appriver®
a zix company

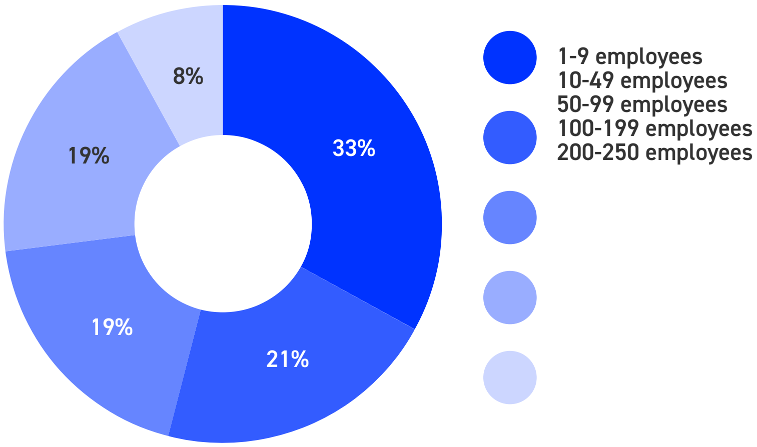
ALL SYNCED

APPRIVER CYBERTHREAT INDEX FOR BUSINESS: Q3 2019

The AppRiver Cyberthreat Index for Business was developed by independent firms Idea Loft and Equation Research, in consultation with the University of West Florida Center for Cybersecurity, using survey data collected online in August 2019.

The survey has a + / – 3% margin of error. The national sample of respondents comprises 1,083 C-level executives and IT professionals in small-to-medium-sized businesses and organizations (SMBs). 72% of these SMBs have compliance requirements.

Company Sizes

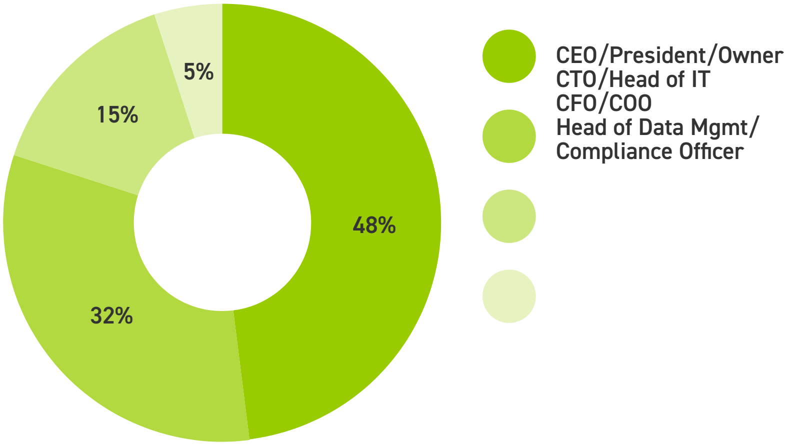


Industries

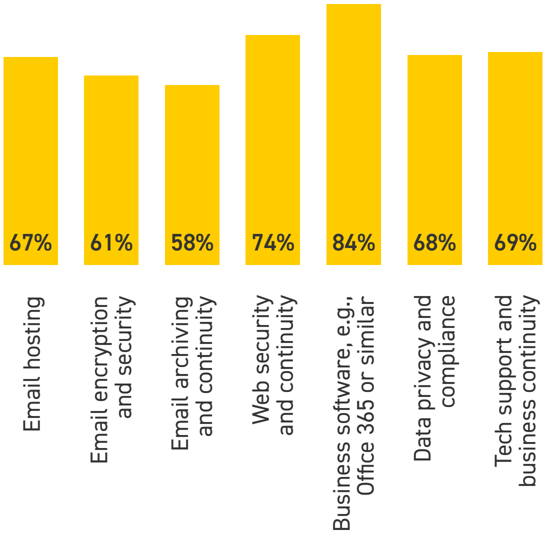
Respondents' industries include:

- Business Services and Consulting
- Construction and Real Estate
- Education
- Financial Services and Insurance
- Government
- Healthcare and Pharmaceutical
- Hospitality, Restaurants and Entertainment
- Legal
- Manufacturing
- Media and Marketing
- Nonprofit
- Retail
- Technology and Telecom
- Transportation and Logistics

Job Titles



Product Relevance



Each respondent needs to be a key purchase decision maker or influencer in at least two of these product categories to participate in the survey.

This proprietary and first-of-its-kind cyberthreat index was developed by measuring small- to medium-sized business decision makers' attitudes and experiences in twelve cybersecurity-related dimensions.

