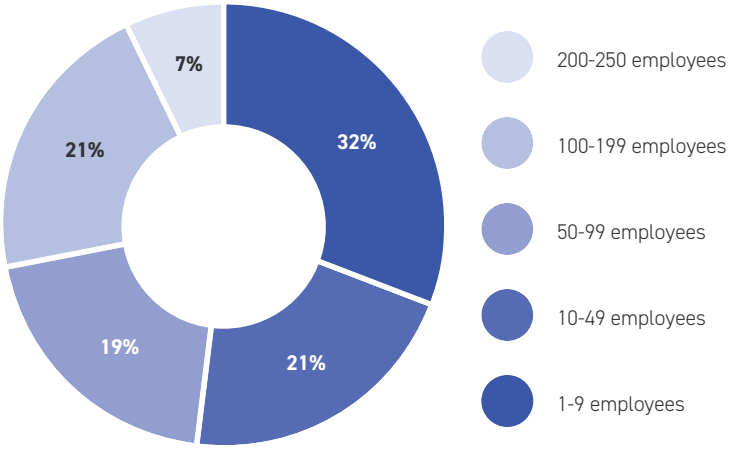
appriver®

APPRIVER CYBERTHREAT INDEX FOR BUSINESS: Q1 2019

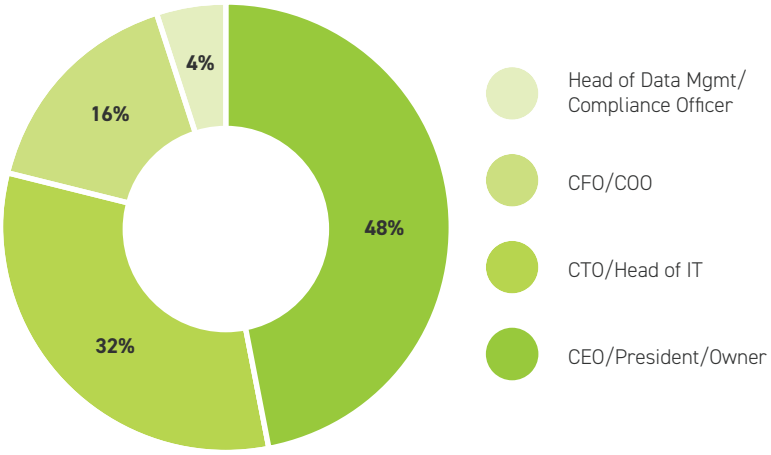
The AppRiver Cyberthreat Index for Business was developed by independent firms Idea Loft and Equation Research, in consultation with University of West Florida Center for Cybersecurity, using survey data collected online in January of 2019.

The survey has a +/– 3% margin of error. The national sample of respondents comprises 1,059 C-level executives and IT professionals in small- to medium-sized businesses and organizations (SMBs). 71% of these SMBs have compliance requirements.

Company sizes



Job titles



Industries

Respondents' industries include:

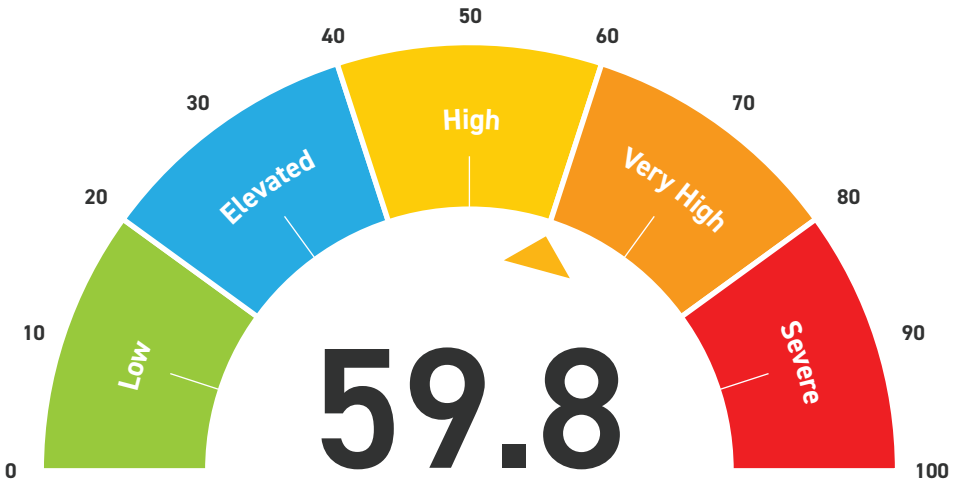
- technology
- marketing and media
- business services and consulting
- retail
- financial services and insurance
- healthcare and pharmaceutical
- telecom
- manufacturing
- hospitality
- construction
- government
- nonprofit
- legal
- transportation and logistics

