



A CPA's introduction to

Cybersecurity

This tool was developed
by PCPS in conjunction with:



DISCLAIMER: The contents of this publication do not necessarily reflect the position or opinion of the American Institute of CPAs, its divisions, and its committees. This publication is designed to provide accurate and authoritative information on the subject covered. It is distributed with the understanding that the authors are not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

For more information about the procedure for requesting permission to make copies of any part of this work, please email copyright@aicpa.org with your request. Otherwise, requests should be written and mailed to the Permissions Department, AICPA, 220 Leigh Farm Road, Durham, NC 27707–8110.



Contents

2	Overview
---	----------

3	Why CPA firms are at risk
---	---------------------------

5	Risk to clients
---	-----------------

6	Cybersecurity policies and practices every CPA firm should have in place
---	--

8	Cybersecurity insurance considerations
---	--

9	Why CPA firms are in a good position to assist with cybersecurity
---	---

10	Approaching cybersecurity with clients
----	--

11	Conclusion
----	------------

12	Glossary
----	----------

Overview

In recent years, there's been no shortage of headlines about cybersecurity attacks against some of the world's largest organizations: Sony, eBay, Target, Anthem, Home Depot and JPMorgan Chase have all experienced massive security breaches. While the breaches of these large organizations have been very high profile and have received lots of press coverage, organizations of all sizes face the same types of threats and are experiencing similar breaches. While many organizations are still struggling to effectively address cybersecurity issues, they're no longer ignoring them.

Cybersecurity is the process of designing, implementing and operating controls to: (a) protect information and systems from security events that could compromise the achievement of the entity's objectives, and (b) to detect, respond to, mitigate and recover from, on a timely basis, security events that are not prevented. In other words, a company's cybersecurity program should identify and categorize potential security threats, implement controls designed to prevent the most significant threats whenever possible, and detect when security breaches occur so the organization can respond properly.

A CPA firm might wonder what cybersecurity has to do with them, particularly if the firm is a small- or medium-sized firm that mainly serves small- and medium-sized organizations. The answer may be found both in the cybersecurity risks that CPA firms face themselves, and in the potential business opportunities that this introduces for the firm to better serve its clients.

Why CPA firms are at risk

Most companies recognize that cybersecurity is a risk, and that the threat is growing. However, CPA firms may be at an even greater risk for cyberattacks — or compliance requirements — because of the nature of their work. Below are several reasons why a CPA firm should be aware of their cybersecurity position:

Single access point

Data in a variety of places

Compliance obligations

They offer a single access point

Attackers want to get the most out of their efforts, so they're looking for targets that will provide lots of potentially useful data. Why would attackers try to infiltrate a single company, when instead they could go after CPAs and other types of consulting firms and access a repository of sensitive information from a multitude of organizations? Hackers increasingly recognize that outside service providers such as CPA firms hold a wealth of valuable data and, in many cases, have lax cybersecurity protections in place.

Further, many small- and medium-sized businesses whose data would be in the firm's possession don't have the resources to develop strong cybersecurity defenses, leaving these businesses open to attackers who identified their targets from a CPA's database. These characteristics make CPA firms an alluring target for attackers.

Their clients' data lives in many places

Because CPAs serve numerous clients and often provide multiple services to those clients, the sensitive data to which they have access lives in many places, multiplying the number of potential weak spots that could allow for unauthorized access.

For example, associates at CPA firms likely have data stored on their laptops, on servers in the firm's network, on cloud-based storage sites such as Dropbox and in the email system. Sensitive data may also be stored on mobile devices or portable memory devices like a USB flash drive. The bottom line is that one piece of sensitive financial or personal data belonging to a client might live in half a dozen locations or more, making it difficult to ensure that it is afforded the right level of protection from being lost or stolen. There is an inherent trust and an expectation of protection when a client provides data to its CPA firm, and a loss or breach of that data would severely undermine the firm's credibility with that client, and likely with others, if word gets out.

They may have compliance obligations

Many CPA firms may not be aware that they likely are already subject to some cybersecurity compliance obligations. The three most common situations where a cybersecurity compliance obligation might occur is when firms handle the following types of data: personally identifiable information (PII), protected health information (PHI) and payment card industry (PCI) data.

