2019 Cyber, Management and Professional Liability Conference
July 10-12, 2019
Boston, MA

The New Frontier for Accountant Liability in the Age of Cyber Crimes

I. Understanding the Landscape

With increasing public and legal scrutiny on the protection and use of private and personal information, accountants and CPAs in particular find themselves with new obligations and related risk factors to consider as they go about their practices. For instance, there are numerous privacy and data security regulations codified throughout the federal code and regulations, as well as cyber laws that have been enacted in all 50 states that touch on a firm's practice. The task of wading through the labyrinth of regulations to determine what may apply, how to comply, and what penalties may arise for a lack of compliance, can be daunting. To ensure against risk of federal or state enforcement actions, client or third party lawsuits, and irreparable reputational damage, it is important for a CPA, its insurance partners, and their attorneys, to understand the current landscape of applicable federal and state regulations, as well as how these regulations are being interpreted and applied to keep up with new cybersecurity threats and protections.

A. Federal Cybersecurity Regulations

There are numerous privacy and data security regulations codified throughout the federal code, and those that apply to a accountant or CPA will largely depend on what services it is providing. Regardless of firm size, certain statutes impose stringent and onerous obligations, with related penalties, and it is worth understanding how these regulations apply in practice.

1. Heath Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH)

Most people are familiar with HIPAA, which was enacted in 1996, and generally concerns the protection and dissemination of protected health information (PHI). PHI is "individually identifiable health information" (IIH) (including demographic information) that (i) is transmitted by electronic media, (ii) maintained in electronic media, (ii) or transmitted or maintained in any other form or medium. 45 CFR §160.103. IIH includes basically any information created or received by a provider, employer, health plan, etc. that relates to the health of an individual and can be used to identify that individual. Id.

Under HIPAA, Covered Entities have specific obligations under security and privacy rules. "Business partners" or "business associates" of Covered Entities, such as vendors, CPAs and lawyers, are required to have a contract, referred to as a Business Associate Agreement ("BAA"), with the Covered

Entities that provides for certain protections. Generally, a Business Associate is "a person or entity that performs certain functions or activities that involve use or disclosure of protected health care information on behalf, or provides services to, a covered entity." See 45 CFR §160.103. For example, an accountant with access to patient billing records could be a Business Associate. A Business Associate also includes "subcontractors" of a Covered Entity or Business Associate, that creates, receives, maintains, or transmits protected health information on behalf of another Business Associate.

Before 2009, Business Associates only had to have a BAA with the Covered Entity that identified how it would keep PHI safe. However, there was little specificity required, and a Business Associate was not generally liable to Health and Human Services for breaches of agreement. The Business Associate was not required to offer, or account for, the same security and privacy protections as a Covered Entity. The Covered Entity could terminate or enforce the agreement, but that was about it, and it had the ultimate responsibility for ensuring compliance with security and privacy requirements. 45 CFR §§164.502-.503, .532. This all changed in 2009 when Congress passed the American Recovery and Reinvestment Act of 2009 (ARRA), and expanded the scope of a Business Associate's responsibilities and its related liability.

As part of the ARRA, Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH), which supplemented and expanded existing HIPAA law regarding the security and privacy of PHI. These are colloquially referred to as the Security and Privacy Rules.

i. The Security Rule

The most significant change brought by HITECH was to make the security obligations formally limited to the Covered Entity, also a Business Associate obligation. This can be a significant burden, with stiff penalties for failing to meet the relevant standards. Generally, the Security Rule mandates that a Covered Entity or Business Associate must ensure the confidentiality and availability of PHI, and protect against reasonably foreseeable threats to the exposure or unauthorized uses of PHI. 45 CFR §164.306.

