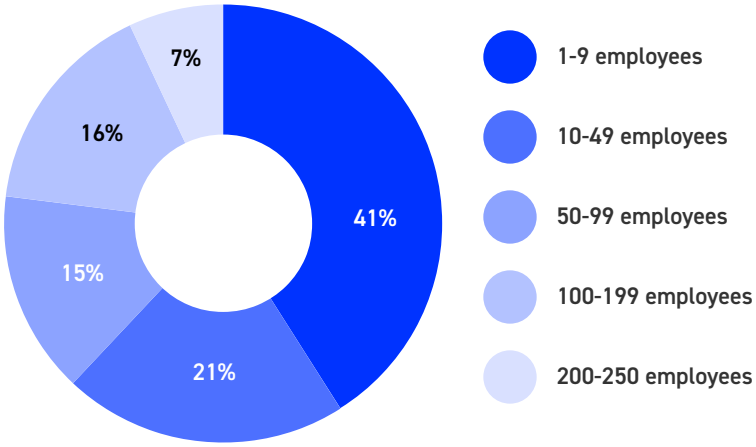
appriver
Now part of zix

APPRIVER CYBERTHREAT INDEX FOR BUSINESS: Q2 2019

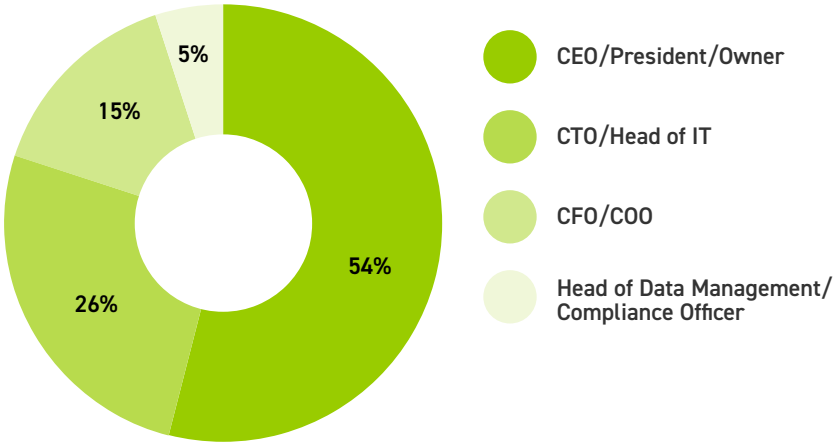
The AppRiver Cyberthreat Index for Business was developed by independent firms Idea Loft and Equation Research, in consultation with the University of West Florida Center for Cybersecurity, using survey data collected online in April 2019.

The survey has a + / – 3% margin of error. The national sample of respondents comprises 1,035 C-level executives and IT professionals in small-to-medium-sized businesses and organizations (SMBs). 69% of these SMBs have compliance requirements.

Company sizes



Job titles



Industries

Respondents' industries include:

- Business Services and Consulting
- Construction
- Financial Services and Insurance
- Government
- Healthcare and Pharmaceutical
- Hospitality
- Legal
- Manufacturing
- Marketing and Media
- Nonprofit
- Retail
- Technology
- Telecom
- Transportation and Logistics

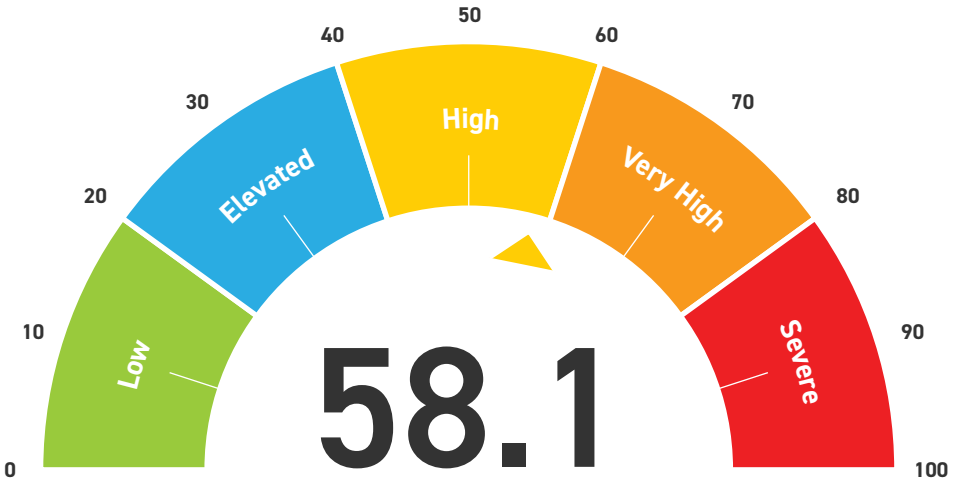
This proprietary and first-of-its-kind cyberthreat index was developed by measuring small- to medium-sized business decision makers' attitudes and experiences in twelve cybersecurity-related dimensions.

