations face public scrutiny – in all its forms

One common myth is that the media only wants to talk about massive and devastating corporate or governmental data breaches. This could lead some smaller organizations into believing that they won’t face much, if any, public scrutiny when they suffer a cyberattack.

FALSE: Last year, smaller organizations faced about the same level of public scrutiny as their larger counterparts.

Figure 1 shows that there isn't substantial evidence for a difference in SMBs and larger organizations in whether they face public scrutiny.

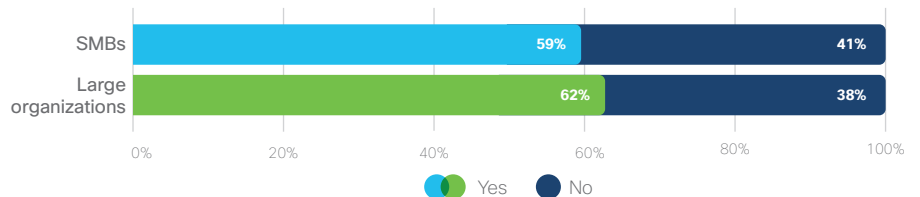
Figure 1. Has your organization ever had to manage public scrutiny from a security breach? SMB N=481; 500+ N=2319.



Source: Cisco's Big Security in a Small Business World Report, 2020

Secondly, 59% of SMBs voluntarily disclosed their most significant data breach last year (compared to 62% of larger businesses). This suggests that smaller businesses take their commitment to their customers and partners seriously.

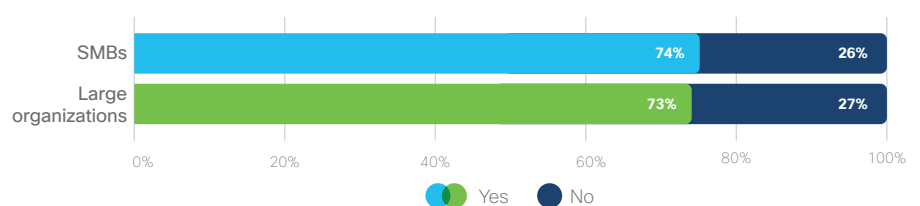
Figure 2. Did last year's most significant security breach that had to be managed under public scrutiny become known to the public because of your organization's voluntary disclosure? SMB N=241; 500+ N=1190.



Source: Cisco's Big Security in a Small Business World Report, 2020

Thirdly, smaller businesses overwhelmingly receive inquiries from customers about how they're handling their data, versus not receiving inquiries. Seventy four percent of SMBs told us that customers/prospects have made these inquiries (similar to 73% of larger organizations). This demonstrates that customers care that their personal data remains private no matter who has it, and that the element of trust with whom they give it to is clearly crucial.

Figure 3. Do your customers (or prospects) inquire about data privacy and your handling of personal information? SMB N=432; 500+ N=2117.



Source: Cisco's Big Security in a Small Business World Report, 2020

The reason SMBs are receiving these inquiries is that regulations and vendor risk management flow downstream. It starts with the big companies. Then the big companies audit their vendors, the mid-sized companies. And then a couple

years later, the mid-sized organizations are auditing their vendors, the smaller companies. Driven by breaches or data privacy, SMBs are not immune to inquiry – and they should be held as accountable as their large counterparts.

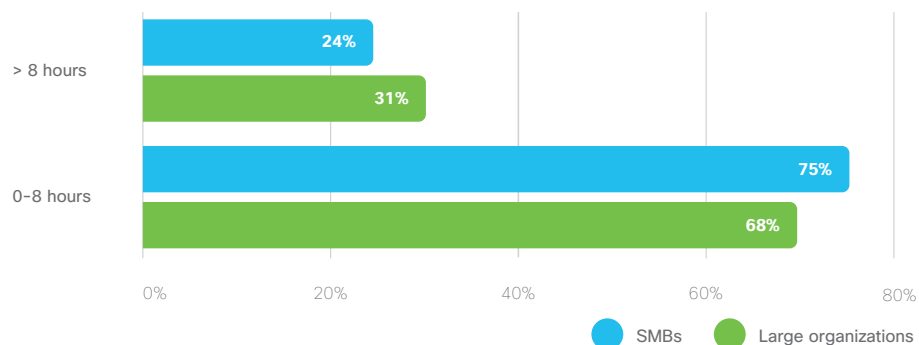
Myth 2: Larger businesses suffer less downtime and recover faster from attacks

When an SMB gets hit by a cyberattack that results in a level of downtime (loss of business hours), the myth suggests that they don't have the resources to rebound nearly as fast as their larger counterparts.

FALSE: Our data suggests that there is very little difference in the amount of downtime suffered by SMBs and larger organizations.

If we summarize some of these findings, we can see that 24% of SMBs faced downtimes of more than eight hours last year for their most severe security breach, slightly below larger organizations at 31%.

Figure 4. Thinking back to the most severe security breach your organization managed in the past year, how long were systems down due to the breach? SMB N=388; 500+ N=1877.