Twelve cybersecurity-related dimensions

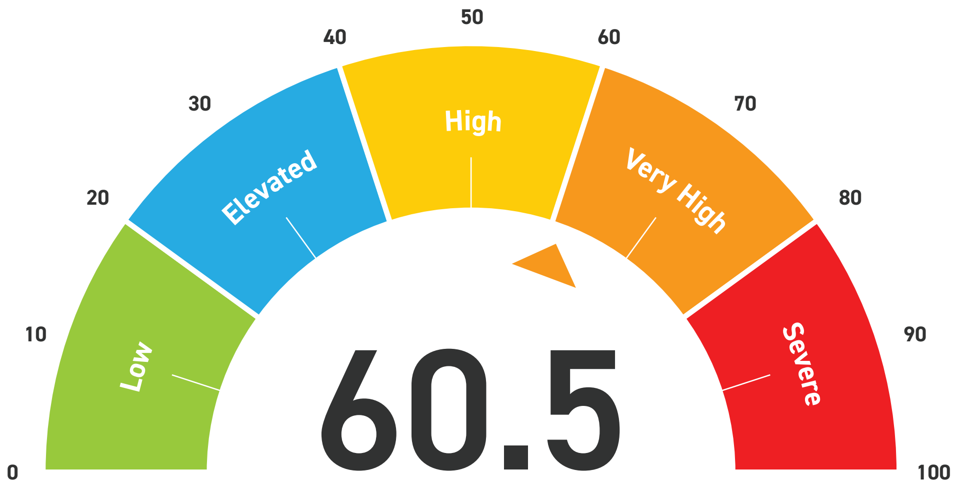
1. Cybersecurity incidents within the past quarter
2. Experience with different kinds of common cyberthreats
3. Estimated prevalence of cybersecurity incidents within the business sector
4. Perceived cybersecurity vulnerability
5. Perceived cybersecurity readiness
6. Perceived cybersecurity confidence
7. Perceived sophistication of cybercriminals
8. Management's prioritization of internal cybersecurity investment and talent
9. Management's prioritization of external cybersecurity partners and resources
10. Effects of cyberbreach and related incidents
11. Estimate of the business's survival rate after a successful future cyberattack
12. Projected needs for future cybersecurity protection

Index Survey Key Findings:

Q3 2019 APPRIVER CYBERTHREAT INDEX FOR BUSINESS

The AppRiver Cyberthreat Index for Business rose from 58.1 in Q2 to 60.5 in Q3.

This is the first time the Cyberthreat Index crossed the 60-point mark since its inception.



Index Level is

VERY HIGH

0 ⟵⟶ **100**

Complete cybersecurity confidence and readiness, with zero threat incidents

Complete absence of cybersecurity confidence and readiness, with constant threat incidents

A busy quarter of reported attacks

- The latest Cyberthreat Index spike was partially driven by increased concerns and Cyberthreat Index scores in the following sectors: Construction and Real Estate, Financial Services and Insurance, Government, Healthcare and Pharmaceutical, Legal, Manufacturing, Transportation and Logistics. Some of these sectors witnessed a busy quarter of cyberattack reports.
- Reports of cyberattack attempts – in particular through phishing – have steadily increased in the Construction and Real Estate sector. Successful phishing that diverts funds into the wrong hands has become more rampant. Professionals and customers in this sector have received caution warnings from financial institutions, real estate brokerage firms and associations, and even through the evening news and other mainstream news outlets. This possibly contributed to an upward trend in Cyberthreat Index level among SMBs in the vertical.
- There have been highly publicized cyberattacks on Government agencies and local municipalities in the past quarter, with victims spanning from the city of Baltimore, MD, the city of Riviera Beach, FL, to the states of Louisiana and Texas.
- High-profile attacks brought to light in the past quarter on the Healthcare and Pharmaceutical sector include the breach of over 20 million patients' records in the possession of Quest Diagnostics and LabCorp.

Growing concerns among SMBs with 50-149 employees

- The Index spike in Q3 was also driven by heightened concerns among mid-tier SMBs. Cyberthreat Index score for this segment grew from 61.5 to 64.5 in the past quarter. This is an interesting segment as they make the transition from start-ups that could run their businesses using cloud-based apps with built-in security. The 50-149 employee range often coincides with a developmental life-stage of an SMB when a dedicated network becomes necessary to handle more users and data. It is possible that some SMBs in this size range perceive a higher risk of exposure to vulnerabilities and attack attempts.

Index Survey Key Findings:

GROWTH IN PERCEIVED ATTACK PREVALENCE AND IMMINENCE

Potential cyberthreats are top-of-mind for SMBs

- 79% of all SMB executives and IT decision makers surveyed in the third quarter report potential cyberthreats are a top-of-mind concern, which represents a 2-point jump from the second quarter. That figure increases to 88% among larger SMBs with 150-250 employees.

Actual attacks are believed to be prevalent

- More SMBs report prevalence of actual attacks in their sector, growing four points since Q2; now 64% of SMBs surveyed say actual attacks are prevalent on a business such as their own.
- After a recent string of attacks, 82% of all SMB respondents in the Government sector say actual attacks are prevalent in their vertical. 73% of respondents in Technology report the same in Q3.

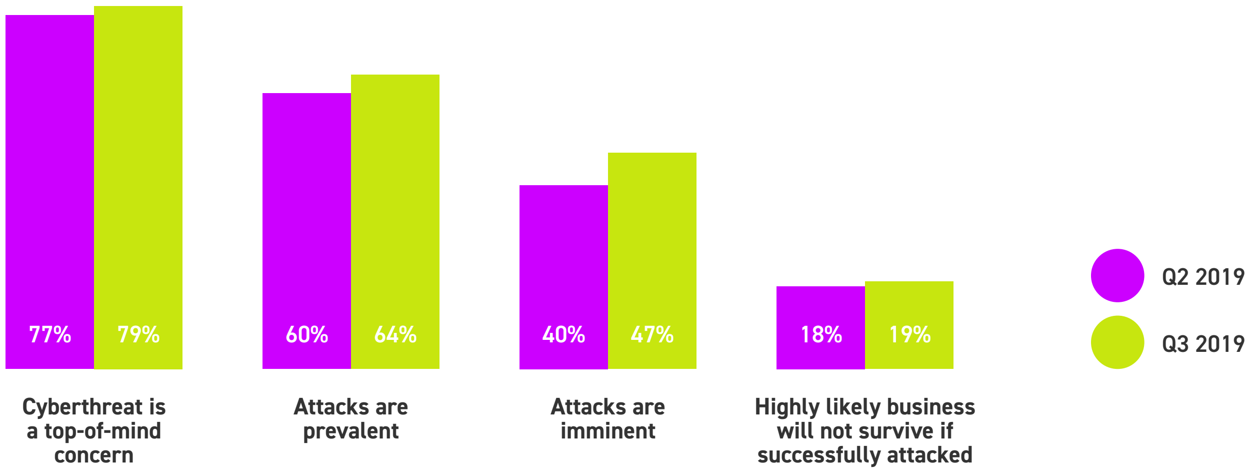
Segment of small-to-medium-sized businesses that fear they are vulnerable to “imminent” cyberattacks jumped seven percentage points in Q3

