appriver®
a zix company

ZIX | APPRIVER CYBERTHREAT INDEX FOR BUSINESS

Q4 2019

Table of Contents

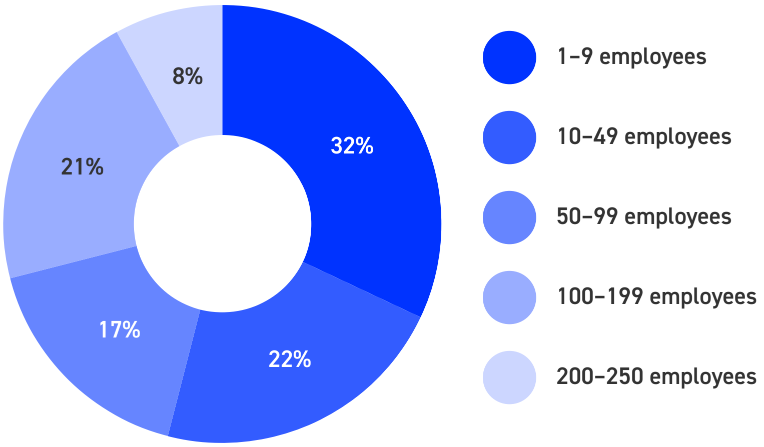
Index Survey Key Findings:

METHODOLOGY

The Zix | 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 October 2019.

The survey has a + / – 3% margin of error. The national sample of respondents comprises 1,049 C-level executives and IT decision makers in small-to-medium-sized businesses and organizations with 1–250 employees (SMBs). 74% of these SMBs have compliance requirements.

Company Sizes

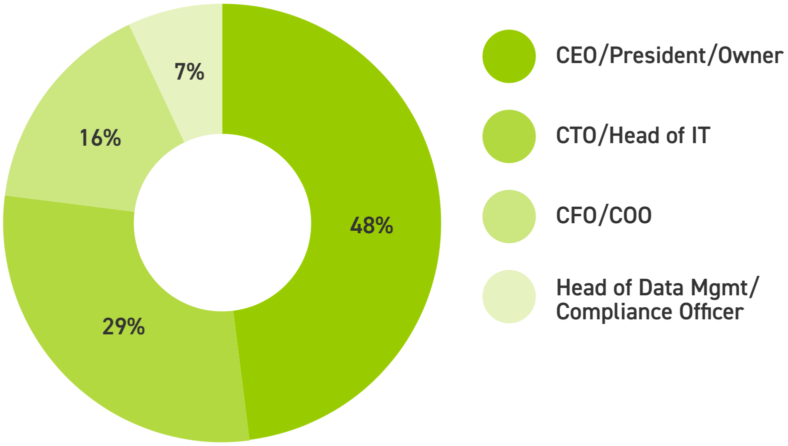


Industries

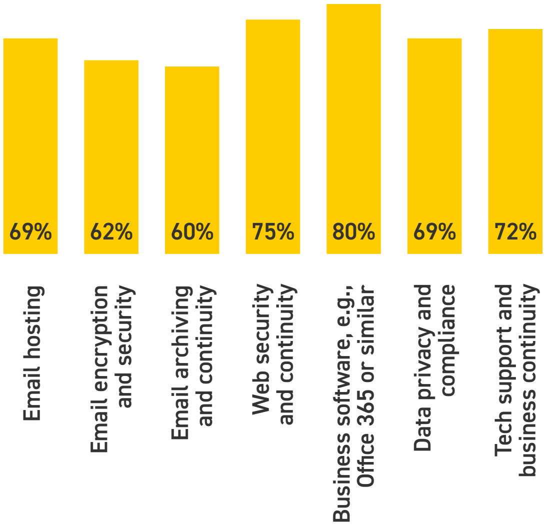
Respondents' industries include:

- Business Services and Consulting
- Construction and Real Estate
- Education
- Financial Services and Insurance
- Government
- Healthcare and Pharmaceutical
- Hospitality, Restaurants and Travel
- 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.

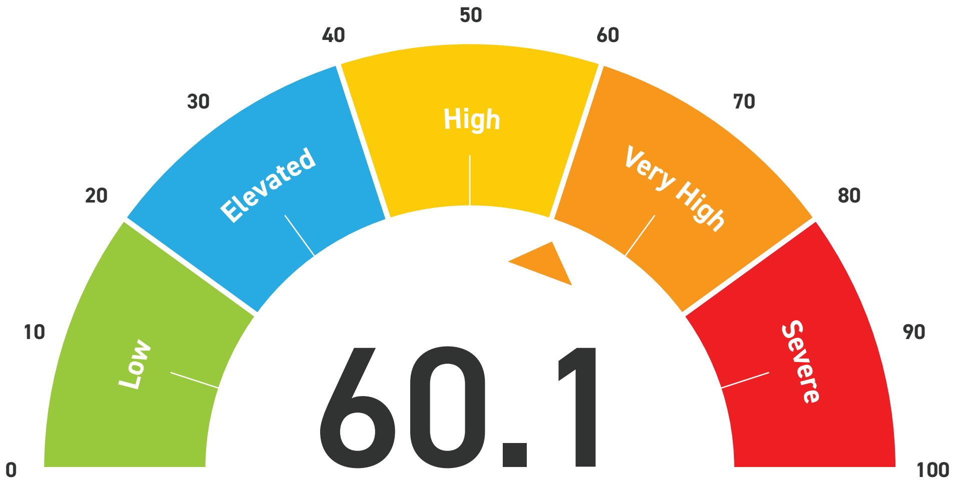
This proprietary and first-of-its-kind cyberthreat index was developed by measuring small- to medium-sized business decision makers' attitudes and experiences in twelve cybersecurity-related dimensions.