Data subject to compliance obligations

Personally identifiable information (PII)

Any sensitive information that can distinguish one person from another — such as Social Security numbers — is considered PII and should be protected. A patchwork of 47 separate state laws establishes breach notification provisions when PII is suspected to be compromised. While there are variations among states, the basic premise is that any organization with information about a state resident (no matter where that organization is based) must protect data that can be characterized as PII. If at any point the company or organization has reason to believe that an unauthorized user accessed PII, the entity must acknowledge that breach directly to the affected individuals and through public notification.

Protected health information (PHI)

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that applies to a type of information called PHI. PHI is information that can be used to identify an individual and an associated malady or treatment. Many CPA firms may think that since they deal mainly with financial and business data, they fall outside the purview of HIPAA. But HIPAA's reach can be broad, especially when working with any clients in the health care space. For example, if a CPA firm provides services to a health care company that falls under HIPAA guidelines (known as a "covered entity"), that company may ask the firm to sign a business associate agreement, which is a document that specifies certain requirements for the storage, processing and handling of data that is in-scope for HIPAA. Signing such an agreement can designate the firm as a "business associate," which would require the firm to implement a HIPAA-compliant cybersecurity program. Because health care companies don't typically know for certain whether a third-party service provider (such as a CPA performing an audit) might access a health record, even by accident, these covered entities tend to require that a business associate agreement is executed by most vendors, including auditors, consultants and professional services firms. If a firm is classified as a business associate, that means the CPA firm must do things such as designate a HIPAA security official and conduct periodic risk assessments, even if its personnel never actually encounter protected health information at the client. It's likely that in the desire to secure business with a prospective client, more than a few CPA firms have unknowingly signed contracts and/or business associate agreements that include these provisions, and, because they're unaware that they're now in scope for HIPAA compliance, the firms don't have sufficient compliance programs in place.

Payment card industry data security standard (PCI DSS)

If a CPA firm accepts credit cards as a form of payment, the PCI DSS will likely apply. While PCI data security protocols are not part of any state or federal law, but rather enforced by the industry, there is a comprehensive set of cybersecurity measures that must be in place to ensure the proper handling of credit card information. These measures can be time-consuming and costly for a firm to implement.

Risk to clients

Business clients of CPA firms often face many of the same cybersecurity risks and compliance obligations outlined previously. Larger businesses will likely already have a baseline cybersecurity program in place.

For smaller companies that are trying to maximize revenue and limit overhead costs, a cybersecurity program can be difficult to justify. However, if a small- or medium-sized client suffers a cybersecurity breach, it may cause that client to go out of business. In other cases, some clients may be asked by their customers to sign a cybersecurity contract addendum to do business with them, which would then obligate the client to ensure that certain security measures have been implemented in their environment.

In these instances, and many others, there's an incentive for CPA firms to recommend to their clients implementing at least some basic cybersecurity elements if they don't already have an adequate program in place.



Cybersecurity policies and practices every CPA firm should have in place

Every CPA firm, whether it offers cybersecurity assistance to clients or not, should have a minimum level of security policies and associated practices that govern how employees interact with systems and sensitive data on the firm's behalf. Below is a list of several high-level policies and practices to consider:

Risk assessment

Conduct a cybersecurity risk assessment to determine the firm's susceptibility to IT vulnerabilities, identifying the most pressing areas to address. Management should make an educated decision on the cybersecurity risk assessment best suited for the firm.

Account for sensitive data

Identify the nature and type of data being stored by firm associates on your IT systems. Inventory what sensitive data you hold and ensure that it's being protected properly and when necessary, disposed of properly. Don't forget to include data stored on laptops, removable drives, mobile devices, cloud-based services with third parties and even hard copy printed records.

Require strong passwords

Make sure that all users on the firm's IT systems have been trained in proper password selection techniques, including frequently changing passwords. Also, ensure that laptops, servers and other devices have been hardened with security software and password protections.

