IF YOU'RE HACKED, WHAT'S YOUR CYBERSECURITY LIABILITY?

By Cathy Whitley

Cybersecurity attacks are inevitable. That's the unfortunate reality. In fact, in a special report, Cybersecurity Ventures projects cybercrime's global cost will exceed $1 trillion between 2017 and 2021[1].

Safeguarding clients' nonpublic information from cybercriminals is a top priority for CPA firms. The latest data breach statistics from the 2018 Identity Theft Resource Center Data Breach Report[2] show an alarming number of exposed consumer records in the U.S., including:

- 1,244 reported breaches, exposing 446 million records;
- 46% of all breaches involved businesses;
- 39% of all breaches resulted from hacking by outside sources;
- 49% of all breaches exposed Social Security numbers.

Now more than ever, organizations and accounting firms of all sizes need to be vigilant about protecting data and responding to threats.

What's My Liability?

"That's a big question we hear from firms regardless of whether they've been attacked," said Stan Sterna, vice president and risk control specialist for Aon. "There are actually no uniform federal laws on business cybersecurity. But there is a patchwork of state and federal rules." Under certain state laws, CPAs can face liability for cybersecurity breaches that expose personal information.

All 50 states have rules for handling breach notifications and for what remediation measures need to be taken. Breach requirements depend on where the client resides – not where your firm is located. We encourage you to learn the dynamic requirements of states that apply to you.

A recent amendment to the Texas Identity Theft Enforcement and Protection Act[3] takes effect on Jan. 1, 2020. It requires that breach notices must be made to affected individuals and the Texas attorney general within 60 days after a determination has been made that a breach of system security involving sensitive personal information has occurred.

1 2019 Cybersecurity Market Report, https://cybersecurityventures.com/cybersecurity-market-report/

2 https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf

3 Tex BC. Code Ann. § 521.053, https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm#521.053

A recent amendment to the Texas Identity Theft Enforcement and Protection Act takes effect on Jan. 1, 2020.

The attorney general must also be notified if the breach affects more than 250 Texas residents. The data breach notification law has been amended several times since its passage in 2009. It requires notification of affected individuals in the event a data breach results in the disclosure of unencrypted personal information consisting of an individual's first name or first initial, last name and certain personal information, such as Social Security and driver's license numbers.

Federal Rules and Law

The Safeguards Rule is enforced by the Federal Trade Commission and applies to all companies defined as financial institutions under the Gramm-Leach-Bliley (GLB) Act. Businesses that prepare tax returns fall within this definition. Under the rule, businesses are required to develop a written information security plan that describes their program to protect customer information. There are five additional requirements. Learn about the rule and implement applicable compliance protocols.[4]

Do clients have standing to sue a CPA firm if they did not suffer damages as a result of a data breach? At the federal level, the circuit courts are split as to what constitutes sufficient standing to sue in cyber breach cases. Some courts hold that companies may be liable for damages if client or employee data is stolen, even if the theft causes no harm; instead, it's sufficient to merely allege that the information was compromised. This broad interpretation will only further increase the risk of cyber liability claims.

Two recent decisions illustrate these differences:

- The Sixth Circuit court, citing the defendant's offer for free credit monitoring as evidence, joined the Seventh and Ninth Circuits in holding that a cyber victim's fear of future harm is real and provides sufficient standing to sue. This particular ruling specifically undermines the defense that if no actual cyber fraud or identity theft occurred, the victim has not been damaged and has no standing to sue.[5]
- However, in another case, the Fourth Circuit held that a plaintiff must allege and show that their personal information was intentionally targeted for theft in a data breach and that there is evidence of the misuse or accessing of that information by data thieves.[6]

The division among the circuit courts as to standing is not likely to be resolved unless and until the U.S. Supreme Court decides a case on the issue.

New Cybersecurity Regulation Sets the Stage for Other States to Follow

In response to several highly publicized consumer data breaches, in 2017 the New York State Department of Financial Services enacted 23 NYCRR 500, "Cyber Requirements for Financial Services Companies," with which all affected firms must now comply. These "first-in-the-nation" data security regulations establish the steps that covered entities must take to secure customer data. The regulations are designed to combat potential cyber events that have a reasonable likelihood of causing material harm to a covered entity's normal business operations.

Specifically, insurers, banks, money services businesses and regulated vital currency operators doing business in New York with 10 or more employees and $5 million or more in revenues must comply with the new rules. Under the provisions, companies must:

- Conduct a cybersecurity risk assessment, prepare a cybersecurity program subject to annual audit and establish a written policy tailored to the company's individualized risks that are approved by senior management;
- Appoint a chief information security officer (CISO) responsible for the cybersecurity program, who regularly reports on the integrity, security, policies, procedures, risks and effectiveness of the program, and about cybersecurity events;
- Establish multi-factor authentication for remote access of internal servers;
- Encrypt nonpublic information (PII) and regularly dispose of any nonpublic information that is no longer necessary for conducting business (unless required to be retained by law);
- Prepare a written incident response plan that effectively responds to events and immediately provides notice to the superintendent of the New York Department of Financial Services of any breaches where notice is required to be provided to any government body, self-regulatory agency or any other supervisory body or where there is a "reasonable likelihood" of material harm to the normal operations of the business;
- Implement a written policy addressing security concerns associated with third parties who provide services to the covered entity, which contain guidelines

4 https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

5 *Galaria v. Nationwide Mutual Insurance Co.,* Nos. 15-3386/3387 (6th Cir. Sept. 12, 2016) (unpublished)

6 Beck, et. al. v. McDonald, et. al., No. 15-1395, (4th Cir. February 6, 2017)

for due diligence or contractual protections relating to the provider's policies for access, encryption, notification of cybersecurity events impacting the covered entity's nonpublic information and representations addressing the provider's cybersecurity policies relating to the security of the covered entity's information systems or nonpublic information;
- Annually file a statement with the New York Department of Financial Services certifying compliance with the regulations.

Meanwhile, the California Consumer Privacy Act of 2018 (CCPA) goes into effect on Jan. 1, 2020. The CCPA represents a significant expansion of consumer privacy regulation. Its GDPR-like statutory framework gives California consumers the right to:

- Know what categories of their personal information have been collected;
- Know whether their personal information has been sold or disclosed, and to whom;
- Require a business to stop selling their personal information upon request;
- Access their personal information;
- Prevent a business from denying equal service and price if a consumer exercises their rights per the statute;
- A private cause of action under the statute.

What is the Impact of These New Regulations on CPA Firms?

Whether or not a CPA provides professional services for an entity covered by the New York Department of Financial Services or the CCPA, these new rules are important.

Regulation in one state frequently results in regulation in other states. Both the New York and California cybersecurity regulations have served as a template for other states establishing cyber security legislation.

The regulations also create a framework for plaintiffs' attorneys to follow when alleging that a company (regardless of whether it is a covered entity) should have done more to protect private information, keep consumers informed and prevent a data breach, or that a CPA firm should have detected data security issues while providing professional services.

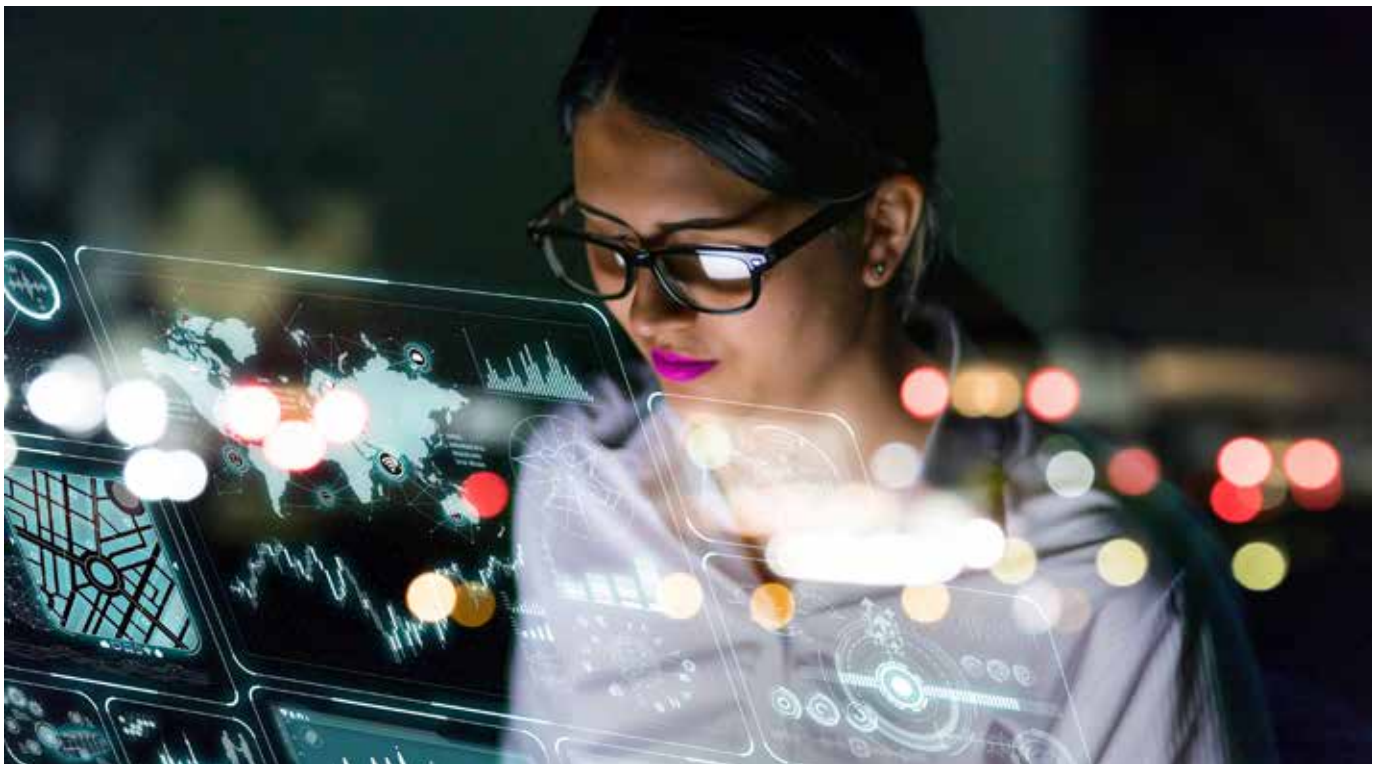
Take Preventative Action Now

"If someone sues your firm because of a data breach, you may have a stronger case if you can show that you've taken reasonable measures to help prevent an attack or theft," Sterna advised. "Setting up systems to assist in prevention is an important aspect of managing cybersecurity risk."

Three Tips to Get You Started

Start with an assessment. What are your cybercrime defenses? Do you have gaps in your data security procedures? Do you have controls in place? How do you document incidents when they happen? What is your response plan when incidents occur?

"Mapping where you stand today and your vulnerabilities is the best way to understand your next steps," Sterna said. AICPA's cybersecurity risk management reporting framework helps you assess existing risk management programs. The Private Companies Practice Section



cybersecurity toolkit can also help you understand the most common cybersecurity threats.

Implement best practices. At a minimum:

- Use encryption wherever appropriate to protect sensitive data; this includes laptops, desktops and mobile devices; failing to do so threatens your data and your reputation;
- Train employees to recognize threats and safeguard equipment and data;
- Develop and practice your response plan for various situations, such as a ransomware attack, hack or ID theft;
- Back up your data so you'll still have access to it if it's lost or stolen;
- Keep your equipment physically secure in your office and on the road.

Get an outsider's perspective. What better way to learn your firm's vulnerabilities than to hire an expert for penetration testing? Through a penetration test, a third-party consultant will perform a test tailored to your firm's needs and budget.

They'll provide insights on your firm's vulnerabilities and educate you about solutions for protecting your practice. A consultant can also help you implement regular drills that test your firm's response in the case of various attack scenarios.

Legal and Insurance Considerations

CPA firms should consult with their legal counsel to assess the firm's risk of first/third party data security claims and assess vendor data security coverage. The existence and adequacy of data security utilized by third party vendors (including contract tax return preparers) is often overlooked.

CPA firms should also consult with their insurance agent or broker to review their current cyber policy to ascertain the adequacy of coverage.

About the Author:

Cathy Whitley is Senior AICPA Risk Advisor for Aon Insurance Services, the national administrator of the AICPA Professional Liability Insurance Program since 1974 and has more than 20 years' experience with Aon. For more information, contact her at cathy.whitley@aon.com or visit www.cpai.com.