45 CFR §164.308-316 describes what a Business Associate must do ensure it complies with this mandate. There several requirements, but they fall into three main categories: administrative, (refers to how a Business Associate should internally ensure the standards are met), physical (requirements for how data is stored and protected), and technical (encryption and software requirements).

ii. The Privacy Rule

The Privacy Rule generally mandates that a Covered Entity or Business Associate must not make any unauthorized uses or disclosures of PHI. 45 CFR §164.502-503. For the Business Associate, the Privacy Rule applies through the obligations set forth in the BAA it must have with the Covered Entity. The law requires that a Covered Entity and Business Associate, as well as a Business Associate and its subcontractors, enter into a BAA that describes how the Security and Privacy Rules will be complied with. 45 CFR §164.504. A Business Associate can violate the Privacy Rule through improper disclosure, or through use of information that the Covered Entity improperly disclosed to the Business Associate , 45 CFR §164.504(e)(2), **or** if a Business Associate knows a Covered Entity or a subcontractor is breaching the rule, a Business Associate has to report it, or face a penalty. 45 CFR §164.504(e)(1)(iii). A subcontractor is a Business Associate, and so breach violations can be enforced directly against a subcontractor that is not in direct contractual privity with the Covered Entity and does not receive PHI from the Covered Entity.

iii. Violations of the Security or Privacy Rules

Under 42 U.S.C. §1320d-5(a) breaches of the security and privacy rules are enforced by the Office for Civil Rights (OCR). Penalties can be stiff, ranging from $100 for a single violation where the Business Associate did not know or have reason to know that it violated the law, to $1.5 million for a violation by willful neglect.[1]

As of January 31, 2019, OCR has settled or imposed a civil monetary penalty in 62 cases resulting in a total dollar amount of $96,581,582.00. Of this total, in 2018, OCR collected nearly $29 million in settling or litigating HIPAA and HITECH enforcement actions.[2]

Most violations are enforced by OCR, but the law also gives state Attorneys General that right to bring a claim on behalf of its citizens for violation of the Act. 42 U.S.C. 1320d-5(d). In 2017, according to the HIPAA Journal, State AG settlements and judgment arising from HIPAA/HITECH enforcement actions exceeded $1.8 million.[3] In 2018, there were 12 enforcement actions by State AGs, totaling more than $3.5 million.

As a general rule, a violation does not create a private cause of action. Webb v. Smart Document Solutions, LLC, 499 F.3d 1078 (9th Cir. 2007); Acara v. Banks, 470 F.3d 570 (5th Cir. 2006); Sullivan v. Clallam County Public Health District. No. 2, 2016 WL 3059409 (W.D. WA. 2016); Johnson v. Quander, 370 F.Supp.2d 79 (D.D.C. 2005); Cassidy v. Nicolo, No. 03-CV-6603-CJS, 2005 WL 3334523 (W.D.N.Y. 2005)

However, in some states, violation of federal law can serve as a basis for a consumer protection act claim, and in other states a HITECH violation may be evidence supporting a claim for negligent misrepresentation, or fraud, against a professional. On December 4, 2018, 12 state Attorneys General filed a lawsuit against Medical Informatics Engineering (MEI) and NoMoreClipboard (NMC) over a 2015 data breach that exposed the data of 3.9 million individuals.[4] According to the complaint, MEI licenses WebChart, a web-based electronic health care application, to Covered Entities, and NMC, a subsidiary of MEI, provided services that, among other things, enabled patients to access their health records electronically.[5] The lawsuit alleges HIPAA/HITECH violations as well as state law violations of consumer protection acts and data security/privacy statutes. MEI and NMC were both Business Associates under HIPAA/HITECH.

Finally HITECH also includes breach notification requirements, 45 CFR §§ 164.400-414, where Covered Entities must provide notification of the breach of unsecured data, (breach notification is not required where the information is secured data, like encrypted or unreadable or unusable), to affected individuals, the Secretary, and, where the breach affects 500 or more people, the media. The notification requirement does not apply to Business Associates, but HITECH gives Covered Entities the ability to delegate notice responsibility to the Business Associate where it was the Business Associate that caused the data breach. See 45 CFR §164.410.