Update software

Keep operating systems updated to the latest version, and install any security patches. Don't forget to apply patches to third-party software on firm computers, such as Adobe, Java and internet browsers, as those have been found to have numerous security vulnerabilities and therefore are frequent targets of attack. Also, ensure that security software, such as anti-virus, malware protection and desktop firewall software, is updated to stay ahead of the latest cybersecurity threats.

Audit security measures

Periodically assess the security measures around the firm's IT systems, ensuring that they still fall within the guidelines of a baseline program established by the firm. Include the results of this assessment in the risk assessment described previously, as the results of the security audit may impact the firm's risk posture.

Monitor problems

Implement a security monitoring system to become aware of any potential issues and to respond promptly. Security monitoring should include intrusion detection capabilities as well as security log review of logs from servers, databases, key software applications and firewalls. Security monitoring and alerting should be automated as much as possible, and review of the alerts should be conducted in near-real time. Many firms choose to outsource security monitoring to third-party organizations that specialize in this service.

Hold outside parties accountable

Develop a list of outside parties providing support to the CPA firm that could potentially have an impact on cybersecurity. Hold those companies accountable for undertaking basic cybersecurity measures both via contract requirements and by obtaining an annual independent validation of their compliance (such as a SOC 2® report).

Train employees on an ongoing basis

Users are a very common target for cyberattacks, so ensure firm employees are regularly trained in IT security policies, both when they're hired and on an ongoing basis. In addition, educate employees about the dangers of fake emails (phishing) that hackers use to gain access to a system. One user's mistake can lead to a significant security breach.

Develop an incident response plan

An incident response plan is designed to minimize the impact of a security incident, restore the affected environment to full working order, and communicate with affected parties as necessary. Be sure to create an incident communication plan for your firm, so that the firm can communicate quickly and clearly with necessary parties if a security breach occurs, whether it's in the form of public relations or internal communication with employees. And practice your plan before you must execute it in the heat of battle, so employees will be aware of their responsibilities and so you can ensure the plan covers the bases.

Limit the number of administrators

The more employees who have administrator access, the more the possibility of a cybersecurity breach grows. Limit the number of people with IT administration privileges to as few as possible, and ensure that administrators have a separate, non-privileged user account for daily functions such as email, so that compromised credentials won't be given to an attacker.

Develop and test a continuity plan

Unexpected disasters and unplanned outages can hit at any time, and firms will need current and accurate backups of key computer systems, as well as a continuity plan, to ensure the firm can serve its clients when the unexpected occurs.

Cybersecurity insurance considerations

The increased risks around cybersecurity have sparked many new questions about the role of insurance in helping to manage a firm's security risks. Many firms are adding a cybersecurity insurance policy to insulate the firm's finances against a major security breach. Below are some important considerations when evaluating the need for a cybersecurity insurance policy:

- Cybersecurity coverage is not typically included in most commercial policies. A separate policy or rider is likely required.
- Begin by putting a basic cybersecurity program in place — an effective program can reduce premiums.
- Clearly understand the scope of cyber coverage; brokers can help clarify.
- Firms should consider both first- and third-party coverage, to cover potential losses because of firm weaknesses or weaknesses of third-party vendors.
- Be responsible: A cyber policy can be an important part of a firm's cybersecurity program, but it shouldn't replace cybersecurity policies and controls.

The [National Association of Insurance Commissioners \(NAIC\)](#) outlines some of the types of cybersecurity coverage being offered:

- Liability for security or privacy breaches (first- and third-party coverage)
 - Costs associated with breaches, such as customer notification and support (first and third)
 - Replacement costs for restoring, updating or replacing business assets stored electronically (first)
 - Costs associated with business interruption (first)
 - Liability associated with copyright infringement or product disparagement as the result of a breach (first)
 - Expenses paid for ransomware or cyber extortion (first)
 - Expenses related to regulatory compliance failures (first)
-



Why CPA firms are in a good position to assist with cybersecurity

While it's true that there are companies devoted to cybersecurity, there are six compelling reasons why it makes sense for CPA firms to provide cybersecurity capabilities:

-
1. Are risk specialists
 2. Understand business
 3. Handle sensitive information
 4. Design, implement and assess controls
 5. Are often in company leadership positions
 6. Are trusted to report on effective controls
-

1. CPAs are specialists in risk

CPA firms understand business and financial risk. Cybersecurity is simply another type of risk that a business must manage, and CPAs should be able to put cybersecurity risks in perspective against other business risks that their clients may be facing.