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

Q1 2019 AppRiver Cyberthreat Index for Business



Index Level is

HIGH TO VERY HIGH

0
Complete cybersecurity confidence and readiness, with zero threat incidents

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

INDEX SURVEY KEY FINDINGS

Cyberthreats are prevalent among American small- to medium-sized businesses (SMBs)

- 64% of all SMBs – and 77% among SMBs with 150-250 employees (large SMBs) – report cybersecurity attacks are "prevalent" among businesses such as theirs
- 71% of all SMBs report to have experienced at least one incident of attempted cyberattack in their office within the last quarter
- SMBs in the technology, finance, and healthcare sectors were most likely to report high prevalence of attempted cyberattacks within the past quarter

Cybersecurity threats tend to be top-of-mind for SMBs

- 78% of all SMBs and 92% of large SMBs say cybersecurity threats are often on their minds
- Over 1 in 4 large SMBs (27%) say cybersecurity threats are "constantly" on their minds
-

Many SMBs feel vulnerable to cyberattacks and lack confidence in their readiness

- 45% of all SMBs and 56% of large SMBs believe they are vulnerable to "imminent" threats of cybersecurity attacks
- 61% of all SMBs and 70% of large SMBs believe cyberhackers have more sophisticated technology at their disposal than the SMBs' own cybersecurity resources
- SMB decision makers in the technology sector are more likely than their peers in other sectors to believe hackers have better technology and that their own business is more vulnerable to imminent cyberthreats. This suggests SMBs in some sectors could be naive about realistic threats they are exposed to. Respondents in the hospitality, retail and nonprofit sectors are among SMBs that are more likely to believe they have sophisticated technology comparable to cybercriminals', and that they are not susceptible to cyberattacks.

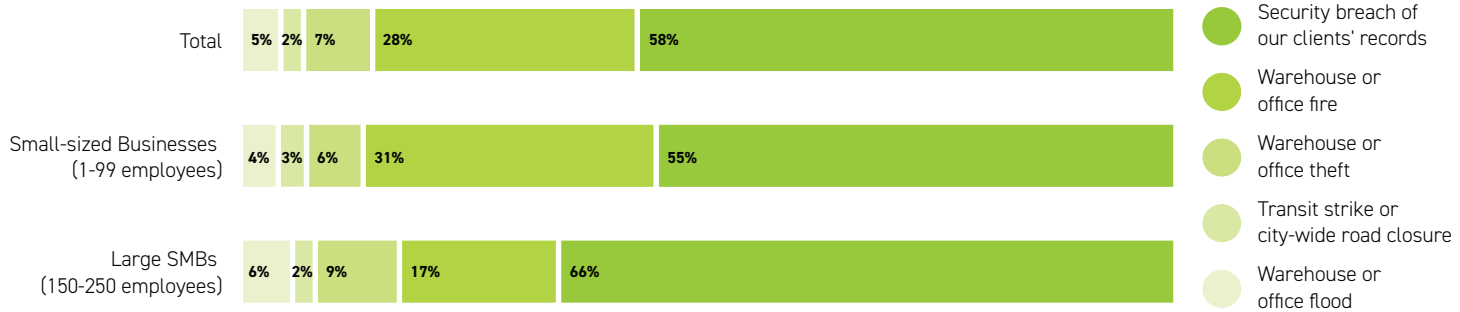
Majority of SMBs predict a successful cyberattack would inflict damages to their business

- 63% of all SMBs and 69% of large SMBs believe a successful incident of cyberattack could lead to short- and long-term business losses
- 20% of all SMBs predict there is a high-to-definite likelihood their business woud not survive at all after a successful cyberattack
- 31% of all large SMBs predict a successful cyberattack would be "extremely harmful" to their business
- Only 5% of all SMBs estimate they could survive a successful cyberattack without suffering damage to their business