- In Q3, 47% believe their business is vulnerable to “imminent” cyberattacks, up from 40% who believed the same in Q2. The hike was driven by increases in the 1-49 and 50-149 employee-size segments. However, it is worth noting that while the lowest-size segment of SMBs is catching up with the reality of their vulnerability and cyber risks, there is still a considerable gap (17 points) between their perception of imminent attacks and that of larger-sized SMBs’.
- Education, Finance and Insurance, Government, and the Technology sectors experience the highest level of perceived vulnerability of “imminent” attacks.

Larger SMBs lead concerns over damages

- Overall, 73% of all SMBs believe a successful cyberattack would be harmful to their business, with 19% believing there is a high likelihood their business will not survive a successful attack. Among SMBs with 150-250 employees, those figures jump to 81% and 21% respectively.
- Industries most concerned about not surviving a successful cyberattack include the Education, Media and Technology sectors.

Among all SMBs surveyed



ALL SYNCED

Index Survey Key Findings:

MOST SMBS EXPERIENCED PHISHING IN THE PAST QUARTER

Over 7 in 10 SMBs experienced phishing

- 72% of all SMB respondents report to have experienced at least one phishing attempt at their office within the past quarter. This is an increase from 69% who reported the same in Q2.
- 49% of all respondents in Q3 report they were personally the phishing victim.
- Construction and Real Estate (78%), Government (82%), Media and Marketing (79%), Technology (77%) are among industries reporting the highest rates of experience with phishing in their offices within the past three months.

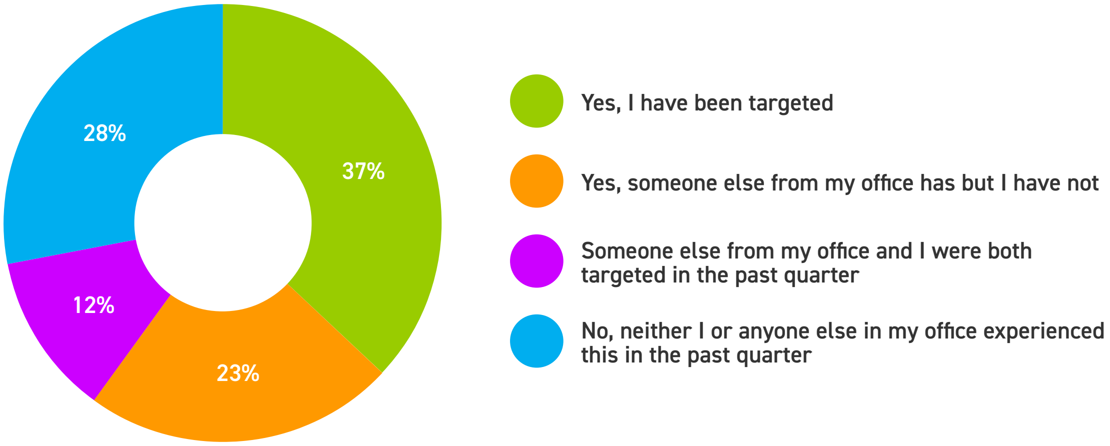
Smaller SMBs could be underestimating phishing attempts

- SMBs with 1-49 reported a lower rate of phishing experience (66%) than respondents in mid-tier SMBs (79%) with 50-149 employees, and top-tier SMBs (79%) with 150-250 employees. As small businesses are routinely targeted by spoofed emails daily, it is possible that some respondents are unaware of phishing attempts that came through their offices.

Over half do not trust employees could detect social engineering

- 54% of all SMB executives and IT decision makers are worried their employees would fall victim to social engineering, a rise from 48% who reported the same in Q2.
- Only 8% say they are "not worried at all" about their employees being fooled by cybercriminals' social engineering attempts. Among SMBs with 150-250 employees, figure for this measure drops to 3%.

In the past quarter, have you or has someone else in your office been targeted in a phishing attempt?



Index Survey Key Findings:

MOST SMBS FEEL IN BETTER SHAPE NOW THAN IN 2018

Despite recording a higher AppRiver Cyberthreat Index score for the third quarter in 2019, most small-to-medium-sized businesses that participated in this survey believe they are in better shape now than in 2018 when it comes to their cyber preparedness. However, for at least some of these businesses, this could prove to be a case of wishful thinking, as a sizeable number of respondents also admit they did not make improvement in their cyber preparedness in the past year, negating sound rationale for feeling "in better shape."