Source: Cisco's Big Security in a Small Business World Report, 2020

We also compared these figures to the Cisco “Small and Mighty” SMB report from 2018, and there have been some significant improvements made over the last two years for smaller organizations. Two years ago, 40% of SMBs endured downtime of more than eight hours after their most severe breach.

It needs to be acknowledged here that a severe breach can cause huge disruptions – across any sized business. This isn't about who has the longer levels of downtime, but what your SMB can do to ensure your resources aren't stretched beyond their capabilities. This is where [automation](#) can be a force multiplier to provide early warning and fast recovery to minimize downtime and keep your business afloat in such times of adversity. According to our [2020 CISO Benchmark Report](#), a majority (77%) of respondents from all sized organizations are planning to increase automation to simplify and speed up response in their security ecosystems over the next year.

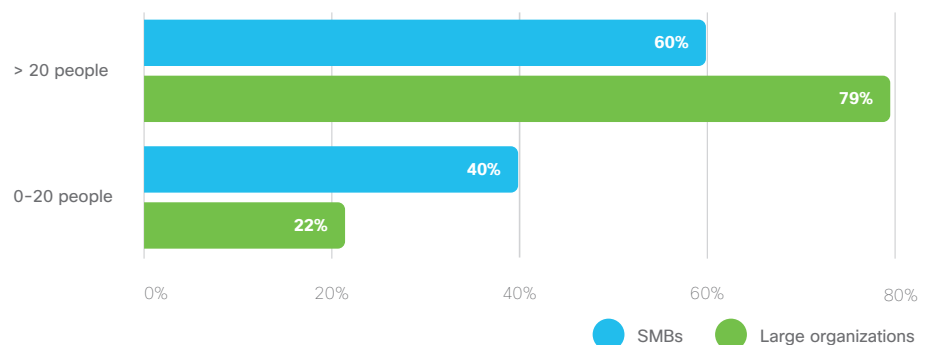
Myth 3: SMBs lack personnel dedicated to security

With everyone pitching in wherever necessary in SMBs, there's an assumption that cybersecurity is just one aspect of someone's job. And that this person is also balancing other aspects of IT management such as managing data centers and evaluating new hardware. The myth is that SMBs have few, if any, dedicated resources for cybersecurity.

FALSE: While this may be the case for some, SMBs overwhelmingly told us that they do have dedicated employees for cybersecurity. In fact, less than 1% of SMBs told us that they didn't have anyone dedicated to security. Perhaps even more surprising, 60% said they had over 20 people dedicated to security – although we didn't specify what level of involvement that dedication may entail or if the employees were outsourced with a managed security service provider (MSSP).

And how does that compare to larger businesses? The percentage of larger organizations who have more than 20 people dedicated to security is significantly higher (79%), which is to be expected.

Figure 5. How many employees in your organization are dedicated to security? SMB N=481; 500+ N=2319.



Source: Cisco's Big Security in a Small Business World Report, 2020

These figures show that SMBs have more dedicated security resources than perhaps we first thought. Does this mean that the cybersecurity talent shortages are no longer an issue for SMBs?

We certainly wouldn't go that far.

SMBs told us that a lack of trained personnel is actually their third biggest challenge. Their top challenge is budget constraints, followed by compatibility with legacy systems. Third place is tied between trained personnel and jointly competing priorities.

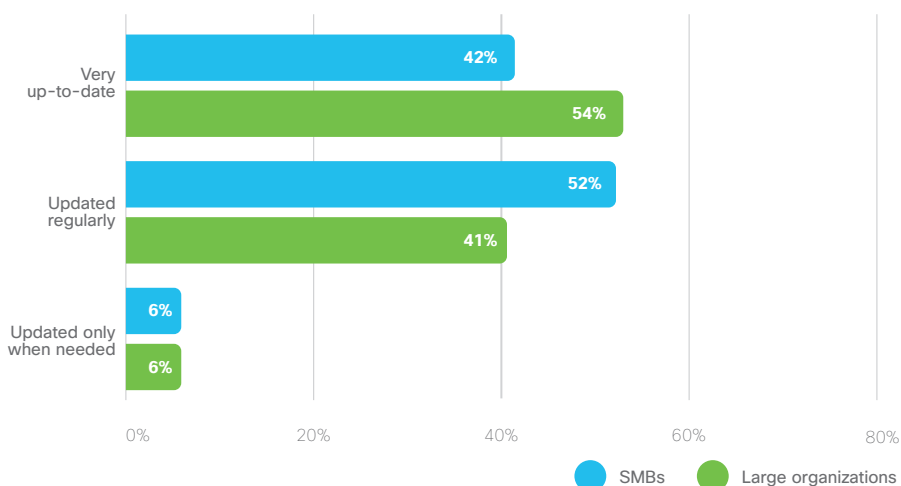
Consider this a sign of the cybersecurity challenge facing smaller businesses – they recognize they’re a target, and that attacks against them are getting increasingly sophisticated. In order to combat that, they’re putting themselves in the best possible position. And for SMB organizations, that means investing in the right people.

Myth 4: Large businesses have more updated infrastructures

With the frequency of consumers upgrading to the latest smartphone, it may seem that larger organizations can afford to replace each element of their security infrastructure. But what about smaller businesses, where that cycled investment might have greater impact on their annual IT budget?