2. CPAs understand business

Accounting is the language of business. CPAs understand the environment in which businesses operate, and can use their knowledge of the client's industry and local market influences to help offer perspective about how cybersecurity considerations fit with other business risks.

3. CPAs realize the importance of securing the information of their clients

CPA firms are regularly handling and processing sensitive information for their clients, such as tax returns, audit records and Social Security numbers. Requesting, obtaining and interacting with clients' sensitive data provides a natural opportunity for the CPA to observe existing

controls related to data security, remind the client of the importance of labeling and protecting sensitive information, and to suggest and/or evaluate appropriate cybersecurity controls over such data.

4. CPAs design, implement and assess controls

Often, accounting firms help design, establish and evaluate internal business controls to help clients manage their operations. To insulate them against cybersecurity risks, businesses need to implement cybersecurity controls, which are simply another aspect of a client's internal control functions.

5. CPAs are often in company leadership positions

Sometimes CPAs move into company leadership positions such as CEO and CFO. When that happens, they're in a strategic position in which they must make decisions about how to direct company resources toward things like cybersecurity. Having a CPA firm that offers cybersecurity capabilities can provide the C-level CPA with a firm that can speak the right language to assist in emphasizing the investment in strong cybersecurity resources.

6. CPAs are trusted to report on effective controls.

CPAs are the trusted business advisers to organizations of all sizes, advising clients on an array of risks. With clients facing an increase in cybersecurity risks, CPAs can help them identify and understand some of the risks they face.

Approaching cybersecurity with clients

CPA firms with limited cybersecurity experience may not want to pursue cybersecurity as a practice, but they can:

Start client conversations — Regardless of you or your firm's level of cybersecurity knowledge, it's still important to broach the topic. With businesses of all sizes facing an increase in cybersecurity risks, you can help clients identify and understand those risks. Ask about what kinds of protections they have in place, staff training programs, privacy and security policies, response plans and other controls that help mitigate risks and/or manage the aftermath of security incidents. Connect clients to experts who can help them put together an effective cybersecurity risk management program. Even if you cannot solve cybersecurity challenges outright, by demonstrating concern for their business's well-being, you'll strengthen client relationships.

CPA firms with knowledge and experience in cybersecurity can:

Help clients navigate threats — Firms that specialize in information technology may be well-equipped to step in and provide advisory services that help companies spot cybersecurity weaknesses, identify potential risks and offer advice on how to safeguard information and systems. CPA firms providing these services may find the AICPA's new [cybersecurity risk management reporting framework](#) helpful. For example, the description criteria developed as part of the framework presents a common language — or criteria — for organizations to develop and describe their cybersecurity risk management programs and practitioners to evaluate the descriptions. In addition, the trust service criteria can be used to evaluate a client's cyber controls and make recommendations for improvement, including appropriate policies and processes, as part of a readiness service. CPAs and CPA firms with the appropriate cybersecurity knowledge may also provide additional support for clients wishing to commission a report on the effectiveness of their organization's cybersecurity risk management program.

Conclusion

Cybersecurity is a growing concern for businesses of all types, and CPA firms should be considering the impact of cybersecurity on their own operations as well as their clients'. Firms that invest the time and effort to plan and prepare will be well-positioned to defend against cyberattacks. Firms may also find themselves in a position to assist their clients in assessing their cybersecurity needs. This provides firms with an opportunity to strengthen their client relationships by showing their concern for the client's overall success and well-being.



Glossary

The following is a list of cybersecurity terms that may arise for CPA firms in conversations around cybersecurity.

Data breach — A data breach occurs any time sensitive or personal data has been accessed by a person who has not been authorized to do so, including internal employees accessing data inappropriately. Note that this is much broader than simply saying a hacker broke in and accessed data. Breaches often include obtaining private information such as Social Security numbers, financial information, health records, credit card numbers, trade secrets, intellectual property or other protected data.