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 AppRiver Cyberthreat Index for Business fell slightly from 59.8 in Q1 to 58.1 in Q2.

The Index drop correlates with a quiet first quarter for cyberbreach news coverage, after an eventful year in 2018 when large-scale, high-profile cyberattacks – including on Facebook, Marriott, Quora, Target, and Under Armour – received high-visibility coverage in the news cycle.



Index Level is

HIGH

0
Complete cybersecurity confidence and readiness, with zero threat incidents

100
Complete absence of cybersecurity confidence and readiness, with constant threat incidents

Potential cyberthreats are top-of-mind for SMBs

- 77% of all SMB executives and IT decision makers surveyed in the second quarter report potential cyberthreats are a top-of-mind concern. That figure jumps to 91% among larger SMBs that employ 150-250 employees.

Actual attacks are believed to be prevalent

- The concern for potential threats are not surprising, considering 75% of SMB respondents say actual attacks are prevalent on a business such as their own.
- 40% of SMBs believe their business is vulnerable to "imminent" cyberattacks. This is a drop from 45% in Q1, consistent with the slight drop in overall Cyberthreat Index level, and also likely correlated with the drop in high-profile breach coverage.
- Finance and insurance, and the technology sectors experience the highest level of perceived vulnerability of "imminent" attacks.

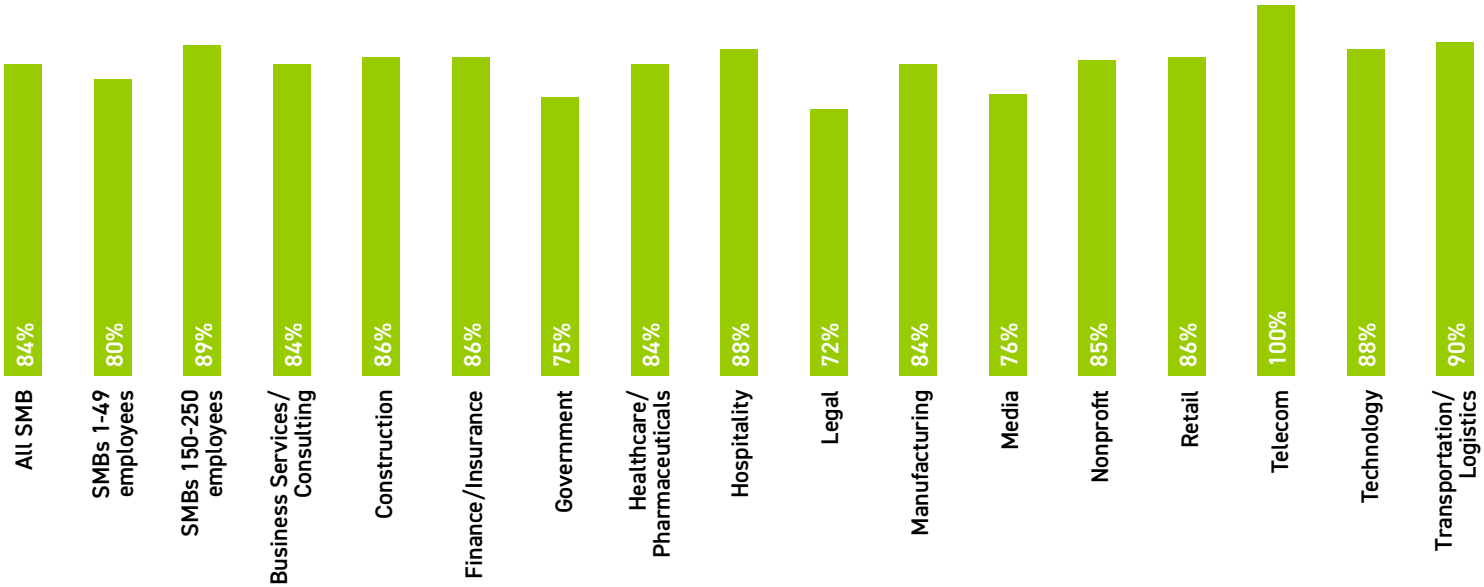
Index Survey Key Findings:

SOCIAL MEDIA CONSIDERED A CYBERSECURITY RISK

The use of social media apps and websites at the workplace or on a business device concerns SMB leaders and IT decision makers as a cybersecurity risk, according to 84% of all respondents surveyed. That figures increases to 89% among the larger SMB community.

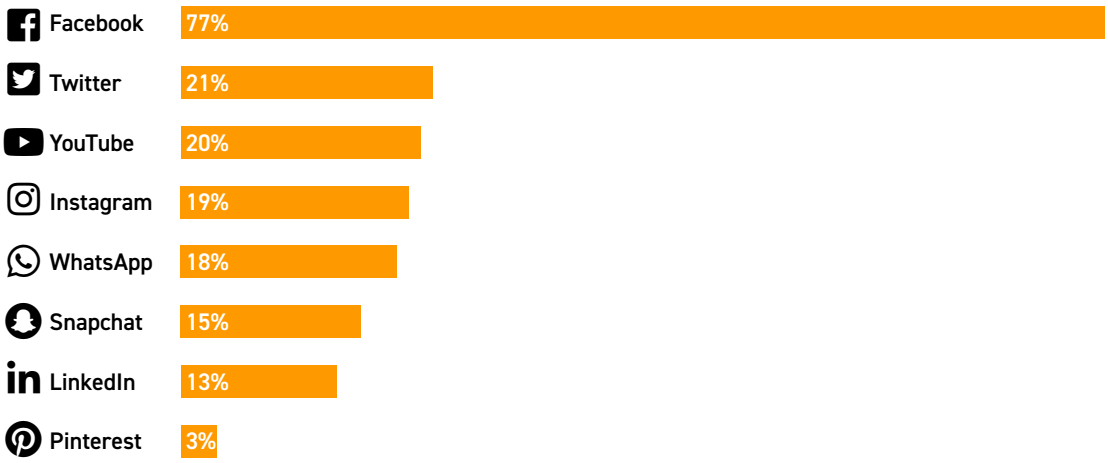
Among those concerned, 77% say they are most worried about employees' use of Facebook as a security risk, followed by 21% who say the same about Twitter (each respondent was given the option to name none, one, or two social media platform that concerns them most as a cybersecurity risk).

Percentage of SMB in verticals concerned about social media use as a cybersecurity risk



% of all surveyed SMB executives and IT decision makers who are concerned about employees' use of social media apps and/or websites at the workplace or on a business device as a cybersecurity risk.

Percentage who thinks this platform presents the highest cybersecurity risk



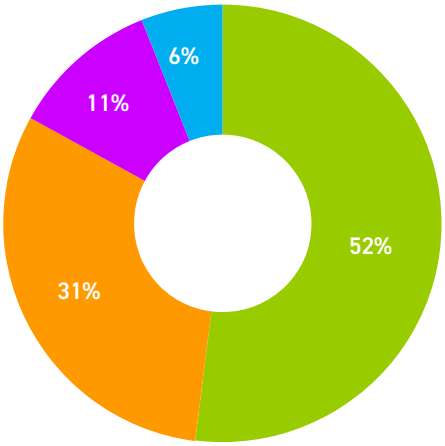
SMB respondents who are concerned about employees' use of social media apps and/or websites at the workplace or on a business device as a cybersecurity risk were given option to choose none of these, or one or two among these social media platforms as most concerning to them as a cybersecurity risk.