PARTIALLY TRUE: When asked to describe their infrastructures, and their strategy for investing and replacing key security technologies, here’s what SMBs told us: Almost all SMBs are diligent about keeping their infrastructure up to date.

Figure 6. How would you describe your organization’s security infrastructure? SMB N=481; 500+ N=2319.



Source: Cisco's Big Security in a Small Business World Report, 2020

It's true that SMBs don't have quite as up-to-date infrastructures as larger businesses (54% of large businesses say they are very up to date, compared to 42% of SMBs). However, a collective 94% of SMBs say they either update regularly or constantly. Thus, the vast majority are certainly not holding onto old equipment until it becomes obsolete and insecure.

For SMBs, it's about maximizing what they have, rather than chasing every shiny new security product. Many times, we've seen our SMB customers thinking outside the box to stretch their security even further.

“As a small business, we need as much information from as few systems as possible to maximize efficiency. Our cloud-based security solution (Cisco AMP for Endpoints) has proven to be a crucial system for operating our entire infrastructure. It's not only important for securing the assets, it also provides instant access to machine information, user environments, and reporting to assist with help desk troubleshooting. This eliminates the need for a separate software system. We're constantly able to learn and adapt by operating this way.”

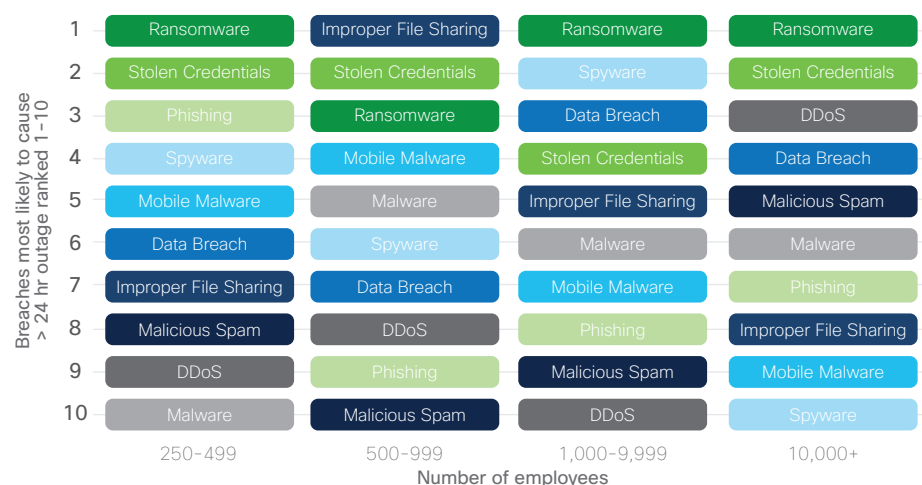
Alan Zaccario, Vice President, Information Technology and Cybersecurity, New Castle Hotels and Resorts

Myth 5: SMBs face different threats than larger businesses

Cyber criminals want the biggest prize, so they'll use their most stealth and dangerous tactics against the larger businesses, right?

PARTIALLY TRUE: We compared the types of cyberattacks that SMBs and large enterprises reported they've experienced in the past year, with how much downtime (loss of business hours) the attacks caused. We did this using four categories based on organizational number of employees and ranked the events most likely to create more than 24 hours of downtime.

Figure 7. Number of employees correlated with downtime in hours due to most severe breach in the past year and which type of attack caused it. 250-499 N=388; 500-999 N=746; 1,000-9,999 N=863; 10,000+ N=268.



Source: Cisco's Big Security in a Small Business World Report, 2020

The results are interesting in terms of which threats cause the most damage. What we found is that ransomware doesn't discriminate. For both the SMBs and large enterprises, ransomware was the #1 most likely threat to cause more than 24 hours of system downtime.

DDoS in contrast rarely causes the most impact for smaller organizations but is the third most destructive attack type in terms of downtime for 10,000+ employee organizations. In contrast, phishing is reported to be a large problem for small organizations but is well down on the scale for larger organizations.

Attackers who deploy wiper malware have a singular purpose of destroying or disrupting systems and/or data. For both SMBs, and enterprises with more than 10,000 employees, wiper malware caused downtime of between 17 and 24 hours in the last year. Unlike malware that holds data for ransom (ransomware), when a malicious actor decides to use a wiper in their activities, there is no direct financial motivation. For businesses, this is often the worst kind of attack, since there is no expectation of data recovery.

Stolen credentials also appear to be a significant problem for SMBs, causing on average 17-24 hours of downtime in the last year.

Also to consider is that some threat actors specialize in certain sized companies, verticals, or geographical regions. Therefore, while the tactics may be comparable (as shown in the previous figure), threat actors are themselves different.