There are fewer solely breach notification enforcement actions, with the first reported enforcement and related settlement occurring in January 2017. The Covered Entity failed to report

---

[1] https://www.hhs.gov/sites/default/files/2018-ocr-hipaa-summary.pdf

[2] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

[3] https://www.hipaajournal.com/2017-hipaa-enforcement-summary/

[4] https://images.law.com/contrib/content/uploads/documents/292/Indiana-Suit.pdf

[5] *Id*.

within 60 days and agreed to pay $475,000.[6] Penalties are assessed for breach notification in the same way as for breaches of the Security or Privacy Rules. Ranging from $100 for an unknowing breach, to $1.5 million for willful neglect. 42 U.S.C. §1320d-5. An accountant with access to patient billing records could face similar exposure for failing to report a breach by it, or its Covered Entity.

2. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act, (GLBA), also known as the Financial Modernization Act of 1999, requires "Financial Institutions" to explain how they share and protect their customers' private information. 15 U.S.C. §§6801-09, 6821-27. GLBA is enforced by the Federal Trade Commission, though the Securities and Exchange Commission has adopted the GLBA privacy and security rules, and also enforces GLBA violations.

Under the Act, tax return preparers are Financial Institutions. 16 CFR §313.3(k)(2)(viii). However, the Act "applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family or household purposes…" and "…does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes." Id., at 313.1(a)-(b).

The Act has three basic requirements applicable to Financial Institutions: the Privacy rule mandates that Financial Institutions are to provide consumers with a privacy notice; under the Safeguards Rule, Financial Institutions must develop a written security plan describing how the company has prepared for, and plans to protect client data; and under the Pretext Rule, Financial Institutions must not access non-public personal information under false pretense. See 15 U.S.C. §§6801-09, 6821-27; 16 CFR § 313-314.

i. Privacy Notice

All Financial Institutions, regardless of size, must provide a "clear and conspicuous" written notice describing their privacy policies and practices. What the notice says will depend on what the Financial Institution does with the protected information. Generally, however, the notice must accurately describe how you collect, disclose, and protect the information.[7]

ii. Safeguard plan

Though there is some flexibility in what the plan must specifically include for each firm, depending on firm size and the nature and scope of services, generally a plan must:

- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program, and regularly monitor and test it;

[6] http://wayback.archive-it.org/3926/20170127111957/https://www.hhs.gov/about/news/2017/01/09/first-hipaa-enforcement-action-lack-timely-breach-notification-settles-475000.html

[7] *See* FTC guidance for more specific information regarding what the notice requires: https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm

- select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.[8]

As with violations of HIPAA/HITECH, a violation of the GLBA is treated as an "unfair or deceptive act or practice" enforceable by the FTC pursuant to 15 U.S.C. §57a, and 15 U.S.C. §45 et seq. Civil penalties for violations can be up to $100,000 for each violation by an organization and up to $10,000 for each violation by an officer or director. Criminal penalties can be up to five years in prison. 15 U.S.C. § 6823.[9] Fortunately, however, the GLBA does not provide for a private right of action. 15 U.S.C. § 6805(a); see also Dunmire v. Morgan Stanley DW, Inc., 475 F.3d 956, 960 (8th Cir. 2007) ("No private right of action exists for an alleged violation of the GLBA.").

[8] *See* FTC guidance at https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying. *See also* IRS publication 4557 for useful information.

[9] *See F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 245 (3d Cir. 2015) (court held that FTC has authority to cybersecurity breaches, where the data breach constituted an "unfair and deceptive act" pursuant to 15 U.S.C. §45(a).

3. Sarbanes Oxley

The Sarbanes Oxley Act, ("SOX") was enacted in 2002, and generally endeavors to protect shareholders and the public from accounting errors and fraudulent conduct by organizations. For large companies, Section 404 of SOX has a requirement that management annually assess the effectiveness of the company's internal control over financial reporting ("ICFR"), which can include an audit of its cybersecurity protocols and protections. Increasingly, CPAs are being engaged to perform these cybersecurity audits in connection with an ICFR engagement, or such an audit may be necessary to the extent the company determines disclosing cybersecurity protocol and risk facts is necessary on a Form 10-K financial statement. In either case, the CPA or firm must understand what its obligations are in this regard, how to protect itself, and what the potential exposure is for a failure to identify or report cybersecurity risks.

