Cyber & Homeland Security

Increase Business-Government Collaboration to Protect the Nation

RECOMMENDED ACTIONS

- Expand partnership between business and government to report and manage cyber and homeland security threats and reduce systemic risk
- Increase government support to limit liability in the event of a cyberattack and create incentives that encourage transparency, cross-industry knowledge sharing and the adoption of best practices
- Provide federal technology, tools and best practices to businesses (e.g., encryption) to ensure high protection of U.S. assets against cyber threats
- Train a national cybersecurity workforce through public-private partnerships (e.g., apprenticeship models, government placements, training of veterans)

Nearly 500 million
Personal records stolen or lost in 2018

~246 million
New unique pieces of malware identified in 2018

$6 trillion
Estimated annual cost of counterattacks globally by 2021, up from $3 trillion in 2015

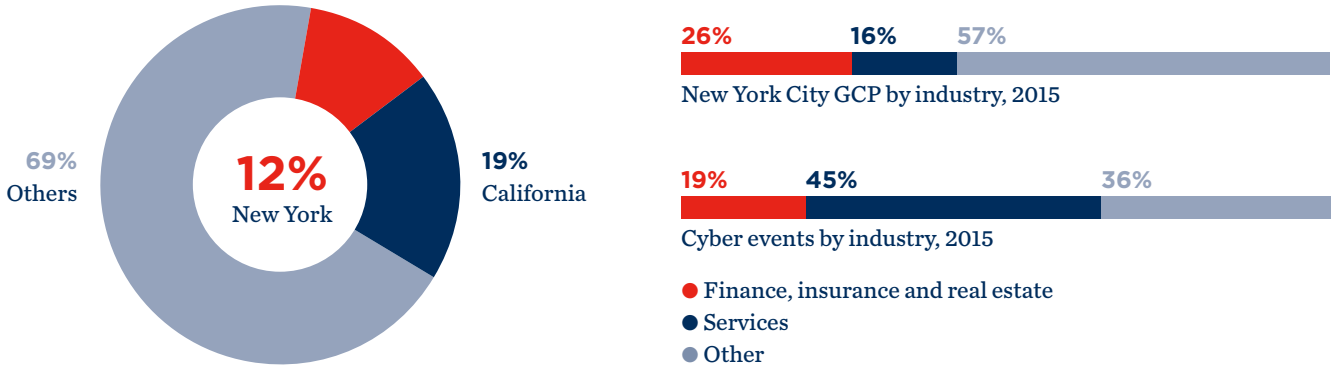
Competition for cyber talent is increasing, leading to a major skills shortage.

~3.5 million
Expected global shortfall in cybersecurity professionals by 2021

300,000+
Unfilled cybersecurity jobs in the U.S.

Figure 6

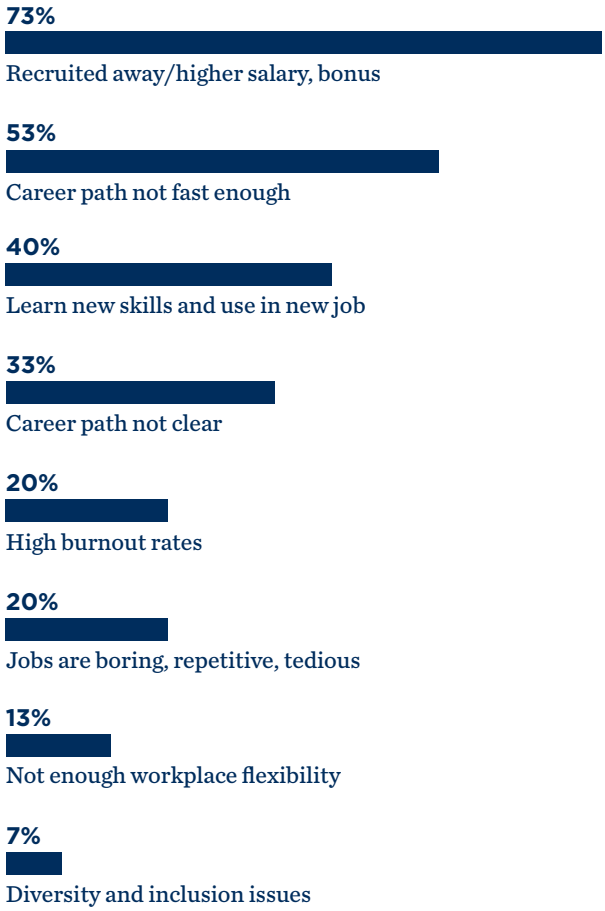
As a global financial, media and services center, New York City is a target for cyberattacks.



Share of U.S. events by state to date.

Figure 7

There are a number of reasons the cyber industry struggles to recruit talent.



Based on a 2016 global survey.

Figure 8

New York City suffered the highest number of terrorist incidents of any U.S. city (2002–2017).

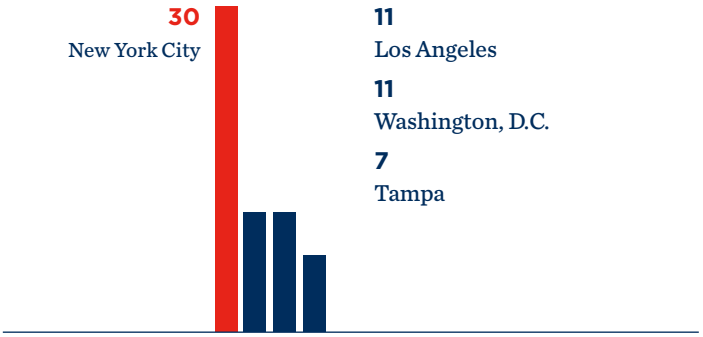
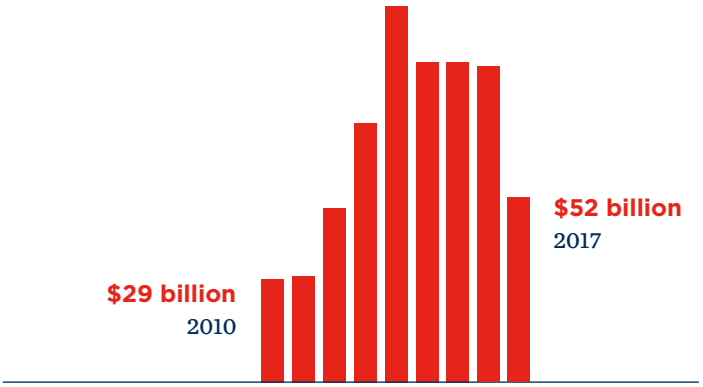


Figure 9

The global economic cost of terrorism is significant.



Economic cost includes direct and indirect costs from the loss of life, destruction of property and losses from ransom payments.