Index Survey Key Findings:

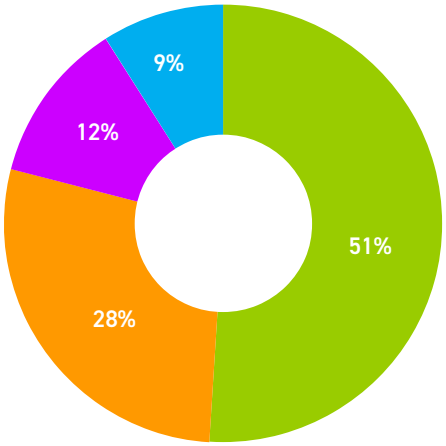
MANY SMBs ARE NOT VIGILANT ABOUT STORAGE SECURITY

While they are concerned about employees' social media usage as a security risk, many SMB leaders might also want to step up their own management of data storage. 48% admit their most confidential and important data is not stored exclusively on a secure network, but is instead spread across multiple unsecure locations, or they do not know where the data is stored.

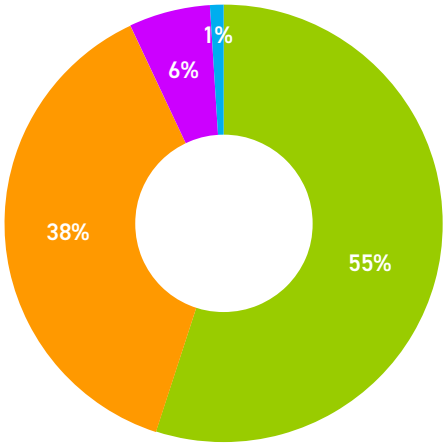
All SMBs



SMBs 1-49 employees



SMBs 150-250 employees



- Exclusively on our secure network and nowhere else
- On our executives' and employees' laptops, smartphones, tablets, other devices, in employees' home, as well as on our network
- On our executives' and employees' laptops, smartphones, tablets, other devices, in employees' home, but not on our network
- I don't know where the data is stored; we're busy so it's hard to keep up

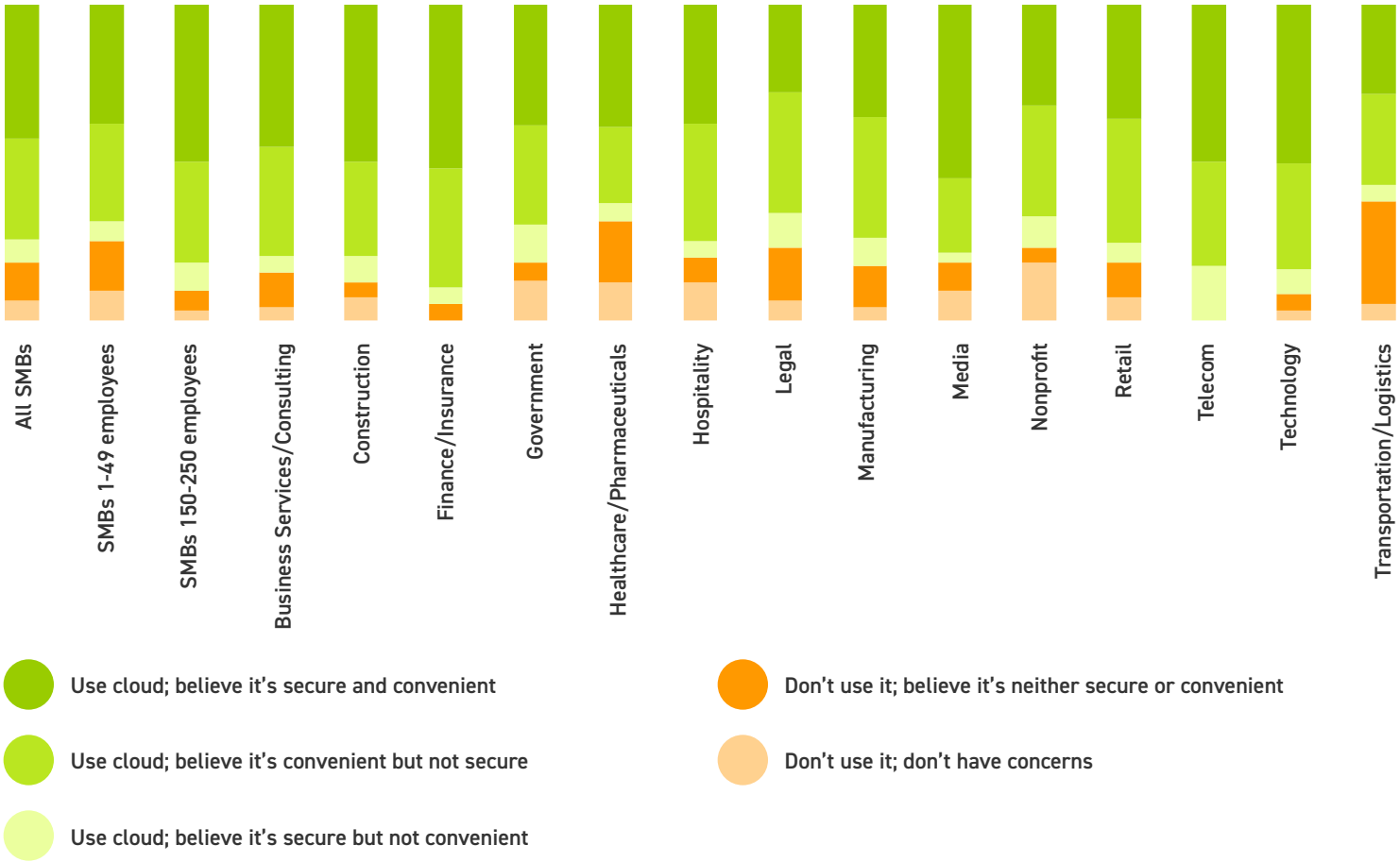
Index Survey Key Findings:

CLOUD STORAGE IS PREVALENT AMID TRUST ISSUES

81% of all surveyed respondents report they use cloud-based data management for their business.

- However, only 42% of all respondents – and 52% among those who currently use cloud – believe it is both secure and convenient.
- 44% of all surveyed respondents do not believe cloud-based storage is secure.
- 19% do not believe cloud-based storage is convenient.

SMBs' self-report of cloud storage and attitudes



Cloud prospect opportunities

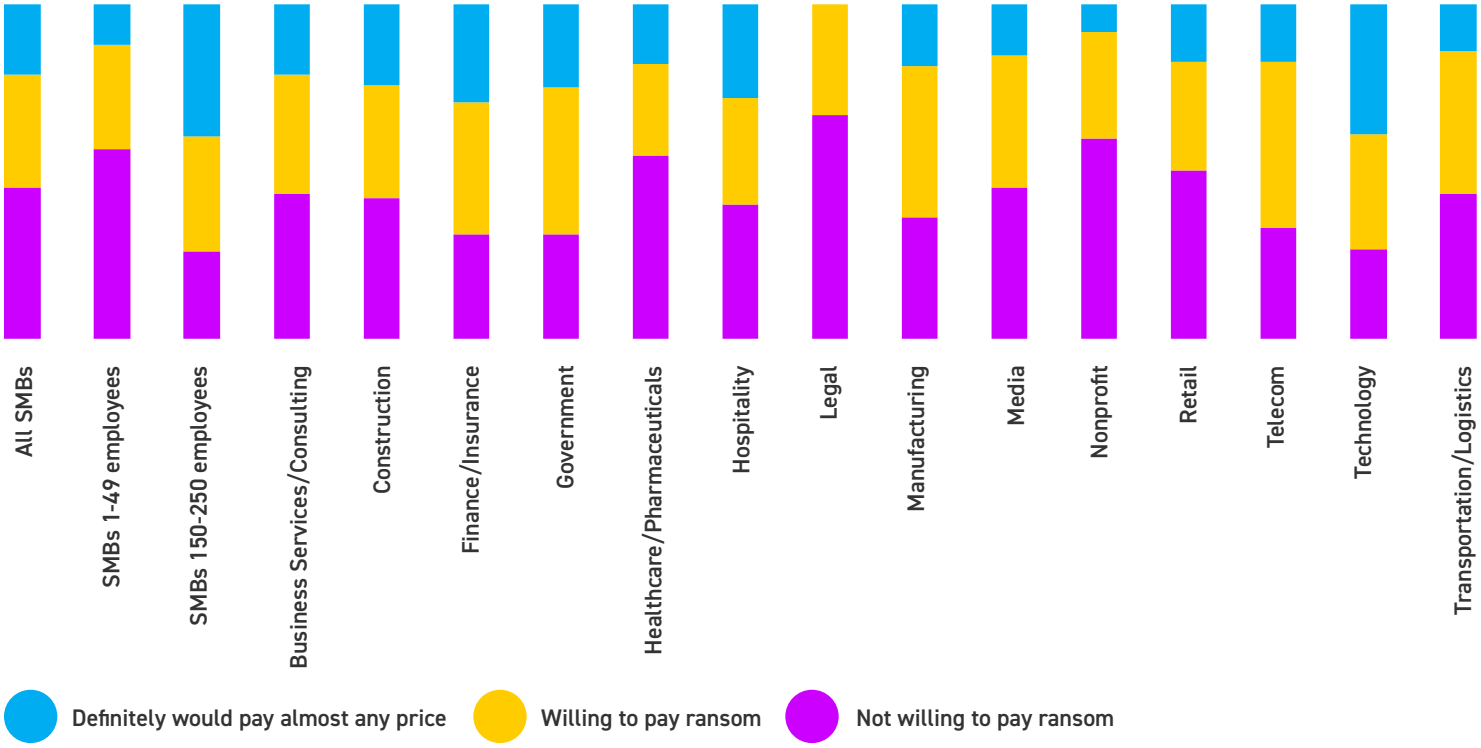
Over 10% of the following industries report they do not currently use cloud-based data storage but have no perception bias or concerns over its adoption:

- Government
- Healthcare/Pharmaceuticals
- Hospitality
- Nonprofit

Index Survey Key Findings:

OVER HALF OF ALL SMBs ARE WILLING TO PAY RANSOM TO CYBERCRIMINALS

- 55% of all SMBs admit they are willing to pay a ransom to hackers in order to recover breached data or to prevent it from being shared.
- 74% of large SMBs say they would be willing to pay ransom; 39% go as far as saying they "definitely would pay ransom at almost any price" to prevent their stolen data from being lost or leaked.
- 45% of all SMBs say they are not willing to give in to cybercriminals, regardless of the ransom amount or value of the hacked data.
- Technology SMBs are the most willing to settle with hackers with a ransom payment. Legal and nonprofit sectors are among the least willing to do the same.



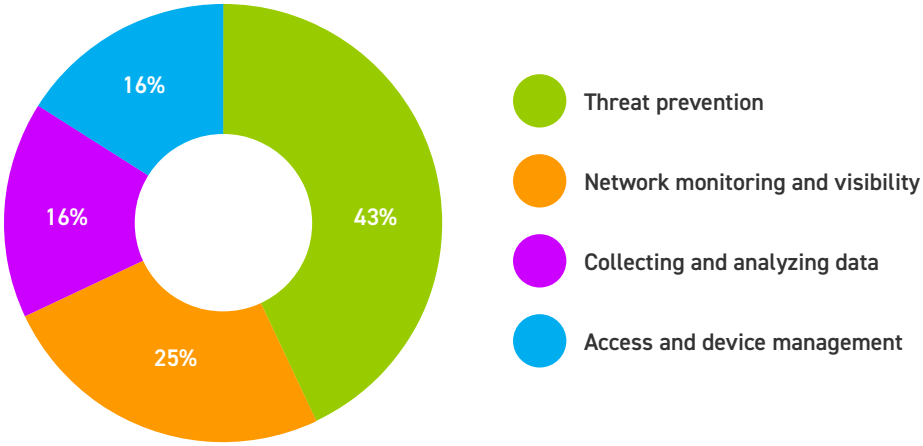
Index Survey Key Findings:

SMBs VALUE MSPs MOST FOR THREAT PREVENTION SUPPORT

Among SMBs surveyed that use an outside managed service provider (MSP) or technology consultant, 43% say they are most in need of support for threat prevention.