The SEC recently issued guidance specific to cybersecurity disclosures as part of SEC filings and ICFR attestation services. Comm'n Statement & Guidance on Pub. Co. Cybersecurity Disclosures, Release No. 10459 (Feb. 21, 2018). The guidance generally describes that "the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents. Companies are required to establish and maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity." Id. The guidance also makes clear a company's obligation to "refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents." Id.

The AICPA has developed System of Organizational Control engagements best practices guides to aid firms in identifying, and reporting on a client's cybersecurity risk management program.[10] These guidelines will help practitioners to ensure compliance with SOX and related SEC guidance, as well as to guard against professional liability claims that may arise from a company's data breach.

B. State Regulations

While most states have enacted data privacy and/or data protection statutes,[11] perhaps the most impactful state legislation to accountants are breach notification statues. All 50 states have enacted legislation addressing cybersecurity breach notification. There are numerous outlets that provide a summary of breach notification laws by state.[12] However, generally speaking, the type of notice, and to whom it must be sent will depend on whether the data was encrypted ("unprotected"), the number of people impacted, and whether there is a "risk of harm" to affected individuals.

Violation of a notification statute does not generally give rise to a private right of action in most states, and each state has different caps on the amount of any civil penalty. However, in most states a

---

[10] *See* https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html

[11] For information summarizing current legislation and proposals in each state, the National Conference of State Legislatures has a useful website: http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx

[12] *See*, for example, *State data breach notification initiatives*, 1 Data Sec. & Privacy Law § 7:58 (2018); https://www.foley.com/files/Publication/c31703ac-ee93-40a5-b295-7e1d9fe45814/Presentation/PublicationAttachment/903a95c5-0154-4091-88c7-b6438fed6127/18.MC12803%20Data%20Breach%20Chart%20012019%20V2_edit.pdf .

breach of the notification statute may give rise to a consumer protection act clam as an unfair or deceptive act or practice.

Further, in addition to state actions to enforce state breach notification laws, in some states, breach of a federal regulation can serve as a basis for a private right of action under state law. For instance, in California, "violations of federal statutes, including those governing the financial industry, may serve as the predicate for a UCL cause of action."
Rose v. Bank of Am., N.A., 57 Cal. 4th 390, 394, 304 P.3d 181 (2013). The UCL, or Unfair Competition Law, provides a cause of action for business practices that are (1) unlawful, (2) unfair, or (3) fraudulent. Cal. Bus. & Prof. Code § 17200. Each prong is a separate and distinct legal theory of liability. Lozano v. AT&T Wireless Services, Inc. 504 F.3d 718, 731 (9th Cir. 2007); In re Yahoo! Inc. Customer Data Security Breach Litigation, 2017 WL 3277318, at *20-24 (N.D. Cal. 2017); In re Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 990 (N.D. Cal. 2016) (holding that HIPAA violations were sufficient to sustain a claim under the UCL).

As state legislatures and state courts become more involved in developing law arising from data breaches, professionals should be diligent about understanding the law in their states to ensure their data protection protocols are consistent with federal and state law. Firms with access to PHI, or engaged to audit a client's cybersecurity protocol as part of an ICFR engagement, should, where possible, also consider robust indemnity and additional insured provisions to help spread the risk.