Myth 6: SMBs don't proactively perform threat hunting

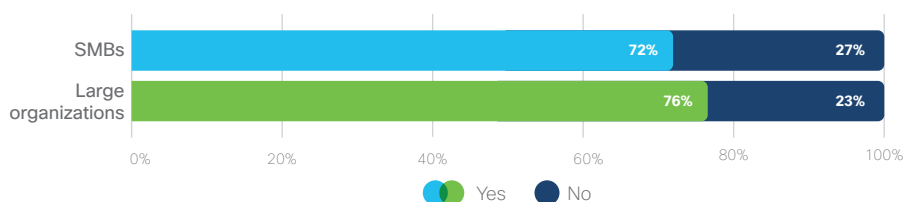
Threat hunting is a proactive security exercise, with the intent of finding and rooting out attackers that have penetrated your environment and haven't raised any alerts. This contrasts with traditional investigations and responses that stem from alerts that appear after potentially malicious activity has been detected.

The whole concept of threat hunting sounds like it involves a mysterious crime scene investigation, with its nuances and complexity out of reach for smaller businesses. SMBs have their hands full trying to investigate alerts; they don't have time to go hunting for other threats, right?

FALSE: From our survey data, not only do 72% of SMBs have employees dedicated to threat hunting, but this is also close to the percentage of large organizations who have a threat hunting department.

Although their levels of maturity may differ from larger organizations due to less resources, our data suggests that SMBs recognize the value of, and are embracing a proactive approach towards cybersecurity.

Figure 8. Does your organization have an internal department or team dedicated to threat hunting? SMB N=481; 500+ N=2319.



Source: Cisco's Big Security in a Small Business World Report, 2020

You can read more about the practice of threat hunting and how other businesses are doing it in our recent report, [Hunting for Hidden Threats: Incorporating Threat Hunting Into Your Security Program](#).

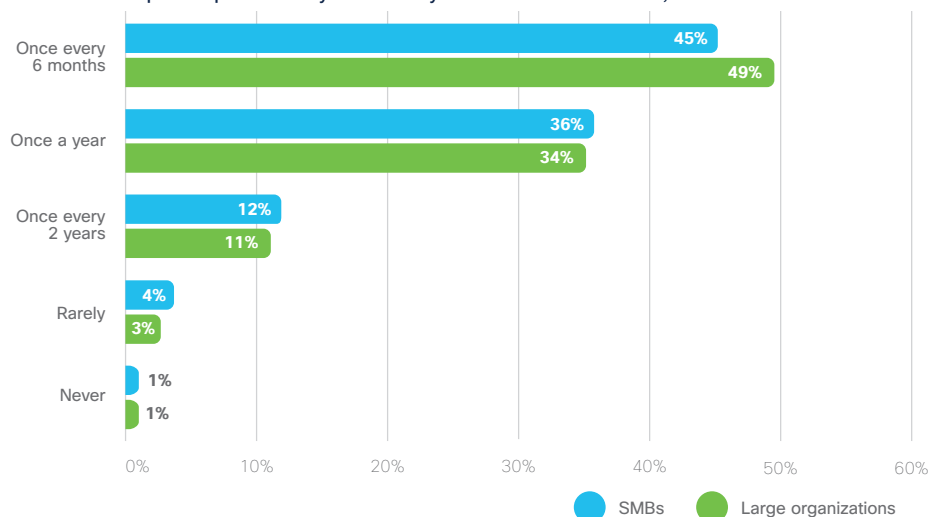
Myth 7: Smaller businesses don't test their incident response plans with drills/exercises

As Mike Tyson often said, “Everyone has a plan until they get punched in the face.” Until you know how your incident response plan performs in action, it's only worth the words on the page.

But smaller businesses don't have the luxury of time and resources to test their plans, right? Surely that would cause more disruption than it would be worth.

FALSE: This myth is simply not true. Only one percent of SMBs never test their plan, and four percent rarely test. Twelve percent test every two years, 36% test annually, and the largest percentage (45%) test every 6 months.

Figure 9. How often – if ever – does your organization conduct a drill or exercise to test its response plan to a cybersecurity incident? SMB N=481; 500+ N=2319.



Source: Cisco's Big Security in a Small Business World Report, 2020

How does that compare to larger businesses? The results are very similar, so the notion that SMBs don't plan as well as larger businesses is debunked in the context of incident response.

Myth 8: For whatever reasons, SMB leadership doesn't take security and data privacy seriously

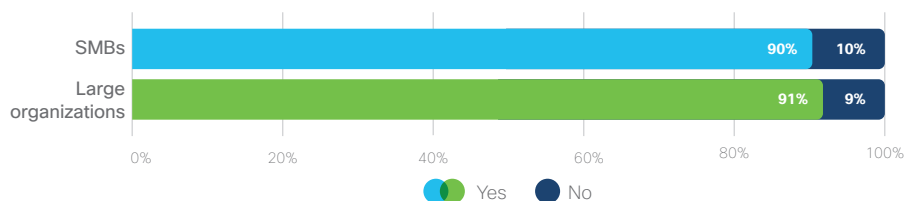
Here's the big one – the one that the collective industry has unfortunately been peddling for years. As an SMB, you're in the dark on how much danger you're in – and haven't nurtured an organizational culture around security and data privacy.

FALSE: Our data proves that this myth is very far removed from the actual truth. And there are three ways to prove this from our survey of IT decision-makers from different sized organizations.

Data privacy

First, our data shows that 90% of IT decision makers within SMBs say they are familiar with their data privacy program, compared to 91% in larger companies – not much of a difference.