- Another 25% say the same about network monitoring and visibility, 16% each about collecting and analyzing data, and access and device management.
- Threat prevention was chosen as the service they need most from their MSPs in all key SMB industry verticals surveyed, with the exception of the legal sector, where SMBs say they most value MSP's support in network monitoring and visibility, ahead of threat prevention.
- Among the 1,035 total SMB executives and IT decision makers surveyed in Q2, 22% (228 respondents) say they do not use an outside managed service provider.

Area most in need of support from managed service providers



Most SMBs do not believe they can escape a successful attack unharmed

- It is not surprising that SMBs most value their MSPs for threat prevention support and some go as far as accepting ransom. 75% of SMBs believe a successful attack would be harmful to their business; 88% of larger SMBs (150-250 employees) believe the same.
- Only 36% of all SMBs estimate they can survive a successful attack without sustaining short- and long-term business losses.
- Interestingly, larger SMBs – which presumably have more or better cybersecurity resources – are most likely to believe business losses are unavoidable after a hacker's attack.
- 27% of healthcare and pharmaceutical SMBs, 20% in hospitality, 22% in retail, 21% in technology, and 24% in the transportation and logistics sectors predict their business would have a high likelihood of not surviving at all after sustaining a successful cyberattack.

Majority of SMBs believe cybercriminals have the upper hand

- 58% of C-level executives and IT decision makers at SMBs estimate hackers' attack strategies and technology are more sophisticated than their own threat prevention resources. This is a slight drop from 61% in Q1, within the margin of error.
- Larger SMBs appear again more cautious and feel less optimistic than smaller SMBs. In Q2, 66% feel they are outmatched by cyberhackers. Even given their presumably more abundant resources and better technology than smaller SMBs, only 1 in 5 (21%) of all larger SMBs surveyed believe their technology is more advanced than hackers they are up against.
- Overall, 47% of all SMBs give their own business a positive rating for cyber preparedness, a slight increase from Q1 (again this is likely correlated with the absence of a high-profile breach in the beginning of 2019). Larger SMBs again rate themselves lower (45% positive) than smaller SMBs (48% positive) in cyber preparedness in Q2, as they did in Q1.

After two quarters, a pattern emerged

- Larger SMBs (medium-sized businesses with150-250 employees) have a higher propensity to report they value cybersecurity resources, external cybersecurity partners, and internal cybersecurity talent (88% do in Q2) compared to smaller SMBs with 1-49 employees who say the same (74% in Q2, a 14-point differential).
- Larger SMBs also have a more cautious outlook on potential cyberthreat level, prevalence of attacks, and their own preparedness compared to cybercriminals' technology.
- It is reasonable to presume larger SMBs have more cyber preparedness resources at their disposal, however, they are also more likely to believe they need to invest more in cybersecurity – 63% believe they should invest more, including 36% who believe they should invest "considerably more," compared to 45% and 20% among smaller SMBs that believe the same.
- This consistent pattern suggests smaller SMBs could be underestimating their real cyberthreat risks. Reports of real threat incidents indicate cybercriminals do not discriminate; they are just as prolific in targeting smaller businesses – garnering smaller gains but with higher frequency of success – as they do large enterprises.
- The latest AppRiver survey highlights the urgent need to close the cybersecurity perception-reality gap within the small-to-medium-sized business community. There is a need to raise SMBs' awareness of the real risks they face, and increase their preparedness against likely attacks.

CONTACT

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

For more information about AppRiver, please visit appriver.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.