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

The Zix | AppRiver Cyberthreat Index for Business declined slightly from 60.5 in Q3 to 60.1 in Q4.

The Cyberthreat Index held steady at the 60-point mark, slightly elevated from Q1 and Q2, as SMBs in America close out the year 2019.



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

Larger SMBs report Increased concerns and threat incidents in Q4

- While the overall Zix | AppRiver Cyberthreat Index for Business remains steady near the 60-point level, the overall number only tells half the story. The minimal index movement was driven primarily by the decreased level of perceived vulnerability and concerns among smaller SMBs with under 50 employees, which account for half of all businesses in the U.S.
- Diverging from slight downward trend in the smallest-sized SMB segment, the Cyberthreat Index was flat in Q4 for businesses with the 50–149 employees and shifted upward among businesses with150-250 employees. Among the largest SMBs, the Cyberthreat Index registered at 68.6 in Q4. This is the highest level recorded since the inception of the Cyberthreat Index, edging closer to the 70-point mark, up from 64.8 in Q3.
- In Q4, 89% of all executives surveyed in businesses with 50-149 employees and 93% of those with 150–250 employees reported cyberthreats are top-of-mind concerns for their business, the highest level registered for both segments since the survey inception.
- Another area with a clear uptick for the two larger-sized SMB segments is the prevalence of cyberthreat incidents in their industry. Two-thirds (76%) of executives in SMBs with 50–149 employees and 8 in 10 (80%) among those with 150–250 employees now say cyberthreat incidents are prevalent in their industry among businesses such as their own. Both are highest levels recorded in 2019.

Index Survey Key Findings:

PERCEPTIONS OF CYBERTHREATS

Potential cyberthreats are top-of-mind for SMBs

- 79% of all SMB executives and IT decision makers surveyed in the fourth quarter report potential cyberthreats are a top-of-mind concern, which represents a 2-point jump from six months prior and remains unchanged from Q3.
- However, that figure increases to 93% among largest SMBs with 150–250 employees, up from 88% in Q3. Medium-sized SMBs with 50-149 employees also report an increase in this measure to 89% in Q4 from 86% in Q3.
- Verticals which report notable increases in this top-of-mind concern measure in Q4 include Government (+6 points to 88%), Manufacturing (+11 points to 89%), Retail (+5 points to 82%), and Transportation and Logistics (+8 points to 83%). These sector-wide growths in concern level coincide with seasonal rises in threat incidents in local municipalities and schools, and anticipated increase in shopping and travel activities during the holiday seasons.

Actual attacks are believed to be prevalent

- Among all SMB executives surveyed, report of prevalence of attack continues its growth trajectory that started in Q2; now 66% of SMBs surveyed say actual attacks are prevalent on a business such as their own, up from 64% in Q3 and 60% in Q2.
- More considerable level of increase in this measure is seen among largest SMBs with 150–250 employees, among which 80% of all executives now say actual attack incidents are prevalent on a business such as their own, up from 74% who said the same in Q3. A smaller level of uptick is also recorded among SMBs with 50-149 employees, which report a rise to 76% in Q4 from 73% in Q3 for this measure.

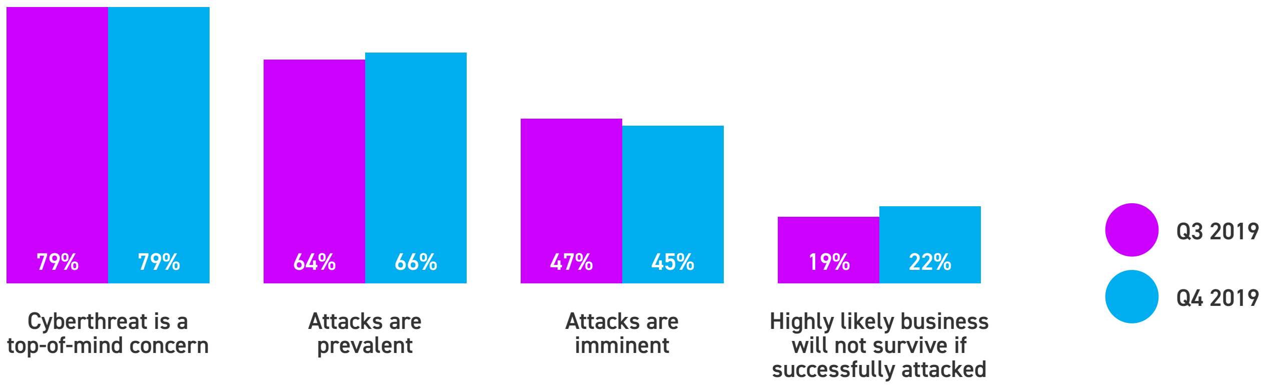
Segment of largest SMBs that fear they are vulnerable to "imminent" cyberattacks jumped ten percentage points in Q4

- In Q4, 63% of executives at SMBs with 150–250 employees believe their business is vulnerable to "imminent" cyberattacks, up from 53% who believed the same in Q3.
- Overall, 45% of SMBs of all sizes believe they are vulnerable to imminent attacks.

More SMBs now concerned about attack damages

- Overall, 72% of all SMBs believe a successful cyberattack would be harmful to their business, with 22% believing there is a high likelihood their business would not survive an attack. The latter is a 3-point jump from 19% in Q3. Among SMBs with 150-250 employees, 1 in 3 (32%) now estimate they have a high likelihood of not surviving a successful cyberattack, up from 21% in Q3.
- Industries most concerned about not surviving a successful cyberattack include Education, Financial Services and Insurance, and Technology and Telecom.