Figure 10. Are you generally familiar with the data privacy program at your organization?
SMB N=481; 500+ N=2319.

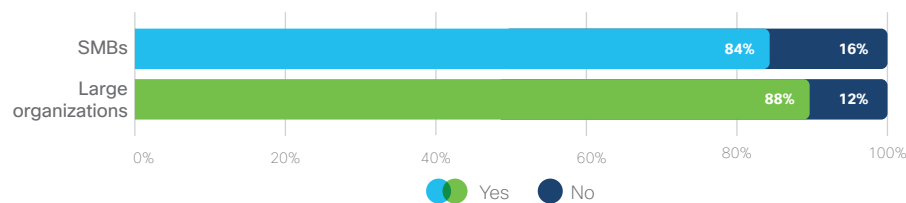


Source: Cisco's Big Security in a Small Business World Report, 2020

Cybersecurity awareness training

Secondly, at 84%, the majority of SMB organizations make security awareness training mandatory, and only at a slightly lower rate than larger organizations.

Figure 11. Is employee cybersecurity awareness training mandatory in your organization?
SMB N=464; 500+ N=2272.

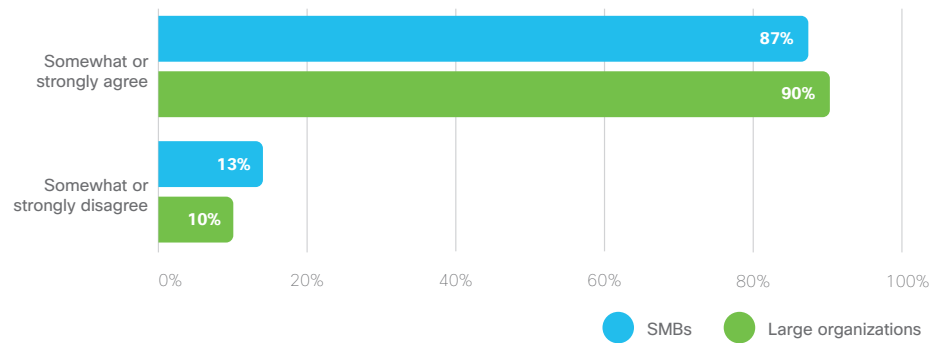


Source: Cisco's Big Security in a Small Business World Report, 2020

Executive buy-in

Thirdly, 87% of executives in SMBs agree that security is a high priority. This is just three percentage points behind larger businesses.

Figure 12. Executive leadership at my organization considers security a high priority.
SMB N=481; 500+ N=2319.

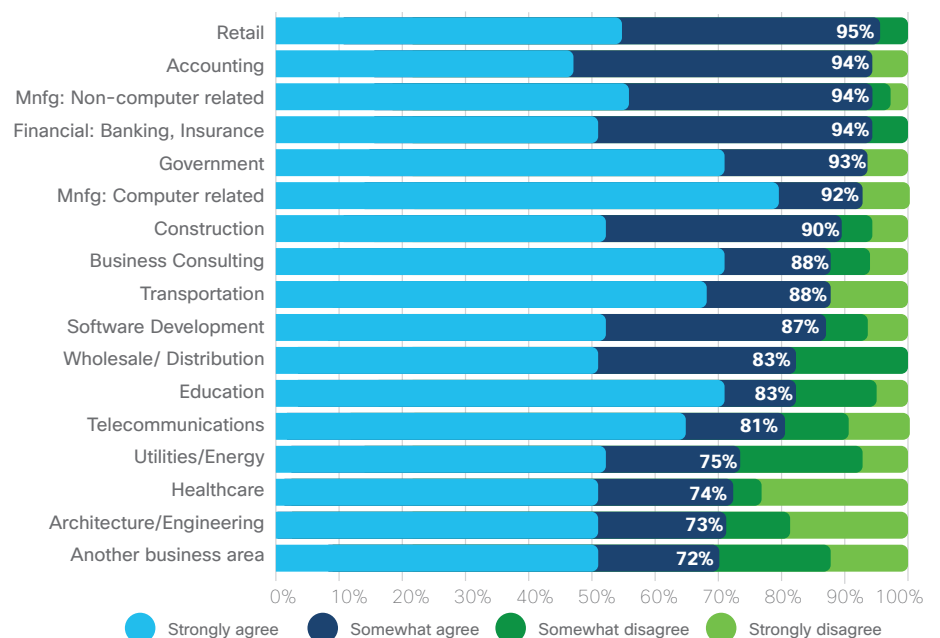


Source: Cisco's Big Security in a Small Business World Report, 2020


We often hear from our customers (and we agree) that security must permeate across the business to have any effect, and that executive support is critical to operationalize security. This is as true for an SMB as it is for a larger organization – and in most cases, easier to achieve in a presumably more agile environment.

Based on the findings to these three survey questions, we find SMBs have, in fact, nurtured organizational cultures around security and data privacy. More than two thirds of respondents across all industries said their executive leadership considered security to be a high priority (see Figure 13 showing only SMB responses).

Figure 13. Executive leadership at my organization considers security a high priority.
SMB N=481.