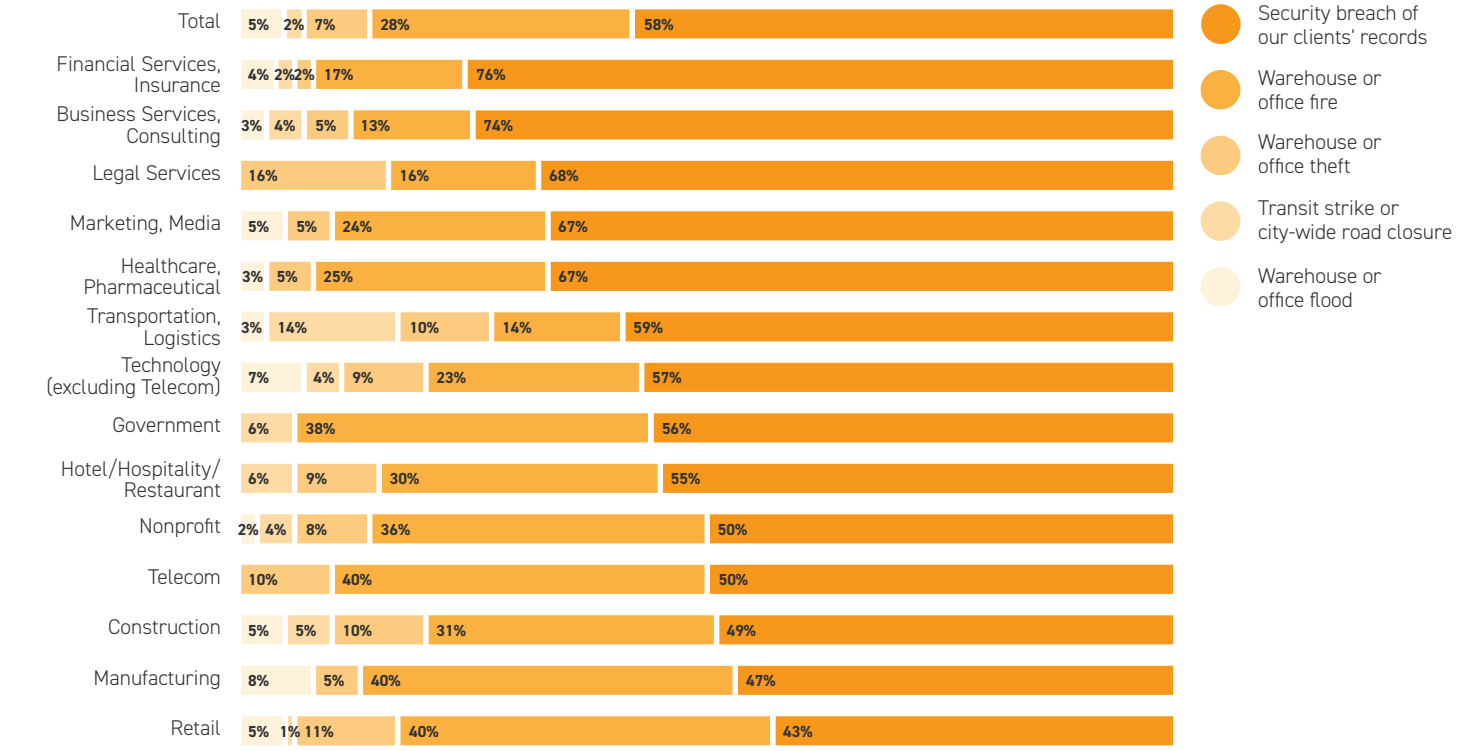
The successful security breach of clients' records in particular is feared by some SMBs as a potentially detrimental, business-ending event

- 58% of all SMBs and 66% of large SMBs believe a security breach of their clients' records would be a more detrimental event that is more likely to end their business than the combined effects of an office or warehouse fire, an office or warehouse flood, an office or warehouse theft, and a transit strike or city-wide road closure
- 76% of financial services and insurance SMBs, and 67% of healthcare SMBs believe a breach of their clients' records would be the most detrimental event
- A customer data breach is chosen as the single most-feared type of data breach by SMBs
- The second most-feared type of data breach is the breach of financial and banking information