Nearly 6 in 10 made preparedness upgrades, and feel more prepared

- 58% of all SMBs surveyed report to have made improvements in their business's cyber preparedness in the past year, and as a result, believe they are in better shape in fighting off potential cyberattacks. Technology SMBs lead the charge in this category, with 68% reporting they have made improvements in the past year and feel more confident in their cyber preparedness.
- The Hospitality sector is least likely to say they feel to be in better shape, with 47% reporting they have made cybersecurity improvements since 2018 and as a result feel more confident to face potential attacks. This sentiment could be partially driven by a new awareness of cyberthreat risks in this sector, after the revelation of a breach of unprecedented scale affecting Marriott's customers last year.

1 in 10 also made preparedness upgrades, but still feel behind

- It is interesting that 10% of all SMBs surveyed report to have made cyber preparedness upgrades since 2018, however, they believe they still trail cybercriminals who they estimate have done even more to perfect their hacking strategies during the same period.
- The Government sector is most likely to be in this pessimistic segment, with 18% saying they have made improvements while also feeling "in worse shape" in their preparedness compared to in 2018. This could be a reaction to recent strings of attacks targeting government agencies and local municipalities across the country, which had left many in the sector feeling exposed.
- Another sector more likely to feel pessimistic is again the Hospitality sector, with 16% saying they have made improvements since 2018, but still feel to be in worse shape. Hospitality, along with Government, should be receptive prospects for new cybersecurity products and system upgrades. Only 37% of SMB respondents in Hospitality and 36% in Government say they believe they currently invest enough in their cybersecurity.

Nearly 3 in 10 feel to be in better shape, despite lack of preparedness improvement

- 29% report to feel in better shape than they did in 2018 in terms of their business's cyber preparedness, despite not having made improvements to their cybersecurity. Their rationale rests on the assumption that cybercriminals "have done even less" during the same period. This is a segment of the SMB market that could be overly confident, and could be caught off guard as a result of underestimating the real threats they face.
- SMB respondents in the Legal, Retail, and Transportation and Logistics verticals are most likely to fall in this segment.

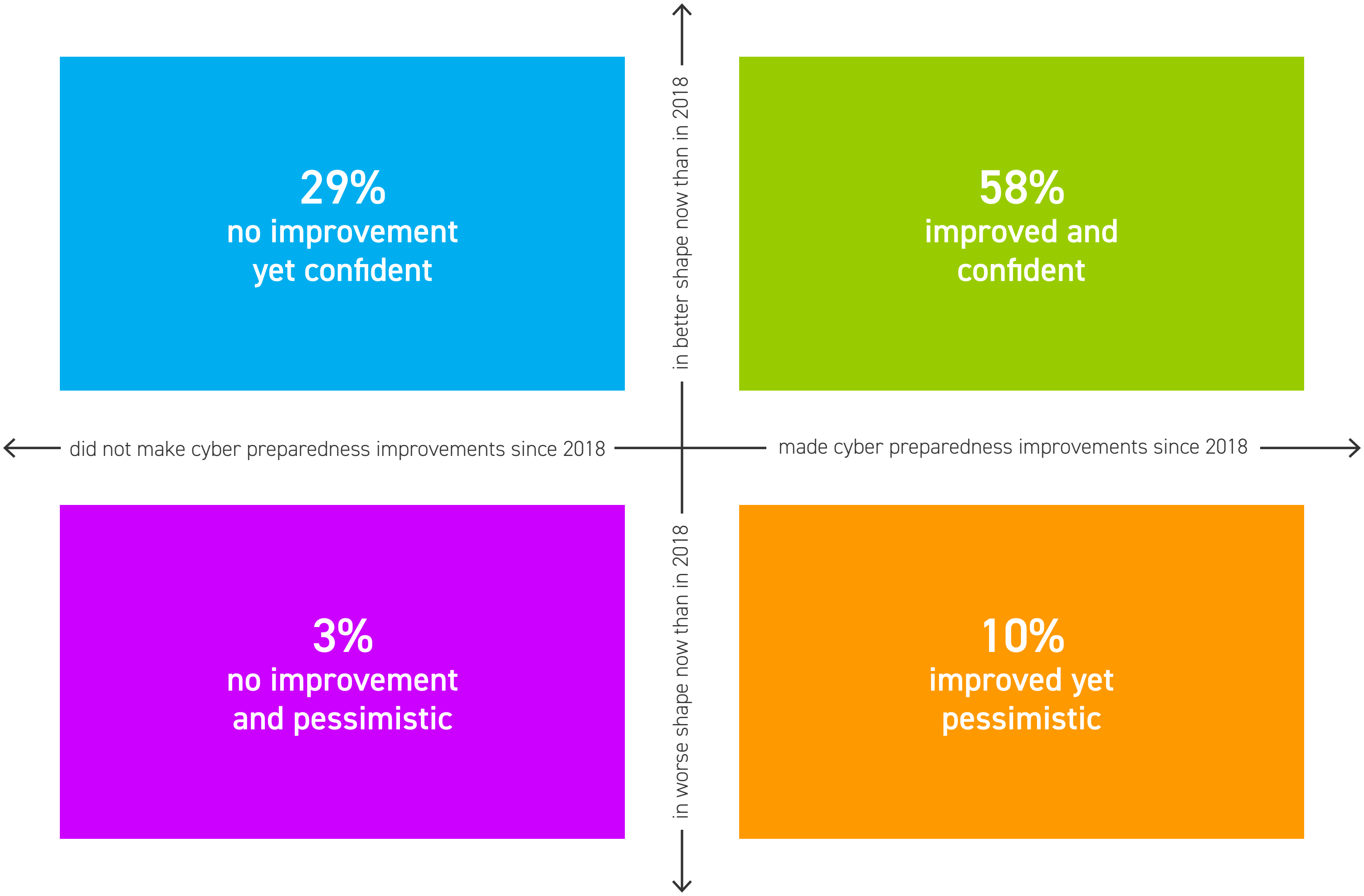
Misconception about small business as a threat target