II. Professional Liability Claims Arising from Data Breach

While there has been a significant amount of data breach related litigation, CPAs and accountants have been largely left out of lawsuits arising from data breaches. This is despite the fact that large firms regularly undertake security audit engagements to opine on a company's cybersecurity protocols and protections. For instance, KPMG and Deloitte were each engaged by Equifax to audit its cyber security protocols, but have seemingly been left out of litigation related to the Equifax data breach.[13] However, given the breadth of case law establishing CPA liability to third parties arising from audit engagements, it is likely only a matter of time until a firm is sued over a client's data breach. This is particularly likely in light of recent case law concerning standing for data breach victims, where courts have held that the mere risk of future harm is sufficient to procure standing.

A. Risk of Future Harm and Standing

In federal court, standing requires a plaintiff to show: "(1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." Krottner v. Starbucks Corp., 628 F.3d 1139, 1141 (9th Cir. 2010). Recent litigation arising from data breaches have forced courts to examine Article III standing relative to individuals, or a class of individuals, alleging that their personal information was exposed, though perhaps not yet misappropriated. The question is: has such a plaintiff suffered "an injury in fact" sufficient to procure Article III standing?

[13] *See In re Equifax Inc. Sec. Litig.*, No. 17-CV-3463-TWT, 2019 WL 337807 (N.D. Ga. Jan. 28, 2019)

Prior to the increase in cybersecurity related claims, federal courts agreed that Article III standing could be achieved based on a claim for future harm: in environmental claims, (Cent. Delta Water Agency v. United States, 306 F.3d 938 (9th Cir. 2002)); exposure to toxic substances, (Pritikin v. Dept. of Energy, 254 F.3d 791 (9th Cir. 2001)); medical monitoring, (Sutton v. St. Jude Med. S.C. Inc., 419 F.3d 568 (6th Cir. 2005); and identify theft, (Pisciotta v. Old National Bancorp, 499 F.3d 629 (7th Cir. 2007)). In revisiting Article III standing in cyber cases, the federal courts, by and large, have decided that risk of future harm will confer standing.

In Krottner, supra, the 9th Circuit decided that Starbucks' employees, whose unsecured personal information was taken when a laptop containing the data was stolen, had met the injury in fact requirement, even though there was no evidence the data had been misused or used for identify theft. The Court reasoned that plaintiffs' allegations, which included enrolling in credit monitoring services, frequently checking banking and 401(k) accounts for theft, and related stress and anxiety, had alleged "a credible threat of real and immediate harm stemming from the theft of a laptop containing their encrypted personal data." Krottner, supra, at 1143. The Court went on to reason that the allegations were not based on the risk that their data would be stolen in the future, it had been stolen, and thus the harm was "real and immediate, not conjectural or hypothetical." Id.; see also In re Sony Gamin Networks and Customer Data Security Breach, 996 F.Supp.2d 942 (S.D. Cal. 2014) (relying on Krottner to find standing where plaintiffs could not show personal information exposed through data breach had actually been obtained by a third party); Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693 (7th Cir. 2015) (holding that plaintiffs "should not have to wait until hackers commit identity theft" before gaining standing).

Standing to bring state law claims turns on the statutory and common law in each state. Different state statutes confer standing in different ways, and standing for common law negligence, negligent misrepresentation and professional liability claims will vary from state to state. To a large extent, however, state court standing is premised upon the same inquiry as in federal court: has, or will, the plaintiff sustain a direct injury, and is the injury redressible? We are still waiting on a reported decision concerning accountant liability to a breach victim, at either the federal or state level, arising from a client data breach. However, assuming the plaintiffs can secure standing, the outcome of the case will hinge on whether any duty was owed to the plaintiff, and/or the extent of the duty owed to the plaintiff.

B. Scope of the Duty

Firms owe duties of confidentiality under IRS regulations, AICPA Ethical Rules, as well as myriad state laws governing tax payer information. Claims from firm clients arising from firm data breaches are more common than third party claims, but few get litigated. In those cases, standing is not in question, and the scope of the duty owed is relatively straight forward. However, the potential damages and costs that arise from a firm a data breach can be significant in terms of liability exposure, and the value of time lost resolving the breach event. Thus, firms need to be especially vigilant in developing its cyber protocols, use of encryption software, and strict email policies in order to avoid their own cyber breach events. Not only is it good policy to have clear cyber protocols in place to protect against cyber crimes, but a clear, written policy will help define the scope of the duty owed, and whether adherence to the policy could have reasonably prevented the data breach.

Firms engaged to conduct security audits, ICFR attestations, or even prepare Form 10-K financial statements, may find themselves in federal or state court defending investor claims, derivative claims, and/or indemnity claims arising from a client's data breach, where the breach victim's damages include

"risk of future harm." And though it is less likely at this time, in light of the increasing number of data breach cases, and the expanding scope of their impact and related public scrutiny, it is a matter of time before a firm's exposure extends to the data breach victim directly. In such cases, the duty likely arises from allegations that the victim was a third party beneficiary to the firm's security engagement, and/or where a plaintiff can establish that its harm was a foreseeable consequence of a firm's negligence. In any case, in light of the recent Yahoo! data breach settlement of $35 million, significant damages may arise from these kinds of claims, despite the seeming lack of provable damages.

III. Cyber Insurance

Though cyber insurance for professional firms is nothing new, in the evolving cyber landscape it is critical for firms to have an understanding of the type of coverage available, its limits, and how carriers determine when coverage is triggered in the event of a data breach.

As a starting point, coverage generally falls into two categories: first party coverage and third party coverage. First party coverage generally covers firm data breaches and the associated costs of dealing with a data breach, such as costs associated with breach notification and asset protection.[14] Limits are usually up to $100,000 in the aggregate, and contained within endorsements.[15] Third party coverage typically arises from damage as a result of a firm's work for a client, (e.g. damaging client information, exposing client's data, negligence, defense costs, etc.)[16] Firms must ensure that their first and third party coverage limits are adequate, reflecting the types of work and engagements they undertake, and their associated risks.

In addition to ensuring the proper level of coverage, it is critical that firms ensure compliance with internal cyber protocols, or risk a denial of coverage. Further, depending on the nature of claim, coverage may be limited to the "publication" of compromised data, such that coverage may not apply to firms that are hacked, i.e. the firm has not made personal information "public" and/or where there is no evidence that private information has been misappropriated.[17] This is a developing area of law, and coverage will depend on the specific policy language, state law regarding interpretation of insurance policy language, and the facts and circumstances involved. However, firms should work with their broker and/or legal counsel to ensure that they have adequate protection reflective of the work, and related risks, the firm engages in.

IV. Educational Resources

Fortunately, together with the rise of cyber crimes, data breach risks, and complex cybersecurity related engagements, there has also been a significant increase in educational resources to help guide professional firms as they enter this new frontier. The AICPA provides guidance on a myriad of cyber related issues that impact a CPAs practice.[18] For instance, the AICPA has developed guidance for firms

---

[14] *See* https://www.cpajournal.com/2017/03/20/cpas-need-know-cyber-insurance/

[15] *Id.*

[16] *Id.*

[17] *See e.g. Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 147 Conn. App. 450, 464, 83 A.3d 664 (2014) (holding that mere data loss does not trigger coverage under policy)

[18] https://www.aicpa.org/

engaged to audit a company's cybersecurity protocols. For these System of Organizational Control engagements, the AICPA has developed basic reporting requirements to include in an attestation or audit report. Additionally, the IRS, offers practice tips and guidance for safeguarding client information in Publication 4557. The SEC and FTC provide helpful guidance on their respective websites, as does the PCAOB.

The National Institute of Standards and Technology (NIST) has created a set of industry standards and best practices relative to data and information security.[19] NIST is generally applicable to all organizations, and provides guidance on how to improve cyber protections.

ISO 27001 and IEC 27002 are standards created by the Internal Organization for Standardization and the International Electrotechnical Commission to provide guidance for securing financial and other critical information. Finally, the Journal of Accountancy has numerous articles prepared by industry professionals that provide valuable information and practice tips.

[19] https://www.nist.gov/