Cyberattacks have affected an unprecedented number of people.

Equifax: 147.9 million
Target: 41 million
Yahoo: 3 billion

And those are just a few of the big names. Smaller organizations are just as susceptible. In fact, Symantec reports that 43% of cyberattacks target small businesses.

It’s no surprise cybercrime’s global cost is estimated to reach $6 trillion by 2021.

Now, more than ever, organizations and accounting firms of all sizes need to be vigilant about protecting data, responding to threats and seizing opportunities to improve cybersecurity for clients.

Today, four of the leading 13 information security and cybersecurity consultants are CPA firms.

You’re the solution.
CPAs are fighting back, helping businesses protect sensitive information. How can you help your clients?

First, assess your practice area. Then, talk to your clients about why CPAs play an important part in their cybersecurity programs. There’s an action plan on the next page to help you.
Step 1: Assess your practice area.

Cybersecurity is not a key practice area for your firm.

Not every CPA firm is equipped to tackle clients’ cybersecurity concerns, but here’s what you can do:

• Ask your clients about staff training programs; privacy and security policies; response plans; and other controls and policies in place that help mitigate risks and/or manage the aftermath of security incidents.

• Introduce your client to the Cybersecurity Risk Management Reporting Framework. This market-driven, flexible and voluntary framework helps organizations evaluate their cybersecurity programs. Organizations of any size and in any industry around the world can benefit.

• Connect clients to experts who can help them put together an effective cybersecurity risk management program. By demonstrating concern for their business’s well-being, you’ll strengthen client relationships. The AICPA Private Companies Practice Section’s (PCPS) Building a Cybersecurity Practice Toolkit can help you begin those critical discussions.

Your firm has specialized knowledge and experience in cybersecurity.

You’ve got cyberskills. Here’s how you can use them:

• Introduce your client to the Cybersecurity Risk Management Reporting Framework.

• Consider providing advisory services that help companies spot cybersecurity weaknesses and offer advice on how to safeguard information and systems.

• With SOC for Cybersecurity, your firm could examine and report on an organization’s description of its cybersecurity risk management program and the effectiveness of controls within that program.

Step 2: Talk to your clients about CPAs and cybersecurity.

Why should clients look to your firm for cybersecurity guidance? Because of your education, experience and expertise. All CPA firms that provide advisory and/or assurance services have:

• Expertise in evaluating processes and control effectiveness

• Proficiency in measuring performance against established criteria and reporting results

• Objectivity, credibility and integrity

• Independence, professional skepticism and commitment to quality

• Strong analytical skills

Many specialized firms also have:

• Knowledge of relevant IT systems and technology

• Understanding of IT processes and controls

• Experience with common cybersecurity publications and frameworks (NIST CSF, ISO 27001/27002, COSO’s 2013 Framework, COBIT 5, etc.)

• Multidisciplinary teams that include certified information security professionals, such as Certified Information Systems Security Professionals (CISSP), Certified Information Systems Auditors (CISA) and Certified Information Technology Professionals (CITP®)

• Holistic understanding of an entity’s industry and business, including whether the industry in which the entity operates is subject to specific types of or unusual cybersecurity risks and uses specific industry technology systems

Visit aicpa.org/cybersecurity to download our cybersecurity toolkit.