Among all SMBs surveyed



Index Survey Key Findings:

HOLIDAY SHOPPING AT THE WORKPLACE

Majority of SMBs estimate employees are holiday shopping with a business-use device

- 82% of all SMB executives and IT decision makers surveyed estimate "many" of their employees will shop online this holiday season using a work computer or a business-use device, on which business and customer data are also stored and transmitted.
- Holiday shopping online using a business device appears to be highly prevalent. Education, Financial Services and Insurance, Government, Manufacturing, Media, Nonprofit, Technology and Telecom, and Transportation and Logistics are among key industries in which over 85% of all executives surveyed estimate "many" employees would be using a business device to shop online this holiday season.
- The propensity for executives to believe many of their employees will shop online at work or using a business-use device is even higher among those at larger-sized SMBs. 88% of executives at medium-sized SMBs with 50–149 employees and 90% of executives at largest-sized SMBs with 150–250 employees believe many of their employees will be doing so this holiday season.

SMBs know the practice is a security risk, but most have no plan to stop it

- Among the majority of IT decision makers who know employees would be holiday shopping using a business-use device, 61% admit they know this increases cybersecurity risks for their business and customers, but they believe it is a fact of life, and there is not much they can or plan to do about it.
- 64% of executives at medium-sized SMBs (50–149 employees) and 68% at large-sized SMBs (150–250 employees) say there is nothing they could do to stop the practice they know to be risky.

3 in 10 are not aware the practice is in fact risky

- Perhaps equally troubling as executives who know it is risky but plan to do nothing, 32% of all IT decision makers surveyed were not previously aware shopping with a business-use device could expose their organization to higher cyberthreat risks.
- Nearly half (48%) of all IT decision makers at nonprofit organizations admit they did into know the practice could increase their security risks.

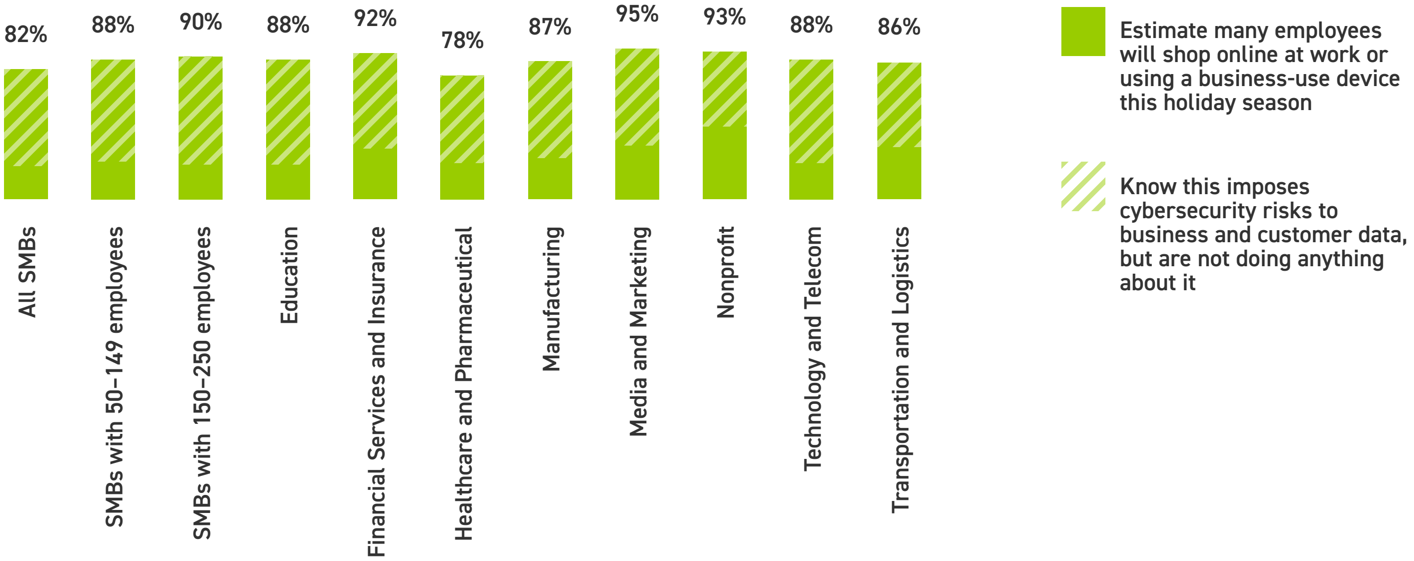
Half do not trust employees could detect a fake retailer link

- Compounding the risks of shopping online using a business device, nearly half (49%) of all surveyed estimate most of their employees would not be able to spot an illegitimate link posing as an online retailer in potential phishing attempts.
- Among these executives and IT decision makers, 4 in 10 lack confidence that they themselves could consistently distinguish an illegitimate link from a real one.
- In several highly regulated industries where employees have access to sensitive data — including Financial Services and Insurance (52%) and Healthcare (63%) — over half are pessimistic and believe most of their employees would not be able to distinguish a fake retailer's link in a phishing attempt from a legitimate one. 92% in Financial Services and Insurance and 78% in Healthcare believe many of their employees will be holiday shopping using a business-use device.