- One possible explanation for some SMBs' (nearly 3 in 10) optimism in being "in better shape" despite lack of preparedness upgrades may be linked to their misconception that small businesses are unlikely targets of cybercrimes. 41% of all SMBs currently believe their smaller size means criminals will not target them. This is a perception discrepancy in the face of real attack reports that show small businesses of all sizes are routinely targeted daily by cybercriminals.

Index Survey Key Findings:

MOST SMBS FEEL IN BETTER SHAPE NOW THAN IN 2018 (CONTINUED)

Is your business in better or worse shape than it was in 2018 when it comes to cyber preparedness and the ability to fight off cybercriminals’ hacking attempts?



in better shape now than in 2018
in worse shape now than in 2018
did not make cyber preparedness improvements since 2018
made cyber preparedness improvements since 2018

29%
no improvement yet confident

58%
improved and confident

3%
no improvement and pessimistic

10%
improved yet pessimistic

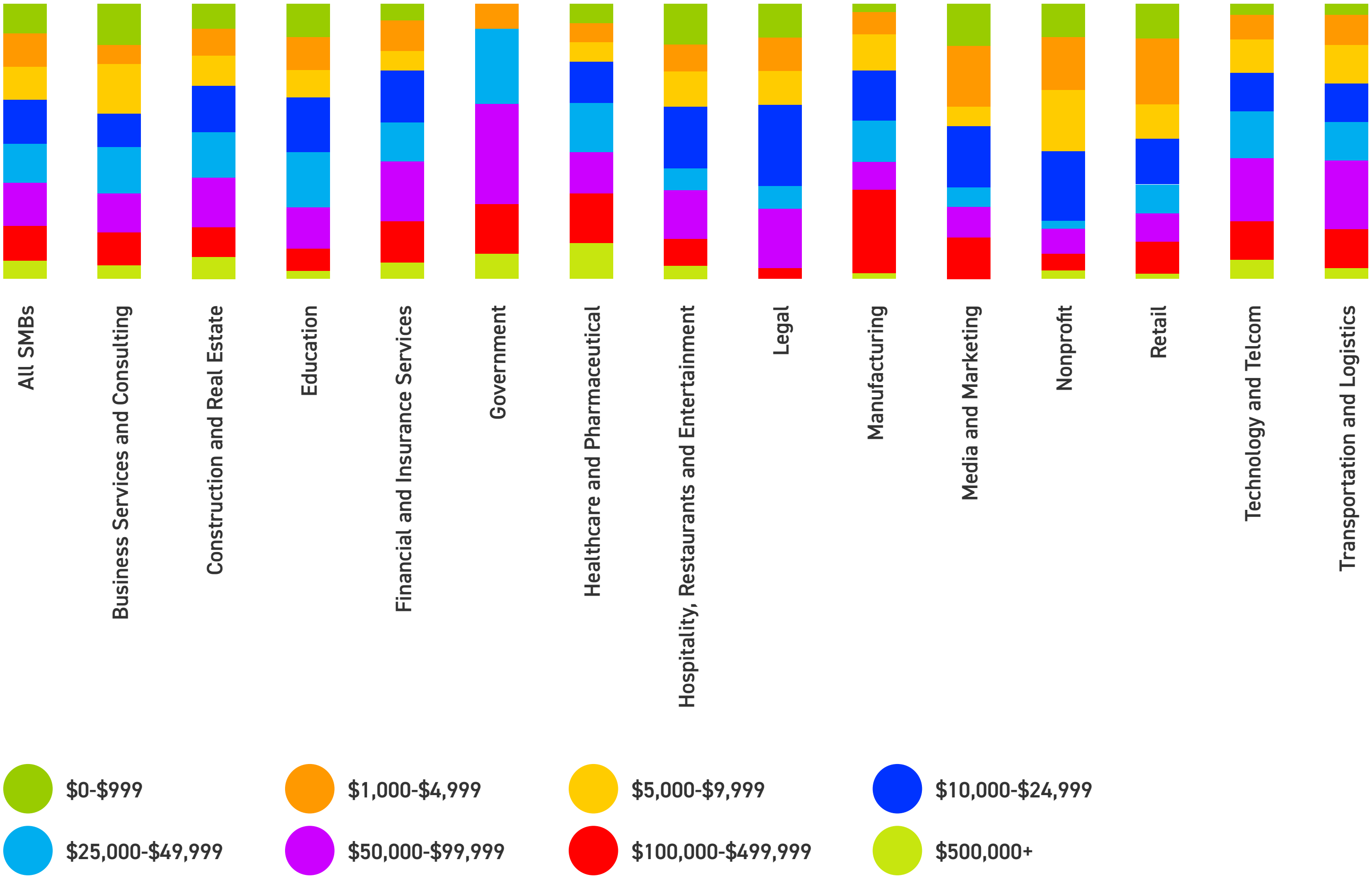
Index Survey Key Findings:

SMBS MAY BE UNDERESTIMATING COSTS OF ATTACKS

Half of all SMBs estimate attack to cost under $25,000

- Among all SMB executives and IT decision makers surveyed, 51% estimate a successful cyberattack and data breach would cost their business under $25,000 of damages. 35% place that estimate even lower to under $10,000.
- It is important to note that survey respondents were reminded to take all potential damages and costs into consideration when tabulating an estimate, to include but not limited to the costs of hacked data retrieval, ransom payment, restoring system to operation, network repairs and upgrades, lost businesses, PR and damage control, potential law suits and compensation to breached customers.
- 19% estimate a successful attack would cost their business $100,000 or more. A report last year put the estimated average cost of breach to an SMB in North America at $149,000.[1]
- Legal (65%), Media and Marketing (66%), Nonprofit (78%), and Retail (65%) are verticals most likely to estimate the cost of a successful cyberattack at under $25,000. Government and Healthcare SMBs are most likely to estimate higher costs of a cyberbreach.

How much do you estimate a successful cyberattack and data breach on your business would cost you?



[1] Kaspersky Lab Report, 2018

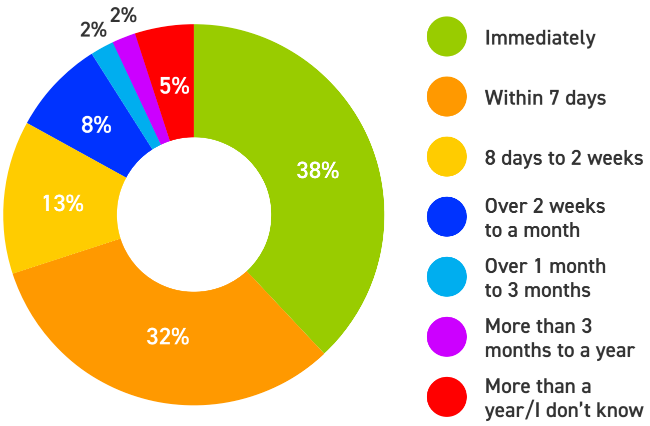
Index Survey Key Findings:

MOST SMBS ARE NOT QUICK TO APPLY PATCHES

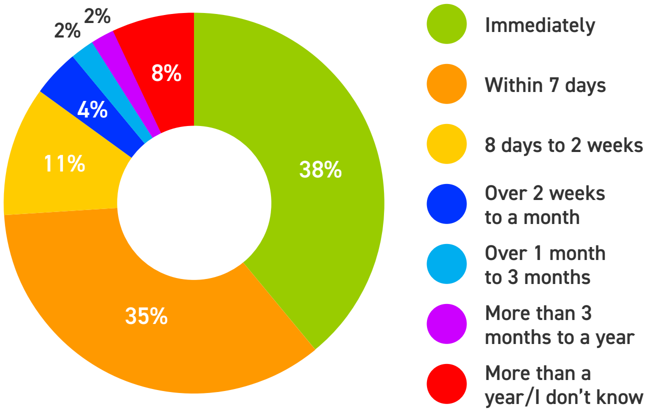
Fewer than 4 in 10 apply security patches immediately

- When asked how long it takes them to apply patches to security vulnerabilities after they are made available, 38% of all SMB respondents report they apply patches immediately.
- This is an indication that there is a disconnect among SMB executives – while 79% report potential cyberthreat is a top-of-mind concern for their business, fewer than half as many are leveraging turnkey and accessible everyday solutions to minimize their risks.
- Among the fourteen key verticals surveyed, none reports more than half of all IT decision makers who apply patches immediately, not even in the Technology sector.
- Another 32% say they typically apply patches within seven days. This leaves 30% of all SMBs surveyed that take over a week to apply patches.
- This is one of the few areas where higher degree of vigilance is not reported among larger-sized SMBs compared to their smaller peers. 67% of SMBs with 150-250 employees say they apply patches within seven days, which leaves 1 in 3 businesses still vulnerable a week after a security patch is made available.

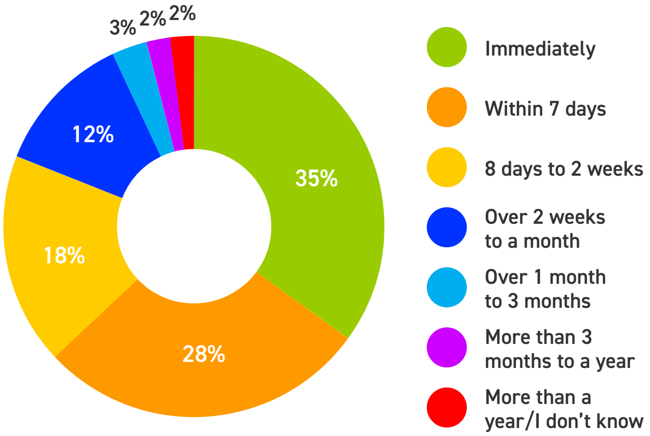
All SMBs



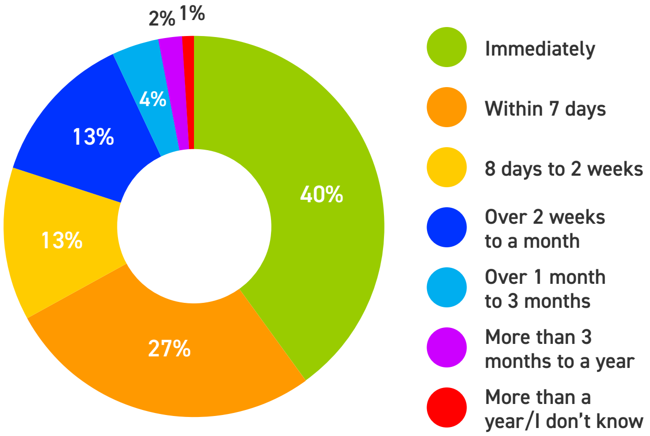
SMBs with 1-49 employees



SMBs with 50-149 employees



SMBs with 150-250 employees



Index Survey Key Findings:

WHAT SMBS WANT IN A SECURITY SERVICE PROVIDER

SMBs value expertise as top criterion when selecting a cybersecurity service provider

- When asked to rank criteria that carry the greatest influence when they select a cybersecurity service provider, 75% assign their top-two rankings to "expertise, including technical know-how and vertical industry expertise."
- Twelve key verticals place "expertise" highest in their criteria ranking when choosing a cybersecurity service provider. These verticals include Construction and Real Estate, Education, Financial Services and Insurance, Government (tied with "cost and affordability"), Healthcare and Pharmaceutical (tied with "24/7 availability and support"), Hospitality, Legal (tied with "24/7 availability and support"), Media and Marketing (tied with "experience"), Nonprofit, Retail, Technology, Transportation and Logistics.
- Among SMBs of all sizes, the collective ranking order of cybersecurity service provider selection criteria are:
    1. Expertise, including technical know-how and vertical industry expertise
    2. 24/7 availability and support
    3. Experience, including tenure in the industry and track record of success
    4. Cost and affordability
    5. Breadth of services, including technical and marketing support
    6. Interpersonal rapport

Perhaps surprisingly, cost is said not to be a most influential factor

- Government is the only one among fourteen key verticals that is most likely to choose "cost and affordability" as a leading factor (tied for first with "expertise").
- Verticals that are mostly likely to name "cost and affordability" as a second-leading factor when selecting a cybersecurity service provider are Education, Hospitality and Retail (tied for second with "experience").
- Among larger SMBs with 50-149 employees and 150-250 employees, "cost and affordability" slips to fifth of six influential factors when selecting a service provider.

24/7 availability and support most valuable to larger SMBs

- 70% of all SMBs with 150-250 employees choose "24/7 availability and support" as its top-two ranked most influential criterion when choosing a service provider, second only to "expertise."
- Round-the-clock support is also most valued by executives who work in Business and Consulting (top ranked), Healthcare and Pharmaceutical (tied for top ranked), Legal (tied for top ranked), Manufacturing (top ranked), and Technology (second ranked).

WHAT SMBS WANT IN A SECURITY SERVICE PROVIDER (CONTINUED)

Which of the following factors carry the greatest influence when it comes to selecting a cybersecurity service provider?

	Total	1-49 employees	50-149 employees	150-249 employees	Business Services and Consulting	Construction and Real Estate	Education	Financial and Insurance Services	Government	Healthcare and Pharmaceutical	Hospitality, Restaurants and Entertainment	Legal	Manufacturing	Media and Marketing	Nonprofit	Retail	Technology and Telcom	Transportation and Logistics
Cost and affordability	4	2	5	5	5	5	2	5	1	3	2	3	4	3	3	2	4	5
24/7 availability and support	2	4	3	2	1	4	4	3	3	1	4	1	1	3	4	4	2	3
Experience, including tenure in the industry and track record of success	2	2	2	3	2	3	3	2	5	3	5	3	3	1	2	2	3	2
Expertise, including technical know-how and vertical industry expertise	1	1	1	1	3	1	1	1	1	1	1	1	2	1	1	1	1	1
Breadth of services, including technical and marketing support	5	5	4	4	4	2	4	4	3	5	3	3	4	3	5	5	5	4
Interpersonal rapport	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6

Index Survey Key Findings:

CONFIDENCE ERODED SINCE Q1; PERCEIVED NEED FOR INVESTMENT ROSE

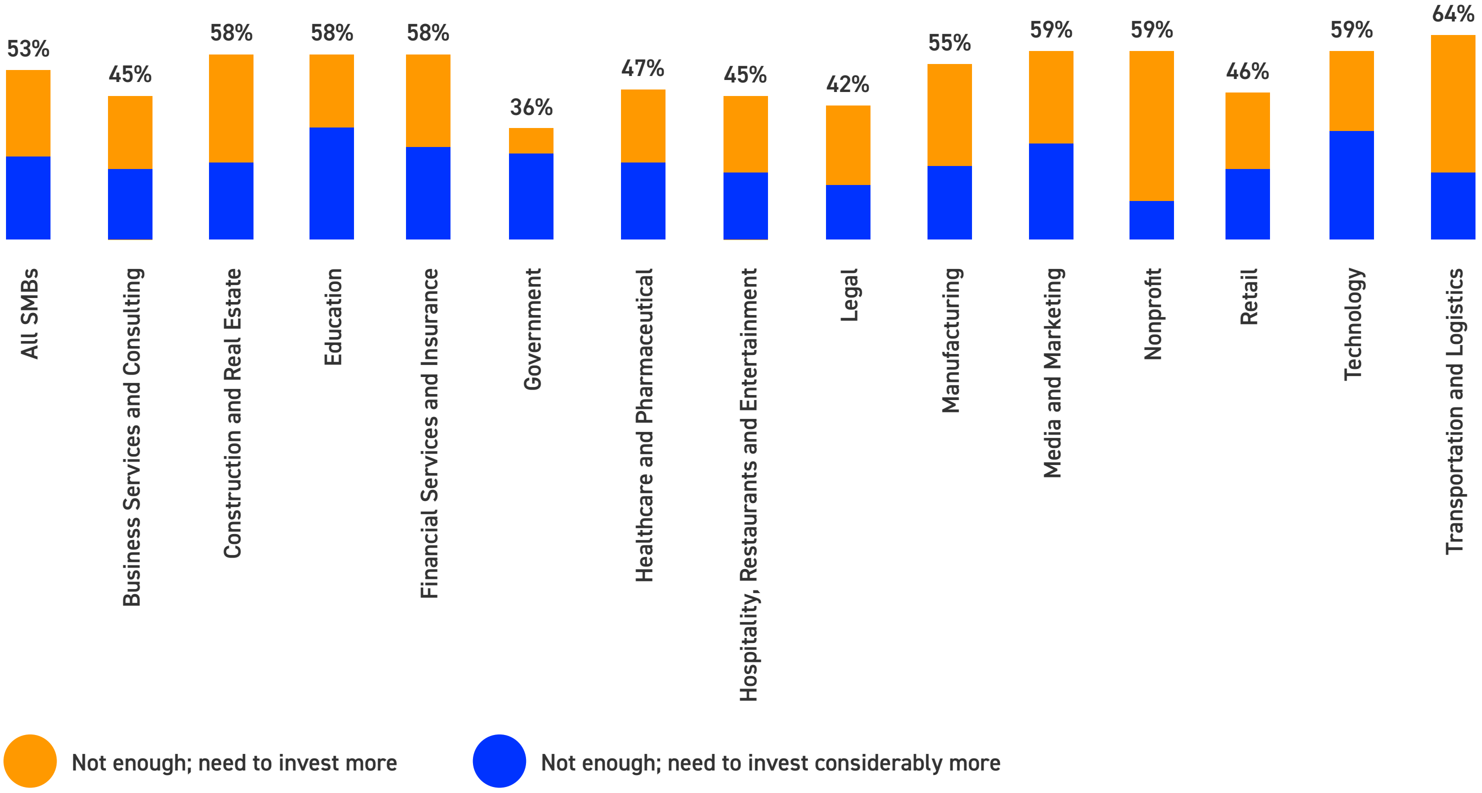
Positive self-rating of cyber preparedness declined from Q2

- While majority of SMBs believe they are now in better shape to defend against cybercriminals than they were in 2018, cybersecurity confidence has receded since the most recent quarter. 41% of all SMBs surveyed in Q3 2019 give themselves a positive rating in cyber preparedness, down six points from 47% in Q2.
- 63% now estimate cybercriminals have more sophisticated attack strategies and technology than their own resources, which is the highest level recorded in three quarters in 2019.

1 in 2 U.S. small-to-medium-sized businesses now see a need to invest more in cybersecurity

- Consistent with the trend of lower confidence and higher Cyberthreat Index score, 53% of all SMB respondents now report they need to invest more to defend against cybercrimes, up from 49% who said the same in Q2.
- 1 in 4 SMB executives and IT decision makers (26%) now believe they need to invest considerably more. Sectors most likely to believe they need to invest considerably more include Education, Financial Services and Insurance, Government, Media and Marketing, and Technology.
- Only 36% of all SMB respondents believe in Q3 their business currently invests enough in its cybersecurity.
- 78% now say their cybersecurity resources and external partners are "vital" to the success of their business, holding steady from 77% in Q2 that said the same.

Do you believe your business invests enough in its cybersecurity, relative to the level of threat your business faces?



Closing Comment:

SLOWLY WAKING UP TO GLOBAL TRENDS IN CYBERTHREATS

Small businesses are catching up with reality, albeit slowly

- The AppRiver Cyberthreat Index for Business crossed the 60-point mark for the first time since the Index's inception, registering at 60.5 in the third quarter, an uptick of 2.4 points since the second quarter of 2019. This indicates small-to-medium-sized businesses in the U.S. have collectively demonstrated a slight increase in cyberthreat vigilance, reports of higher attack incidents and a slight decline in cyber preparedness confidence compared to three months ago.
- This slight uptick should not be a surprise, after a quarter of news coverages on attacks inflicted on larger, presumably iron-clad organizations such as Equifax and LabCorp that affected over 150 million victims in the U.S., as well as increasingly frequent cyberattacks on U.S. local government agencies and municipalities. The attacks on the latter and subsequent reports of ransom payments could be particularly unnerving to small businesses, knowing that even government agencies had to surrender to cybercriminals' demands.
- That said, small businesses still have a way to go to close the gap between their current cybersecurity attitudes and the realistic cyberthreats they are exposed to. Small businesses, specifically at the 1-49 employee-size segment, continue to grossly underestimate their cyber vulnerability, cybercriminals' technological sophistication, and their estimated damage costs in the event of a successful attack. Currently, executives in the lowest end of the SMB size spectrum (1-49 employees) lag their counterparts at the higher-end size spectrum (150-250 employees) by nearly 20 percentage points when asked to estimate the prevalence of cybercrimes. Executives at the lower-end spectrum also may have underestimated cost of a successful attack by over 90%. Put bluntly, many SMBs could be overestimating their own invincibility and longevity in this new cyber business landscape, and could very well be caught off guard.

All Synced Solutions
T. 770.800.2746 x100
ben@all-synced.com
www.all-synced.com