

# Is Your Small Business Prioritizing Cybersecurity?

Article By:

Joseph J. Lazzarotti

Maya Atrakchi

---

A recent [study](#) surveying small and mid sized businesses (SMBs) found that 67% had experienced a cyber attack in 2018, and yet that same study found that cybersecurity is still “not on the to do list” for SMBs – 60% of the SMBs surveyed responded that they did not have a cybersecurity plan in place, and only 9% ranked cybersecurity as a top business priority. The federal government has taken notice of these concerning statistics.

Early this month, the U.S. House of Representative passed five bipartisan bills to help small businesses. Among the bills passed, two specifically aim to enhance a small business’s ability to prevent and respond to a cybersecurity incident. First, the SBA Cyber Awareness Act, [H.R. 2331](#), aims to strengthen the Small Business Administration’s handling and reporting of the cyber threats that affect small businesses. The bill requires the SBA to provide an annual report on the status of SBA cybersecurity, and notify Congress of any incident of cyber risk and how the SBA is addressing it. Second, the Small Business Development Center Cyber Training Act of 2019, [H.R. 1649](#), requires the Small Business Administrator to establish or certify an existing cyber counseling certification program to certify employees at small business development centers. It also requires the SBA to reimburse lead small business development centers (SBDCs) for any costs relating to such certifications up to \$350,000 in a fiscal year.

The Senate has also introduced legislation to help SMBs better address cyber threats. In late June, Senator Marco Rubio (R-FL) joined by Senator Gary Peters (D-MI) introduced the Small Business Cybersecurity Assistance Act of 2019, [S.2034](#) that aims to better educate small businesses on cybersecurity through counselors and resources offered at SBDCs. The bill incorporates recommendations suggested by DHS and SBA’s Small Business Development Center Cyber Strategy in a [report](#) from March of 2019, which described challenges small businesses face with implementing cybersecurity for their business, including the confusing nature of government cyber resources and lack of training.

The cyber threats plaguing SMBs are real, and SMBs need to address the significant risk to their businesses. The cyber insurance industry is increasingly targeting SMBs with robust insurance policies, comparable to offerings for larger companies. While insurance is a helpful component of an overall risk management strategy, it should not be the only component.

In the event of a data breach, the policy might cover costs related to responding to that breach (sending notices, offering credit monitoring, etc.) and business interruption costs, but it might not cover the costs of a federal or state agency inquiry following the reported breach. That is, if, for example, a small health care practice reporting a breach might trigger a compliance review by the federal Office of Civil Rights. In that case, OCR investigators would be looking for information about the breach, but also evidence that a risk assessment was conducted, copies of written policies and procedures covering administrative, physical, and technical safeguards to protect health information, acknowledgments that employees completed HIPAA training, and other information to support compliance. Having these compliance measures in place can substantially limit an SMB's exposure in these kinds of federal or state agency inquiries, as well as strengthen the SMB's defensible position should the SMB be sued as a result of a breach.

---

Jackson Lewis P.C. © 2025

---

National Law Review, Volume IX, Number 220

Source URL: <https://natlawreview.com/article/your-small-business-prioritizing-cybersecurity>