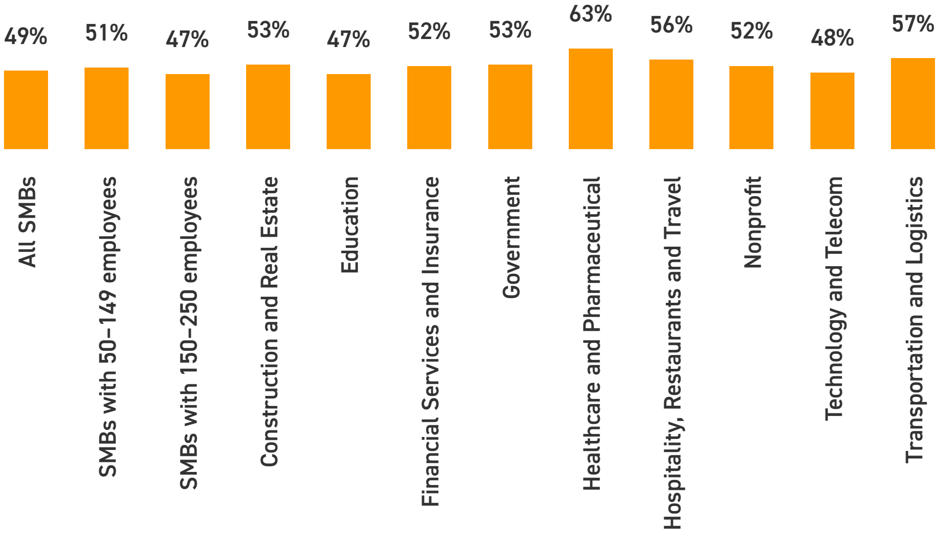
Index Survey Key Findings:

HOLIDAY SHOPPING AT THE WORKPLACE (CONTINUED)

Many employees are expected to shop online using a business-use device this holiday season. 6 in 10 employers are aware this imposes cybersecurity risks, but are not doing anything about it.



Nearly half of all SMBs surveyed lack confidence that most employees can tell the difference between an illegitimate link from a cybercriminal posing as a fake online retailer and a legitimate one.



32%

of all SMBs are not aware that online shopping with a business-use device could be a cybersecurity risk.

Index Survey Key Findings:

A.I. ADOPTION AND CYBERSECURITY

Nearly 9 in 10 interested in A.I. adoption

- Artificial Intelligence (A.I.) appears to be a compelling and relevant business tool for SMB executives in the Zix | AppRiver survey, with 88% of the national sample with diverse vertical representation reporting interest in A.I. adoption for their business.
- Among executives in larger-sized SMBs (150-250 employees), 99% report they are interested in the adoption of A.I.
- Industry sectors that expressed most wide-spread interest in A.I. adoption in the survey include Technology and Telecom (98%), Financial Services and Insurance (95%), Government (94%), Manufacturing (94%), Education (91%), and Transportation and Logistics (91%). The vertical least interested in A.I. adoption is Nonprofit.

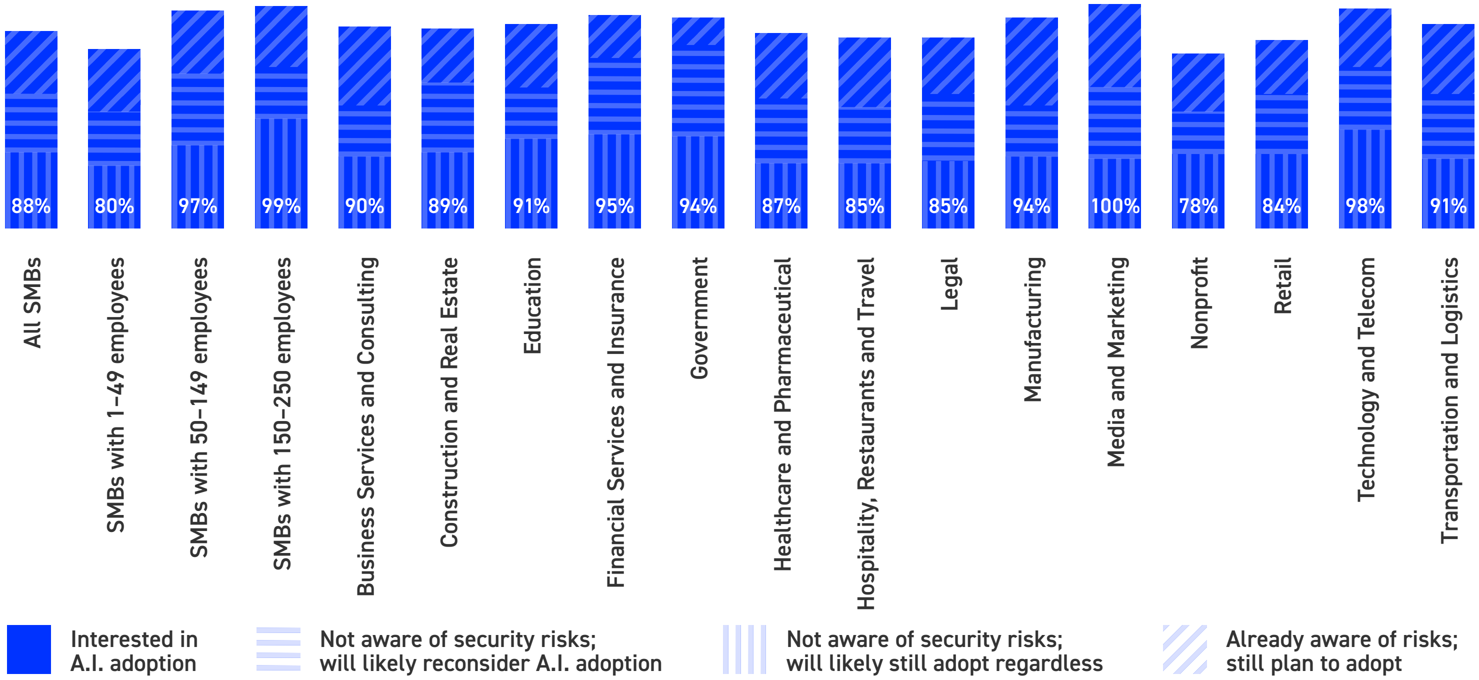
Nearly 7 in 10 unaware of security risks associated with A.I.

- Among SMBs of all sizes that are interested in the adoption of A.I., nearly 4 in 10 (38%) are not aware of potential cybersecurity risks that could accompany its use, and would reconsider its adoption after learning more of such risks.
- Another 30% are not currently aware of cybersecurity risks that A.I. could bring, but say they will likely still move forward with its adoption after learning about the risks.
- In other words, 68% of all who are interested in A.I. adoption are unaware of its potential security risks, making education on A.I. crucial to many SMB executives.

Majority of SMBs would adopt A.I. in spite of risks

- 32% say they already are aware A.I. carries potential cybersecurity risks, but will move forward with adoption as they believe the potential benefits and opportunities A.I. could bring to their business outweigh its risks.
- Including those who are currently unaware of A.I. security risk potentials but are eager for its adoption regardless, 62% of all who are interested will continue to consider A.I. adoption in spite of its potential risks.
- In each of fourteen key verticals represented in the survey, IT decision makers who plan to pursue A.I. adoption in spite of its security risks outnumber those who would reconsider because of the risks.

SMBs' outlook on A.I. adoption and security risks



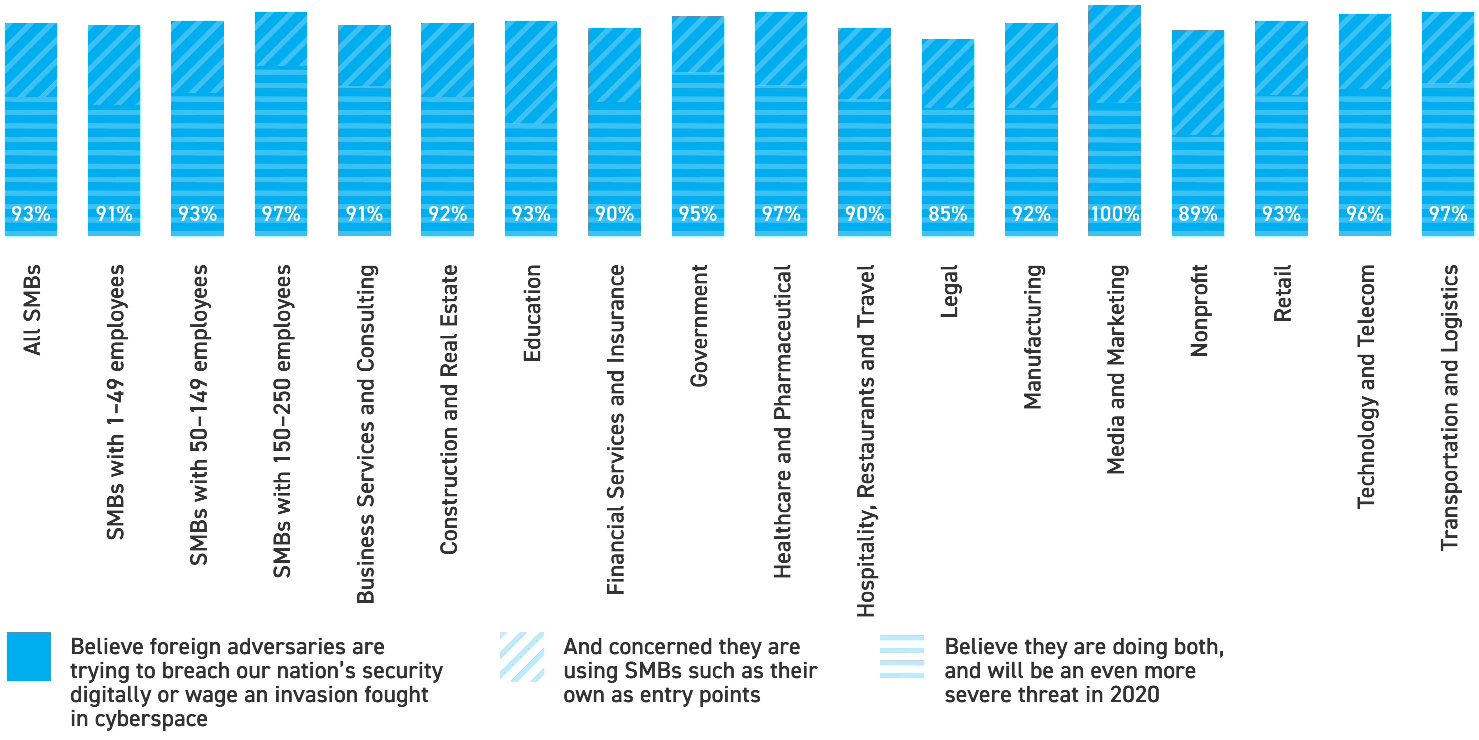
Index Survey Key Findings:

FOREIGN NATION STATES AS CYBERTHREATS

9 in 10 SMBs think foreign nation states are legitimate concerns

- 93% of all SMB executives surveyed believe foreign adversaries are attempting to breach our nation's security digitally or wage an invasion fought in cyberspace using businesses such as theirs as entry points.
- The already-high figure jumps to 97% among larger SMBs with 150–250 employees who believe the same.
- Among the overwhelming majority of SMB executives who believe their business would be a point of vulnerability through which foreign adversaries could wage a cyber invasion, two-thirds (66%) believe this will be more of a concern in 2020 than it already is. Among executives of larger SMBs, three quarters (76%) believe the same, that this cyber defense threat will be more severe in 2020.
- Government, Healthcare and Pharmaceutical, Technology and Telecom, and Transportation and Logistics SMBs are among the verticals most likely to be concerned about increased foreign nation-state attacks in cyberspace through a business such as theirs in 2020.

Believe foreign adversaries are trying to breach our nation's security digitally or wage an invasion fought in cyberspace



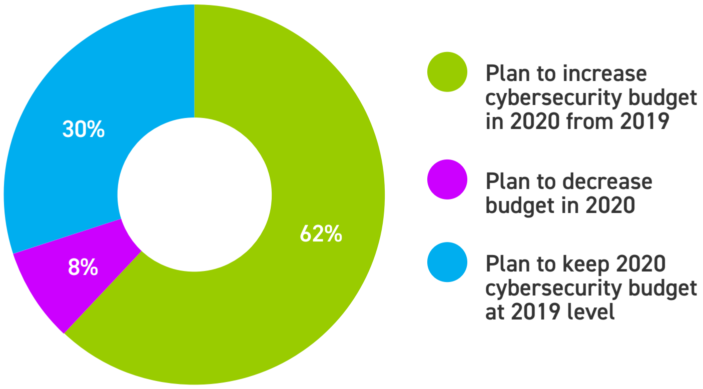
Index Survey Key Findings:

CYBERSECURITY BUDGETS IN 2020

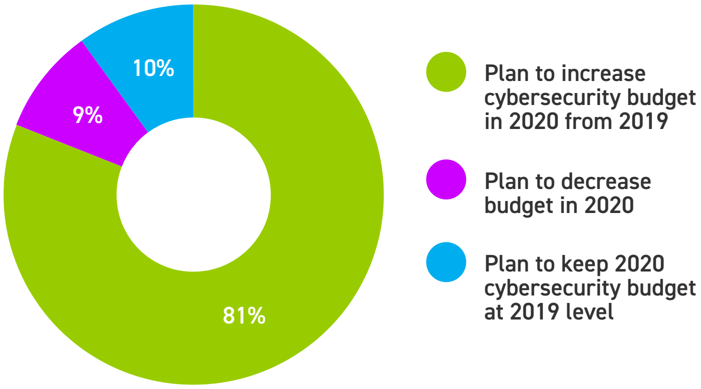
6 in 10 SMBs plan to increase cybersecurity budget in 2020

- Looking ahead to 2020, 62% of SMB IT decision makers plan to increase their cybersecurity budget in 2020, 8% plan to reduce, 30% plan to maintain their budget at the 2019 level.
- The propensity to plan to shore up cybersecurity investment climbs as SMBs increase in size. Among SMBs with 49–149 employees, 75% plan to increase their budget in 2020, 8% plan to reduce, 17% plan to maintain their 2019 budget.
- Among SMBs with 150-250 employees, 81% plan to increase their budget in 2020, 9% plan to reduce, 10% plan to maintain their 2019 budget.
- Sectors with highest propensity to plan to increase cybersecurity budget in 2020 include Technology and Telecom (77%), Government (76%; not a surprise given heightened attack incidents in 2019), Manufacturing (73%) and Financial Services and Insurance (71%).
- Sectors most likely to plan to decrease their 2020 cybersecurity budget from 2019 level are Nonprofit (48%) and Hospitality (47%).

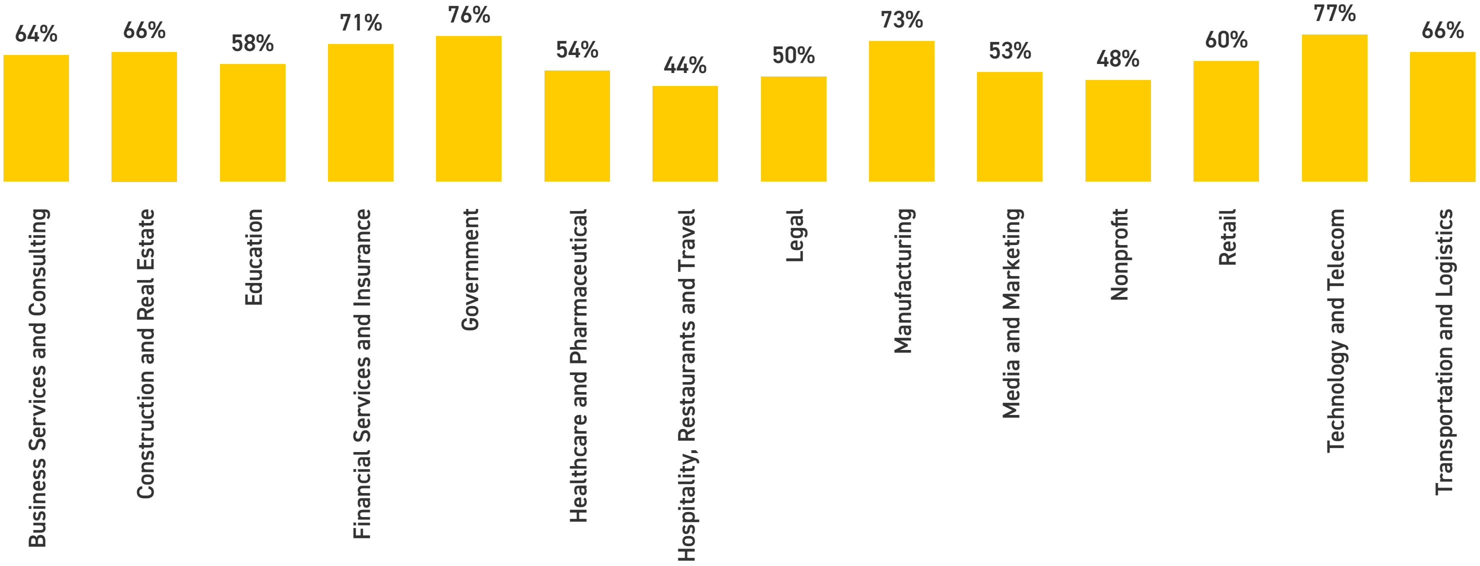
All SMBs



SMBs with 150–250 employees



Plan to increase cybersecurity budget in 2020 from 2019 level



Index Survey Key Findings:

CYBERSECURITY PRIORITIES IN 2020

Alongside plans to boost their cybersecurity budget, SMBs surveyed also have distinct cybersecurity strategies and areas in which they aim to invest.

Technology improvement and training top security priorities in 2020

- Nearly 6 out of 10 (58%) SMBs plan to add more cybersecurity technology, making it the top area in which SMBs plan to invest for cybersecurity improvement in 2020.
- A close second is in the area of training. 57% of all SMB executives and IT decision makers surveyed report they plan to invest in improving their cybersecurity by creating better security awareness training for employees.
- 50% report they plan to invest in conducting more regular reviews of security defenses, followed by 35% that plan to add more in-house security talent in 2020. 30% plan to invest more on outsourcing more security tasks, or on their partnership with a managed service provider.
- 10% of all surveyed report they do not plan to make security improvement in 2020; and add that their cybersecurity strategy in 2020 will remain the same as in 2019.

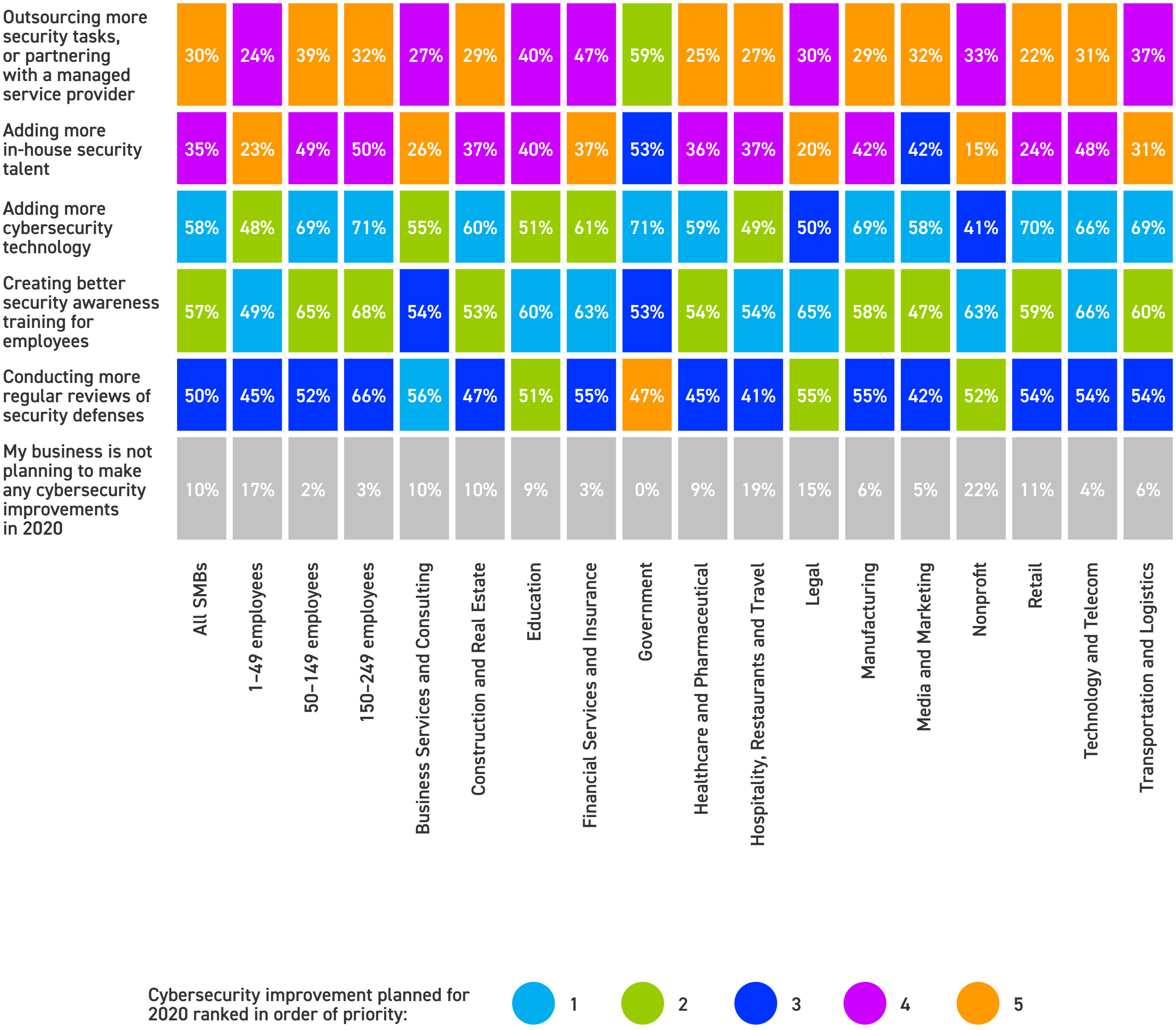
Large SMBs planning robust improvement

- SMBs with 150–250 employees appear to have the most ambitious plans for security upgrades in 2020. About 7 out of 10 plan to invest in adding and upgrading cybersecurity technology in 2020 (71%), and creating better security awareness training for employees (68%). 2 out of 3 (66%) plan to invest in conducting more regular reviews of their security defenses.

