

## Cybersecurity and Small Business Protection

---

### Problem:

Small businesses are relying on information technology more than ever, with the White House and Congress taking notice of technology's impacts on the small-business community. That said, the very tools making small businesses competitive are also putting them in the crosshairs of cyber-attacks.

- According to NSBA's 2021 U.S. Small Business Recovery and Technology Report, just 34 percent of small businesses reported completing a technology audit. Compare this with NSBA's previous technology-related surveys, where 96 percent of small-business owners responded that they were concerned about targeted cyberattacks, with another 35 percent of respondents indicating having fallen victim to a cyberattack already,
- 45 percent of small business owners who responded to the survey informing the Report said they are primarily responsible for handling online security.
- The 2021 Recovery and Technology Report further revealed small businesses' number one challenge is taking appropriate technology security precautions, yet fewer small-business owners today say they have a high understanding of cybersecurity issues compared to even just two years ago.
- This decline is likely driven by growing concerns over pandemic-related economic slowdowns and prioritizing keeping businesses afloat over IT and implementing sound technology practices; however, the decrease among small-business owners who said they are "very concerned" about cybersecurity does not correlate with any kind of easing-up in cyberattacks, highlighting a disconnect between perceived risk and the very real threat of a cyberattack.
- Cyberattacks cost small businesses an average of \$5,120, according to a 2019 NSBS survey, with greater industry data only pointing to increases in average costs of attacks.

### Solution:

There is a sizeable gap between cyber policy and small business practices, and cyber-attackers are becoming increasingly sophisticated. These damaging campaigns are increasingly targeting small-business owners already impacted by a sluggish economy stemming from the downturn of COVID, limited in capacity to create systems to prevent cyber threats, but trends of attacks are only continuing upward.

- Congress must minimize regulatory burdens on small businesses so owners may be able to invest resources in IT and technology security.
- Agencies should continue working to provide resources and platforms that support small businesses' pursuit of adapting to best practices for cybersecurity.