Source: Cisco's Big Security in a Small Business World Report, 2020

A black and white photograph of a historic brick building with a street lamp in the foreground. The building has multiple stories with arched windows and a decorative cornice. The street lamp has several white globe lights. A green rectangular box is overlaid on the right side of the image, containing white text.

“For our phishing tests, the point is not to show the rate at which users click on everything, it’s more about the reporting. Everyone can click a wrong link, but if you don’t report that something unexpected happened, you’re hurting your business even more.”

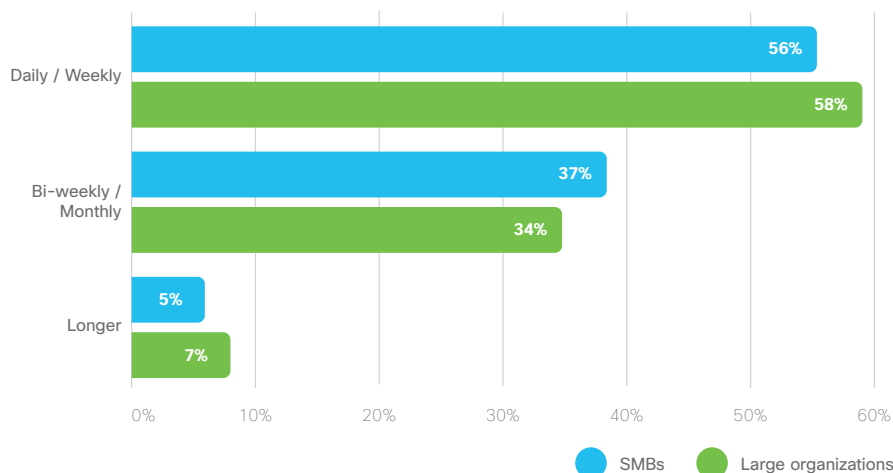
Wouter Hindriks, Technical Team Lead, Network & Security,
Missing Piece

Myth 9: Smaller organizations don't regularly patch vulnerabilities

Patching often falls under the basics of cybersecurity, but in practice, it can be challenging to implement. One myth suggests that SMBs would rather use their resources elsewhere than find ways to minimize the disruption caused by patching.

FALSE: Fifty-six percent of SMBs patch daily or weekly, compared to 58% of large businesses – showing that for the very regular patching routines, all business sizes approach it the same.

Figure 14. How regularly does your company patch disclosed vulnerabilities in software?
SMB N=481; 500+ N=2319.



Source: Cisco's Big Security in a Small Business World Report, 2020

Our data shows that enterprises and organizations with between 500-999 employees are the most likely to experience an incident from a vulnerability that is known, showing that those in the SMB category are actually more effective at patching known vulnerabilities than some larger businesses, resulting in fewer incidents.

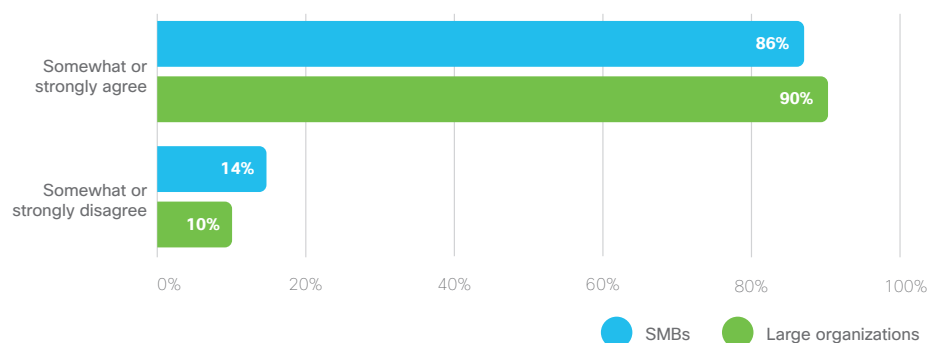
Patching is critical as a first defense, as defined for example in the U.S. by [NIST SP 800-53](#) and the [Center for Internet Security® \(CIS®\)](#). And SMBs are proving that.

Myth 10: SMBs can't measure the efficacy of their security programs

Assumptions have been made that smaller businesses employ more of a 'spray and pray' approach to cybersecurity. The implication is that they don't have the measures in place to be able to monitor and measure what's really working, and therefore can't optimize what they have.

FALSE: An impressive 86% of SMBs say they have clear metrics for assessing the effectiveness of their security program, compared to 90% of larger organizations.

Figure 15. My organization's executive team has established clear metrics for assessing the effectiveness of our security program. SMB N=481; 500+ N=2319.



Source: Cisco's Big Security in a Small Business World Report, 2020

Our survey data showed that there is minimal difference in the use of clear metrics no matter the size of organization. This may be partially due to the way cybersecurity products have evolved over the years; the best ones are designed to give very clear indicators of what they're finding, and what it means, in order to make reporting easier.

But with the importance of 'You can't fix what you can't measure,' SMBs could do better, as only 46% responded that they *strongly agree* their executives have established clear metrics, versus 53% of large organizations.

Seizing opportunities to optimize your security

While we've proven that SMBs deserve a much better reputation for having strong security practices, clearly there is still a desire to make improvements. In the current vendor landscape, security isn't easy to get right, and we wouldn't want to paint a completely rosy, unrealistic picture.

Cybersecurity fatigue

We define cybersecurity fatigue as virtually giving up on staying ahead of malicious threat actors, and surprisingly, smaller businesses are suffering from precisely the same level of cybersecurity fatigue as larger businesses. Both SMBs and large enterprises come in at 41% of respondents experiencing fatigue, and 58% not. There is clearly a desire and need to be more efficient at managing security.

Employees' adoption of cybersecurity awareness

SMBs and larger organizations that had difficulty getting users to adopt cybersecurity awareness programs showed no significant difference in breach downtime.

Clearly, we know that users have impact – they can be your first line of defense. However, it's not about deeming users 'the weakest link.' Rather, it's about involving your users in your security strategy so that adoption becomes commonplace.

Democratizing security is a topic that Wendy Nather, Head of the CISO Advisory Board at Cisco, presented as an [engaging keynote](#) at the RSA Conference 2020. (You can also hear an interview with Wendy on the [Cisco Security Stories Podcast](#).)



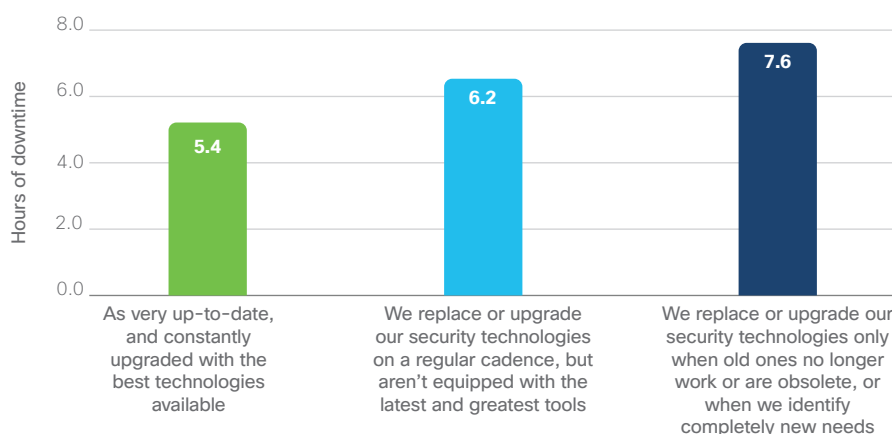
“Rather than pointing the finger at everyone who falls for one of our simulated phishing attacks, we celebrate everyone who reports it. Measure the behavior that you’re trying to encourage.”

Wendy Nather, Head of Advisory CISOs, Cisco

Reducing downtime

Is it true that the older your hardware and software, the less effective it is at defeating new and emerging threats? Our data appears to support this theory for SMBs.

Figure 16. How would you describe your organization's security infrastructure correlated with the number of hours of downtime resulting from last year's most impactful breach? SMB N=481.



Source: Cisco's Big Security in a Small Business World Report, 2020

SMB respondents who said they only replace or upgrade their security technologies when they no longer work experienced 7.6 hours of downtime after their most severe breach last year. For those who told us they have very up-to-date infrastructure, they experienced 5.4 hours.

Does that mean we're encouraging you to throw everything away, and only buy the latest shiny tool? No, not at all. Our experience with cybersecurity has shown that it's more important to focus on integrating what you have that's still working, rather than letting it become obsolete, and supplementing it with newer technologies as needed.

If you're concerned that your infrastructure is out of date, there are some aspects to consider. The most critical one is to ensure it has the flexibility to cope with change. Ideally, it should deliver built-in automation and analytics that aid in policy and device management, detecting unknown threats, and coordinating response and policy change.

Find out if your platform can apply analytics to identify behavioral anomalies across on-prem and cloud network traffic. It should be able to do this while enforcing policies and automatically adapting network and application access for compromised endpoints.

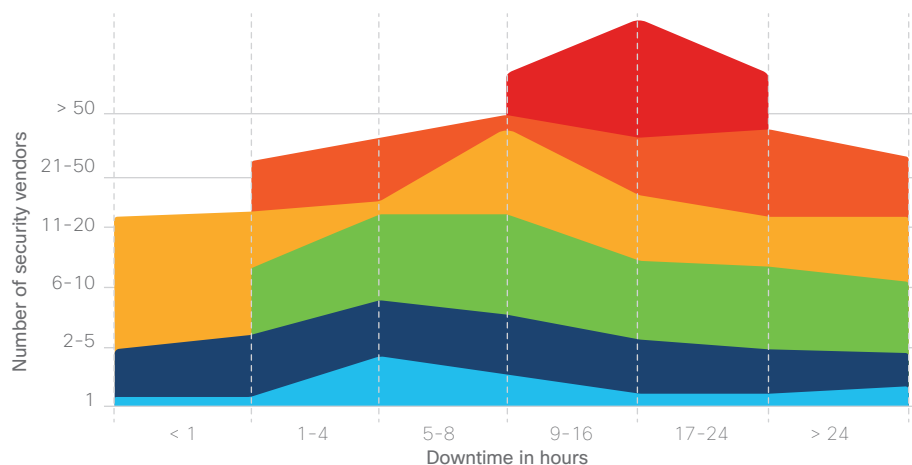
To learn more, read [5 Questions to Ask Your Security Platform Vendor](#).