Most Detrimental Event by Company Size



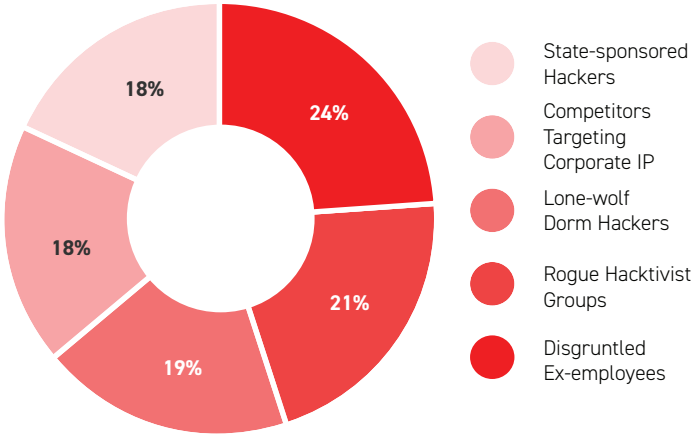
Most Detrimental Event by Industry



Depending on their size and business sectors, SMBs have different sources of cybersecurity concerns

- Smallest SMBs with 1-49 employees are more concerned about breaches committed by disgruntled ex-employees than by professional cybercriminals
- Large SMBs tend to be more concerned about competitors targeting their intellectual properties
- Most SMBs – with the exception of government organizations – consider state-sponsored hackers the least likely source of cyberthreats that would target their SMBs
- Telecom, transportation and logistics, legal, and healthcare sector SMBs tend to be more concerned than executives in other sectors about being targets of rogue hacktivist groups

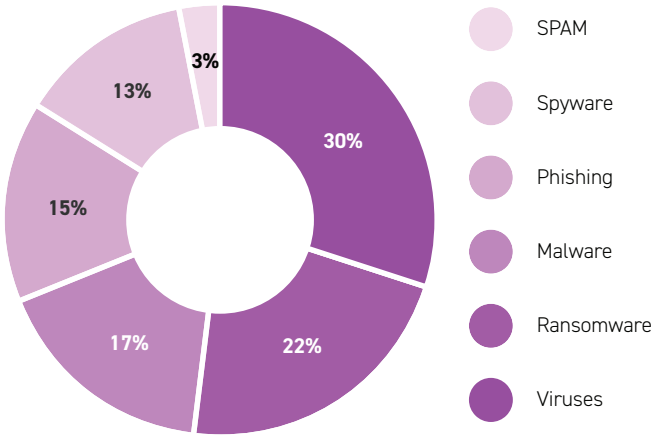
Source of Cyberthreat Feared Most



More SMBs fear viruses than they do other common types of cybercriminals' tools

- 30% of all SMBs surveyed choose viruses as a common cyberhacking tool they fear most, followed by 22% who choose ransomware, and 17% who choose malware
- However, a more accurate picture emerges when examining specific SMB size and business sectors: more large SMBs (29%) say they fear ransomware most than they do other cyberthreat tools
- Media, legal, nonprofit, and transportation and logistics SMBs choose viruses as the most feared cyberthreat tool
- Ransomware is feared most among government and telecom SMBs
- Phishing attempt is perceived by SMBs to be among the most common tool used by cybercriminals to target their businesses, with 71% of all respondents reporting someone in their office having been a target within the past quarter; however, SMBs did not choose phishing as the cyberhack tool they fear most, likely because many phishing attempts are foiled by our SMBs before they become successful

Tools of Cyberthreat Feared Most



Perceived vulnerability and estimated cyber damages do not necessarily translate to practice of vigilance

- 70% of SMB respondents have logged onto public wifi using their work devices at places such as airports, airplanes and coffee shops
- 53% admit to doing so at least from time to time or frequently

Most SMBs believe they could do more to improve their cybersecurity readiness

- Only 44% of all SMBs in the AppRiver survey give their business a positive rating for cybersecurity readiness
- SMBs that are more likely to self-report a positive rating in cyber preparedness include those in the government, technology, and transportation and logistics sectors
- SMBs least likely to self-report a positive rating in cybersecurity readiness include those in the hospitality, legal, nonprofit and retail sectors; SMBs in the hospitality and nonprofit sectors are also among those most likely to believe they are not vulnerable to imminent cyberthreats
- Just over half of all SMBs (53%) admit they do not invest enough in their cybersecurity; when looking at only large SMBs, that number jumps to 63%
- This appears to be another attitudinal dimension that affirms larger SMBs tend to demonstrate a higher level of cybersecurity concerns and to be more likely to value cybersecurity investment
- 74% of transportation and logistics, and 61% of healthcare SMBs say their cybersecurity talent and partners are "highly to extremely vital" to the success of their business, vs. 45% in the construction and hospitality sector SMBs who say the same

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 is a channel-first provider of cloud-enabled security, productivity, and compliance 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, United Kingdom and Spain.