Index Survey Key Findings:

CYBERSECURITY PRIORITIES IN 2020 (CONTINUED)

SMBs’ cybersecurity improvement priorities planned for 2020



	All SMBs	1–49 employees	50–149 employees	150–249 employees	Business Services and Consulting	Construction and Real Estate	Education	Financial Services and Insurance	Government	Healthcare and Pharmaceutical	Hospitality, Restaurants and Travel	Legal	Manufacturing	Media and Marketing	Nonprofit	Retail	Technology and Telecom	Transportation and Logistics
Outsourcing more security tasks, or partnering with a managed service provider	30%	24%	39%	32%	27%	29%	40%	47%	59%	25%	27%	30%	29%	32%	33%	22%	31%	37%
Adding more in-house security talent	35%	23%	49%	50%	26%	37%	40%	37%	53%	36%	37%	20%	42%	42%	15%	24%	48%	31%
Adding more cybersecurity technology	58%	48%	69%	71%	55%	60%	51%	61%	71%	59%	49%	50%	69%	58%	41%	70%	66%	69%
Creating better security awareness training for employees	57%	49%	65%	68%	54%	53%	60%	63%	53%	54%	54%	65%	58%	47%	63%	59%	66%	60%
Conducting more regular reviews of security defenses	50%	45%	52%	66%	56%	47%	51%	55%	47%	45%	41%	55%	55%	42%	52%	54%	54%	54%
My business is not planning to make any cybersecurity improvements in 2020	10%	17%	2%	3%	10%	10%	9%	3%	0%	9%	19%	15%	6%	5%	22%	11%	4%	6%

FINAL COMMENTS

As we approach the final weeks of 2019, the latest quarterly results from the Zix | AppRiver Cyberthreat Index for Business Survey show once again cybersecurity threats felt by our nation's small-to-medium-sized businesses are not easing up. Borrowing a sentiment from our survey respondents who admit employees' risky holiday shopping on business-use devices is a "fact of life," it appears so too is the perpetual state of vulnerability among SMB executives and IT decision makers, many of whom (61% nationally) think they are outmatched by hackers in cyberattack technology and strategies.

It is interesting we continue to witness a significant gap between the smallest businesses (1–49 employees) and their larger peers (150–250 employees) in their cybersecurity confidence. Presumably with higher level of cybersecurity resources and investment, larger SMBs consistently report:

- higher levels of vulnerability — 63% of larger SMBs feel vulnerable to imminent attacks vs. 33% of smaller SMBs that feel the same;
- stronger perceived inferiority compared to cybercriminals — 70% of larger SMBs feel outmatched by cybercriminals vs. 57% of smaller SMBs that feel the same;
- higher estimated incidents of attacks — 80% of larger SMBs feel cyberattacks are prevalent vs. 56% of smaller SMBs that feel the same;
- higher estimates of potential attack loss — 63% of larger SMBs estimate high level of post-attack damages vs. 49% of smaller SMBs that estimate the same; and
- stronger need for cybersecurity investment — 72% of larger SMBs believe they need to invest more vs. 56% of smaller SMBs that believe the same.

It is possible that as a small business grows, it could become a more likely target for bad actors. It is also possible that small businesses with cloud-based services with built-in security and fewer employees have fewer vulnerable attack entry points. However, as this year's growing attacks on local municipalities, schools and small hospitals have shown, smaller organizations can no longer count on flying below the radar and being ignored by cybercriminals.

The latest survey results show that as businesses become more dependent on technology — with more planning the adoption of A.I. — and as global borders become blurred in cyberspace, increased cyberthreats are expected to become a fact of life for all businesses, regardless of size or industry.

CONTACTS

If you have questions about this report, or would like to obtain permission to quote or reuse portions of this report, please contact by phone or email:

Jim McClellan
Director of Marketing and Communications
(850) 932.5338 x6452
jmcclellan@appriver.com

See ***here*** for more on the latest Cyberthreat Index for Business Infographic and Cyberthreat Holiday Shopping Report.

About Zix Corporation

Zix Corporation (Zix) is a leader in email security. Trusted by the nation's most influential institutions in healthcare, finance and government, Zix delivers a superior experience and easy-to-use solutions for email encryption and data loss prevention, advanced threat protection, unified information archiving and mobile security. Focusing on the protection of business communication, Zix enables its customers to better secure data and meet compliance needs. Zix is publicly traded on the Nasdaq Global Market under the symbol ZIXI. For more information, visit www.zixcorp.com.

About AppRiver

AppRiver, a Zix company, is a channel-first provider of cloud-enabled security and productivity services, with a 4,500-strong reseller community that protects 60,000 companies worldwide against a growing list of dangerous online threats. Among the world's top Office 365 and Secure Hosted Exchange providers, the company's brand is built on highly effective security services backed by 24/7 white-glove Phenomenal Care® customer service. AppRiver is headquartered in Gulf Breeze, Florida and maintains offices in Georgia, Texas, New York, Canada, Switzerland, and the UK. For more information, please visit www.appriver.com.