Vendor complexity

For a lot of organizations, spreading the risk of security might seem to mean increasing your vendors. But what are the consequences of this approach? How challenging is it to manage a multi-vendor environment, and does having more vendors broaden your coverage, resulting in better security by reducing downtime?

Incredibly, the more vendors our SMB survey respondents used, the longer their reported downtime from their most severe breach. This range went from an average of four hours using one vendor, to an average of more than 17 hours using over 50 vendors, which is more than four times higher.

Figure 17. Number of security vendors used within security environment [SMB N=472] and systems downtime due to the most severe security breach managed in the past year [SMB N=388].



Source: Cisco's Big Security in a Small Business World Report, 2020

As is clear in Figure 17, the more vendors you have (bottom to top) the more downtime there is (left to right). Not only can vendor sprawl in a typical SMB security environment cause unnecessary complexity and inefficient workflows, it can also make or break your business in terms of system downtime.

A great tactic to mitigate complexity challenges caused by a multi-vendor environment is to adopt an open, portfolio-based platform that enables your solutions to work together.

Resources to secure your journey forward

To sum it all up, our data shows that SMBs have been taking security seriously in their strategic planning and daily operations. This is great news!

But as our [2020 CISO Benchmark Study](#) also showed, new security challenges are cropping up every day.

And for SMBs, the pressure to keep up and grow the business is magnified. Add to this a growing mobile and remote workforce, and we have a perfect storm.

To help you on this journey, visit our website dedicated to your small or medium-sized business, [Small Business Security Solutions](#). And here are some additional resources to help you use cybersecurity to accelerate your success:

- [The End of the Password... Finally](#)
- [Cloud Security for the Future of Your Business](#)
- [Small Business Product Selector](#)
- [3 Tips for Choosing a Next-Generation Firewall for Small Business](#)
- [Cisco Small Business Security Customer Case Studies](#)

At Cisco, we built our security platform with the idea that security solutions should work as a team, learning from each other, listening to each other, and responding as a coordinated unit. We believe this is a systematic approach that both simplifies security and makes it more effective.

[Cisco SecureX](#) integrates your existing infrastructure for a consistent experience. It unifies visibility, enables automation, and strengthens your security across network, endpoints, cloud, and applications.

Securing your remote workforce

Right now, the abrupt shift towards massively supporting remote workers creates a series of security challenges to keep your organization running in a very different environment than ever before. This is putting a sudden strain on both your security and IT teams who are being tasked with quickly providing support for an unprecedented number of offsite workers and their devices – without compromising security.

For any SMB adapting to a more remote working posture, how do you stay secure? Taking into account this new reality, you need a simple and easy way to secure remote workers at the speed and scale of their business.

Cisco wants to help you enable your employees to work remotely and securely. We recommend the following steps:

- **First, master the basics** as we've discussed in this report – patching vulnerabilities, training employees, implementing zero-trust access with multi-factor authentication (MFA), and securing network, endpoints, cloud, and applications.
- **Second, balance security with usability.** Employees shouldn't have to be mind-readers to know what security specialists know. They have their own jobs to do. Make security accessible so that it's seamless to their jobs.
- **And third, partner with security vendors** that help you simplify your security infrastructure, not complicate it. Our data shows there is a correlation with less downtime from breaches when involving less (and more strategic) vendors.

For useful articles, webinars, and offers to support your organization staying connected securely, visit: [Cisco Secure Remote Worker](#).

About our experts

Cisco Security has a CISO Advisory Board comprised of former CISOs holding a wealth of cybersecurity knowledge with backgrounds in a variety of industries. In addition to providing their insight, guidance, and experience to inform the recommendations we offer in the Cybersecurity Report Series, they also support our sellers, partners, and customers on issues from securing digital transformation to compliance, privacy, monitoring and visibility, zero trust and threat intelligence. If you would like to talk with a member of our CISO Advisory team, please contact asktheciso@external.cisco.com.

About the Cisco Cybersecurity Report Series

Throughout the past decade, Cisco has published a wealth of definitive security and threat intelligence information for security professionals interested in the state of global cybersecurity. These comprehensive reports have provided detailed accounts of threat landscapes and their organizational implications, as well as best practices to defend against the adverse impacts of data breaches.

Cisco Security now publishes a series of research-based, data-driven publications under the banner Cisco Cybersecurity Series. We've expanded the number of titles to include different reports for security professionals with different interests. Calling on the depth and breadth of expertise of threat researchers and innovators in the security industry, the reports in each year's series include the Data Privacy Benchmark Study, the Threat Report, and the CISO Benchmark Study, with others published throughout the year.

For more information, and to access all the reports and archived copies, visit: www.cisco.com/go/securityreports.

Americas Headquarters

Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters

Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters

Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Published May 2020

SMB_05_2020

© 2020 Cisco and/or its affiliates. All rights reserved.