Malware — Short for “malicious software,” this is a blanket term used to describe any type of software designed to inflict damage on an IT system or facilitate a data breach. Malware includes computer viruses, ransomware and spyware, for example.

Payment Card Industry Data Security Standards (PCI DSS) — A set of industry IT security standards surrounding the handling, storage and transmission of credit card data. The PCI DSS were created by the major credit card brands and are not law, but are enforced via a process established by the card brands and the PCI Security Standards Council.

Penetration test — A set of activities performed on an IT system, network or website to identify and attempt to exploit vulnerabilities on the target environment. A penetration test is not necessarily designed to identify ALL potential weaknesses in the environment, but rather to provide an indication of the ease with which a target can be compromised and the likelihood that a malicious attacker could accomplish a similar compromise. A penetration test differs from a vulnerability assessment in that the objective of a penetration test is typically to obtain unauthorized access to the target environment or to obtain sensitive data from the environment. Penetration tests can be very invasive and can cause system instability, and therefore should be performed only by individuals experienced in penetration testing tools and techniques. While automated tools are available that can assist a penetration tester in identifying potential exploit vectors, most penetration tests involve both automated and manual techniques.

Personally identifiable information (PII) — Any information that could be used either on its own or with other information to identify a specific individual, such as Social Security numbers or tax return data. Forty-seven U.S. states have breach notification laws in place to protect residents from unauthorized disclosure of such information.

Phishing — A form of computer fraud in which the attacker tries to trick users into disclosing sensitive information such as login credentials or account information by masquerading as a reputable entity or person via email or via other communication channels.

Protected health information (PHI) — Any information that relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual that can be used to identify the individual. Such information is protected under the Health Information Portability and Accountability Act (HIPAA).

Ransomware — A type of malware that denies access to an IT system until the system operators pay a sum of money or agree to other demands.

Risk assessment — A process of cataloging the types of cybersecurity risks an organization faces and determining risk exposure to facilitate decision-making regarding how to appropriately respond to real and perceived threats to protect systems and data deemed most critical.

SOC for Cybersecurity — A new System and Organization Controls (SOC) for Cybersecurity engagement developed by the AICPA includes a cybersecurity risk management reporting framework that assists organizations as they communicate relevant and useful information about the effectiveness of their cybersecurity risk management programs. Through the SOC for Cybersecurity engagement, a CPA reports on an organizations' enterprise-wide cybersecurity risk management program. This information can help senior management, boards of directors, analysts, investors and business partners gain a better understanding of organizations' efforts.

Threat — Any circumstance, adversarial force or phenomenon that could affect the confidentiality, integrity or availability of an information system and/or its networks, including the facility that houses the hardware and software.

Vulnerability — An inherent weakness in an information system that a threat or threat agent can exploit, resulting in an undesirable impact on the protection of the confidentiality, integrity or availability of the computer system.

Vulnerability assessment — A set of activities performed on an IT system, network or website to identify the security vulnerabilities that are present in the target environment. A vulnerability assessment is intended to identify and assign a priority rating to potential security weaknesses in the environment, but not to exploit the weaknesses. Therefore, a vulnerability assessment provides the organization with a perspective on the technical security posture of the organization's IT systems, but does not provide any validation of the likelihood that the organization could be successfully compromised via one of the identified vulnerabilities. A vulnerability assessment is typically conducted using an automated scanning tool, and can be performed with or without authentication credentials. Vulnerability scans that are performed with authentication credentials typically provide much more accurate information about the environment under evaluation.



800.CPA.Firm (800.272.3476) | PCPS@aicpa.org | aicpa.org/PCPS

© 2018 Association of International Certified Professional Accountants. All rights reserved. AICPA and American Institute of CPAs are trademarks of the American Institute of Certified Public Accountants and are registered in the United States, the European Union and other countries. The Globe Design is a trademark owned by the Association of International Certified Professional Accountants and licensed to the AICPA. 1804-3327

This tool was developed
by PCPS in conjunction with:

