Essential Cybersecurity Awareness in Accounting – What You Need to Know

(CYBA2)

KAPLAN

Essential Cybersecurity Awareness in Accounting—What You Need to Know

(CYBA2)

Victorianne Musonza, JD, CISSP, CISA, CIPM, CIPP/E/US

KAPLAN®

ESSENTIAL CYBERSECURITY AWARENESS IN ACCOUNTING—WHAT YOU NEED TO KNOW (CYBA2)

Published in 2021 by Kaplan, Inc.

Printed in the United States of America.

ISBN: 978-1-0788-1448-5

TABLE OF CONTENTS

Unit 1

Cybersecurity Awareness and Data Safeguarding

LEARNING OBJECTIVES

When you have completed this unit, you will be able to accomplish the following.

- ☐ Explain the cybersecurity threat landscape and its economic costs.
- ☐ Identify evolving state regulatory and legal rules related to cybersecurity.
- ☐ Apply the core principles of cybersecurity awareness to limit cybersecurity risk.

INTRODUCTION

Organizations have an increasing need to demonstrate that they evaluate security threats, mitigate their vulnerabilities, and measure and manage security risk. CPAs are often on the forefront of an organization's security program by either controlling the budget and/or running the security program implementation and/or testing.

Accounting professionals and the IT departments that support them do not operate in a vacuum. Objectives and corporate ethics heavily influence business strategy. External factors, such as legal considerations, regulations, and partnerships, create additional concerns. Innovation in new technologies, coupled with untested methods, creates a prescription for a security breach.

Security professionals should not make the sole determination on the required protections for enterprise information assets. Security professionals should consult with the asset stakeholders to gain their input on the sensitivity level that should be assigned to an information asset. Keep in mind, however, that all stakeholders should be consulted. For example, while management should be consulted and have the most significant influence on the decisions about departmental assets, other stakeholders within the department and organization should be consulted as well. This makes accounting professionals key players in the protection of the information assets they work with on a daily basis.

With this in mind, this unit was developed to:

- Introduce accounting professionals to the cybersecurity landscape and the threats that exist;
- Examine selected sample cybersecurity state regulations and rules; and
- Discuss the proper application of regulations, rules, and principles.

CYBERSECURITY THREAT LANDSCAPE

DISCUSSION QUESTION

Do you use a password vault at home or at work? If so, which product do you use?

The cybersecurity landscape appears to become more dangerous with each new disclosure of a significant organization suffering a breach. The most alarming aspects of many of these breaches are the following:

- The organizations involved were large enough and had access to resources and budgets to fund cybersecurity programs. In other words, there seemed to be no reasonable excuse!
- Organizations seem to be applying more resources to managing the public relations response to a breach than assisting those they have harmed—their users, customers, vendors, and business partners.
- There are unacceptable delays in announcing these breaches, in some cases keeping the information secret for months.

It is questionable if these data breaches serve as a warning for organizations that are not diligent in monitoring security threats. The most extensive data breaches occurred during the last 10 years, most notably Target, Equifax, and Marriott. These breaches affected hundreds of millions of individuals globally.

It is time for all organizations to wake up and smell the ransomware. Organizations need to better understand who these attackers are, what they want, and how they go about getting it. Employees and stakeholders should be adequately educated and made aware of the security risks their organization faces. Frequently, the employees and third parties such as vendors are a source of an attack or potential data exfiltration. When users do stupid things (and this behavior runs up to the CEO office), all the fancy IPS, IDS, and firewall systems mean NOTHING.

In January of 2020, Microsoft disclosed that they had a database that was improperly configured, which enabled exposure to the data to unauthorized parties (see https://www.securitymagazine.com/articles/94076-the-top-10-data-breaches-of-2020#:~:text=There%20were%202%2C935%20publicly%20reported,that%20took%20place%20this%20year).

In 2019, Facebook's VP of engineering reported that since 2012, it had not adequately secured the passwords of over 600 million users (Steve Turner, Facebook Makes Disturbing Announcement Regarding User Password Privacy, https://www.identityforce.com/blog/facebook-user-password-privacy, March 21, 2019).

In this unit, we are going to take a look at who these threat actors are, what their goals and motivations are, and what means they use to achieve these goals.

Top Data Breaches of 2020

Company	Information	Cause
Microsoft	Customer support database (250 Million)	Misconfiguration internal security control
Wattpad	Customer PII (268 Million)	Hacking
Broadvoice	Customer Information (250 million)	Vendor
Estee Lauder	Education Database (440 Million)	Weak internal controls
Sina Weibo	Social Media (PII) but not sensitive (538 Million)	Hacking
Whisper	Customer Information (900 million)	Weak Internal Controls
BlueKai (Oracle)	Customer Information (Billions)	Weak Internal Controls
Keepnet Labs	Customer Information (Billions)	Vendor managed database
Advanced Info Service	DNS query logs and NetFlow logs (Billions)	Weak Internal Controls
CAM4	Customer PII (Billions)	Weak Internal Controls

Recent Breaches

Budgeting the cost of technologies and the staff necessary to maintain the security and privacy of the organization's information systems and data can be costly. Nonetheless, the cost to budget these items is far less than the operational, reputational, regulatory, and financial harm that results from data breaches. Unfortunately, companies often invest more in public relations than repairing the harm caused to their customers, vendors, and other business partners.

Who Are They?

Hackers hack for many different reasons. When you really get down to it, they want one of four things:

- Financial gain
- Disruption
- Geopolitical change
- Notoriety

A threat is anything that can cause damage to company assets in a manner that can result in harm (see ISO/IEC 13335). A vulnerability is a weakness in a system or thing. A risk is the probability of an event and the impact that will result, if the harm materializes. For example, a threat is carried out by a threat actor. An attacker who takes advantage of

an inappropriate or absent access control list (ACL) is a threat agent. ACLs are used to limit access to a network and act basically as a network filter. Keep in mind, though, that threat actors can discover and exploit vulnerabilities. Not all threat actors will actually exploit an identified vulnerability.

The Federal Bureau of Investigation (FBI) has identified three categories of threat actors:

1. Organized crime groups primarily threatening the financial services sector and expanding the scope of their attacks

2. State sponsors, usually foreign governments, interested in stealing data, including intellectual property and research and development data from major manufacturers, government agencies, and defense contractors

3. Terrorist groups wanting to impact countries by using the internet and other networks to disrupt or harm society's viability by damaging its critical infrastructure

While there are other less organized groups out there, law enforcement considers these three groups to be the primary threat actors. However, organizations should not disregard the threats of any threat actors that fall outside these three categories. Lone actors or smaller groups that use hacking to discover and exploit any discovered vulnerability can cause damage, just like the larger, more organized groups.

But that only includes the severe bad guys. What about these guys:

- **Hacktivists**. This includes those who hack not for personal gain but to further a cause—for example, the anonymous group that hacks from time to time for various political reasons.

- **Thrill hackers.** These guys do it for the notoriety. They deface websites and brag about their conquests to their fellow thrill hackers on websites where they share tools and methods.

Standard terms also used are white hat, gray hat, and black hat. A white hat does not have any malicious intent. A black hat has malicious intent. A gray hat is considered somewhere in the middle of the two. A gray hat will break into a system, notify the security hole administrator, and offer to fix the security issues for a fee.

Some threat agents are nonhuman. Threats can be grouped into the following five categories:

- **Operational.** Includes any process or procedure that can affect the CIA.

- **Human.** Includes both malicious and non-malicious insiders and outsiders, terrorists, corporate espionage, and terminated personnel.

- **Physical.** Includes wireless camera issues, perimeter measures failure, and biometric breakdowns.

- **Natural.** Includes tornadoes, earthquakes, floods, fires, hurricanes, or other natural disasters or weather events.

- **Technical.** Includes software and hardware failure, malware, and disruptive technologies.

Examples of the threat actors include both internal and external actors and include the following:

- Internal actors
  - Government spy
  - Vendor/sub-vendors (vendors of vendors)
  - Thief
  - Disgruntled employee
  - Reckless employee
  - Untrained employee
  - Partner
  - Internal spy
- External actors
  - Legal adversary
  - Mobster
  - Anarchist
  - Competitor
  - Corrupt government official
  - Irrational individual
  - Activist
  - Terrorist
  - Vandal
  - Data miner
  - Government cyber warrior

Defining Risk

Risk is the probability of an event and the consequence that results from that event (see https://www.isaca.org/resources/glossary#glossr).

Risks are comprised of two components: vulnerabilities and threats.

	Vulnerability	Threat	Risk
Definition	Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.	Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.	The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

Types of Risk

- Operational
- Market (competitive)
- Compliance
- Reputational
- Financial

What Do They Want?

The intent of the malicious individual depends on their motivation. In some cases (thrill hackers), the goal is simply to show proof of hacking something. An attack on a website (such as website defacement) can do significant damage to an organization's reputation, even if it does not result in unauthorized access to the organization's assets, including personal and proprietary information. If a bank cannot safeguard its website, it puts its customers' personal data at risk (Capital One Breach Affects 100 Million Households 2019, see https://www.securitymagazine.com/articles/90622-capital-one-announces-data-breach-affecting-100-million-customers).

In most cases, the end game is money, either gained from selling pilfered data or leveraging the data to steal from individuals (identity theft, credit card fraud, etc.). Information types that are typically used in this way are as follows:

- **Credit card data.** This is the most easily monetized data that can be obtained. When you combine the theft of these numbers with the delay in reporting of breaches

that have become commonplace, in many cases, users have charges in their cards before the breach has even been reported.

- **Personally identifiable information (PII).** Personally identifiable information (PII) is any piece of data that can be used alone or with other information to identify a single person. PII includes full name, identification numbers (including driver's license number and Social Security numbers), date of birth, place of birth, biometric data, financial account numbers (both bank account and credit card numbers), and digital identities (including social media names and tags). Any PII that an organization collects should be protected with the appropriate security measures.

EXAMPLE

A CPA firm's tax department will have personally identifiable information on the taxpayer and all members of the taxpayer's family. That PII will generally include the following:

- Full names
- Social security numbers
- Dates of birth
- Drivers' licenses (required by an increasing number of states for electronic filing)
- Financial account numbers

That data will exist in the tax return processing system's data files (such as the tax return files for ProSystemFX, Lacerte, etc.), the firm's paperless work paper system, and increasingly, in the firm's portal offered to clients.

EXAMPLE

A CPA firm handling attests or accounting work for clients may end up accumulating personally identifiable information of various individuals associated with the client. That data can include detailed PII from a client's payroll systems, accounts payable system, accounts receivable system, tax records, etc. that the CPA may accumulate as part of the attest or accounting engagement. Such documents may exist at various times on both the firm's servers and on laptops used by staff onsite for the engagement.

In a 2006 incident, the auditors for Hotels.com lost a laptop that contained personal information on 243,000 customers of that business.[1]

- **Trade secrets.** A trade secret gives an organization a competitive edge. A trade secret ensures that proprietary technical or business information remains confidential. Trade secrets include formulas, schematic drawings, recipes, and so on that must be protected against disclosure. Once the trade secret is obtained by or disclosed to a competitor or the general public, it is no longer considered a trade secret.

  Most organizations that have trade secrets will attempt to protect these secrets using nondisclosure agreements (NDAs). These NDAs must be signed by an entity that has

[1] "Hotels.com Customer Data Stolen," *PC World,* June 2, 2006, https://www.pcworld.com/article/125962/article.html

access to information that is part of the trade secret. Anyone who signs an NDA will suffer legal consequences should the organization prove that the signer violated it.

- **Personal financial information.** This includes records kept by banks, insurance companies, and brokerage houses.

  Unfortunately, data that can be sold is not the only type of data loss that can get an organization in hot water. While not as easily monetized, when these data types are released in a breach, the organization becomes liable to those whose data they have compromised and, depending upon the circumstances of the breach, to regulators and/or governmental entities.

EXAMPLE

As part of the examination of XYZ Credit Union, CPA firm Abacus and Processor obtains information on the test set of transactions from XYZ's systems. This information contains personal financial information about the customers whose transactions are part of that test set.

EXAMPLE

PST Widgets, Inc. has payroll and benefit information in the payroll databases that are part of its accounting systems. This information represents personal financial information that may be of interest to certain unauthorized parties.

EXAMPLE

Income, Expenses and Credits, CPAs has a number of tax clients for which it obtains information on the activity in the client's brokerage accounts. The firm receives this information after the client authorized the financial institutions to provide that information. That information represents personal financial information.

- **Personal health information (PHI).** This includes medical records for an individual. While not easily monetized, PHI can be held for ransom, which happened to hospitals in Kentucky and California in 2016. Those hospitals, luckily, were able to recover without paying the ransom. Hollywood Presbyterian Medical Center in Los Angeles was not so lucky. In that case, it paid $17,000 to get access to files back. In January 2018, Hancock Health Paid $55,000 in Bitcoin after being attacked through ransomware.

How Do They Do It?

What types of tricks and attacks do hackers use to compromise systems to get to the data? Let's look at some of the most common methods.

Open Web Application Security Project® (OWASP) is a nonprofit organization formed in 2001 and comprised of global security professionals. Through open-source projects, they provide education, training, and conferences. In 2003, the organization's members developed the OWASP Top 10 to raise awareness about the top vulnerabilities facing application security (see https://owasp.org/www-project-top-ten/).

Risk	Description
Injection	Untrusted data is sent to a command or a query.
Authentication	Authentication is improperly configured, and attackers can compromise passwords, keys, and session tokens and assume users' identities.
Data exposure/leakage	APIs (middleware) that do not protect sensitive data—think QuickBooks add-in in Excel
XML	Old or misconfigured xml documents can be manipulated to disclose internal files.
Access controls	Improper access controls can result in the wrong or unauthorized party accessing data and systems that they should not.
Misconfigurations	Failing to change default setting or improperly configuring settings
Insecure deserialization	Reversing data format in unsecure away—found to allow denial-of-service, access control, and remote execution (RCE) attacks
XSS	Application includes untrusted data in a new page
Known vulnerabilities	Issues with privileges and failing to patch/update applications
Insufficient logging and monitoring	Failing to properly monitor, log, and detect threats

Social Engineering Threats

Social engineering attacks occur when attackers use believable language and user gullibility to obtain user credentials or some other confidential information. Social engineering threats that you should understand include phishing/pharming, shoulder surfing, identity theft, and dumpster diving.

The best countermeasure against social engineering threats is user security awareness training. This training should be required and must occur on a regular basis because social engineering techniques evolve constantly.

The following are the most common social engineering threats:

- **Phishing.** This type of attack is usually carried out by creating a fake website that very closely resembles a legitimate website. Users enter credentials on the fake website, allowing attackers to capture the credentials. Phishing is considered a social engineering attack because attackers use an illusion of trust to learn personal information, including credit card information and financial data. Spear phishing is a phishing attack carried out against a specific target by learning about the target's habits and routines. Because of the information that must be gathered, spear phishing attacks take longer to carry out than phishing attacks.

EXAMPLE

James receives an email that claims to be from the firm's portal provider. The email indicates that due to suspicious activity on his account, the provider is going to require him to log in and provide information to verify his identity and that until he does so the provider will shut down access to the site for the firm's clients (arguably to protect them from the security problem). The email provides a link that it tells James to click to initiate the process. While the email shows the link as going to http://www.cpaportal.com/security, the actual HTML code in the email directs James to a different site (http://www.cpaporta1.com/security).

Note that address is subtly different (the letter "l" in portal is replaced with the number 1). When James clicks on this email, he is presented with a page that appears identical to that of the portal. The site asks James to enter his user ID, password, Social Security number, IRS e-Services username and password, and EFIN and CAF numbers, claiming it needs those identifiers to verify James' identity after which the site will be reopened to his clients. When James provides that information, the perpetrator is able to access all client information stored on the portal as well as take control of James' e-Services account with the IRS.

- **Pharming.** Pharming is like phishing, but pharming pollutes the contents of a computer's Domain Name System (DNS) cache so that requests to a legitimate site are routed to an alternate site. DNS is the system used to translate the text we type as addresses on the internet into the numeric address actually needed to route your information to the proper location on the internet.

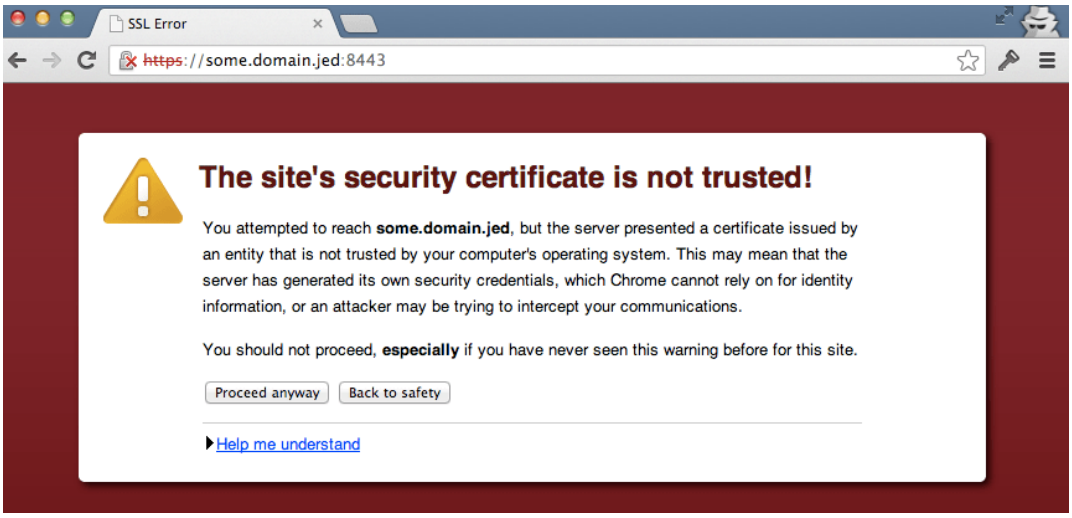
  It may be useful to think of DNS as being like the contacts application on your phone. You can dial your son, Harry, by just telling the phone to call Harry. What the phone does is look up Harry in your contacts list and then send the carrier the actual number that must be dialed to reach Harry. Pharming would be like swapping the numbers in your contacts application so that instead of using Harry's number, the phone would now find a number for someone else.

  There are various ways to swap the DNS records, but one obvious way is to get the user to use a compromised DNS server that may have been placed on a public Wi-Fi system. Another way to manage this modification would be to write a redirected entry into the "hosts" file on the user's computer. Your hosts are first consulted by most operating systems to determine the address to use for a request, so an entry in hosts would normally override the normal system of asking an outside DNS server to provide the address.

  The pharmed or bogus website will not be able to provide a valid SSL/TLS (Secure Sockets Layer/Transport Layer Security) certificate for an encrypted connection. Generally, an SSL/TLS Certificate is a digital certificate issued by a Certificate Authority, ("CA") for a website. Some commonly known CA's are Symantec, Let's Encrypt, and DigiCert. The digital certificate is based on a CA's validation of a domain's ownership and of the domain owner's organizational details. There are several levels of SSL/TLS certificates, with the most expensive option generally featuring a detailed validation level, the highest encryption standard, and some version of a warranty. There is also a self-signed (self-certification) version, which is allowed only under certain conditions (usually a private website with no anonymous visitors). Several encryption levels are available to SSL/TLS Certificate applicants.

The SSL/TLS Certificate, at any level, tells the world that the domain owner uses a form of encryption to secure communications to its website and the certificate itself incorporates an encryption key. SSL/TLS Certificates are critical for organizations that offer/accept any form of online payment.

Example of an SSL/TLS Certificate warning:
https://www.knucklepuckmedia.com/blog/preventing-a-symantec-ssl-warning/



Of course, if a user either "clicks through" a certificate warning or fails to notice that their connection no longer shows as secure (by using an http:// rather than https:// reference), the pharming ruse can still work, especially on less sophisticated users.

Users should be cautioned to check to be sure they are actually communicating via secured (https://) connections to sites where sensitive information will be transmitted.

- Some phishing schemes use https websites that appear to be legitimate. See the following:
  - https://wickedcpu.com/2017/12/06/phishing-schemes-are-using-https-encrypted-sites-to-seem-legit/
  - https://www.wired.com/story/phishing-schemes-use-encrypted-sites-to-seem-legit/

Caution users against using embedded links in email messages, even if a message appears to have come from a legitimate entity. Users should also review the address bar any time they access a site where their personal information is required to ensure that the site is correct and that TLS 1.2 (Transport Layer Security, which has essentially replaced the depreciated SSL. 1.3 is the most recent version)/SSL (extremely rare, but still possible) is being used, which is indicated by an HTTPS designation at the beginning of the URL address.

Note that the use of a "close or similar" domain name (see the portal vs. porta1 name in the earlier example) could allow the use of misdirection without necessarily triggering a complaint about an invalid security certificate.

EXAMPLE

Mary is finishing up work on a project in a local coffee house. Being somewhat security conscious, she has assured that her screen cannot be seen by anyone in the coffee house, both by sitting in a corner and by using a security screen. However, Mary is unaware that the system in the coffee house has been compromised with a rogue DNS server. The system is able to redirect Mary's browser to a site containing malicious code. A security warning appears on her computer stating that the certificate for her search engine is listed as ":/google.com and not google.com." Mary is a hurry and clicks through the warning and all her work files disappear five minutes later. Based on what we have just discussed:

1. What did Mary do correctly to avert a cybersecurity incident or breach?
2. What additional steps should she have taken to reduce her risk of being hacked?

Although Mary took adequate measures to protect her computing activities from physical security threats by selecting an isolated location in the coffee house, she let her guard down by ignoring the certificate warning and by using the coffeehouse's unsecured network without additional measures such as her employer's VPN (virtual private network).

- **Shoulder surfing.** This attack occurs when an attacker watches a user enter credentials or other confidential data. Encourage users to always be aware of who is observing their actions. Privacy screens help ensure that data entry cannot be recorded.

EXAMPLE

Mary has made sure she has complex passwords that are different for each account and is using a WWAN (Wireless Wide Area Network) card in her computer rather than public Wi-Fi to access sites when she is outside the office. But Mary doesn't notice that a third party is watching her as she enters that complex password and her username into her firm's portal's administration system as she eats lunch seated at a bench in a public park.

That third party, having captured Mary's username and password simply by watching her in a public place, is able to access all the data Mary can access in that system.

Based on this series of events:

1. What did Mary do correctly to avert a cybersecurity incident or breach?
2. What additional steps should she have taken to reduce her risk of being hacked?

Although Mary took adequate measures to protect her computing activities from logical security threats by selecting a complex and unique password, and by using a WWAN (Wireless Wide Area Network) card in her computer rather than public Wi-Fi, she let her guard down by ignoring physical threats. Mary could have used a screen protector or could have taken the physical security precautions she used in the previous example.

- **Identity theft.** When someone obtains personal information, including Social Security number, bank account number or driver's license number, and uses that

information to assume the identity of the individual whose information was stolen, identity theft has occurred. After a successful attack, the attacker can go in any direction. In most cases, attackers open financial accounts in the user's name. Attackers also can gain access to the user's valid accounts.

Stolen identities are also used for tax related frauds. Such frauds include using a stolen Social Security number to obtain employment or using the stolen credentials to prepare a fake tax return which then is filed early in tax filing season to obtain a fraudulent refund. Either of these fraudulent uses of confidential personal information may cause a number of issues for the person whose identity was stolen.

- **Dumpster diving.** Dumpster diving takes place when attackers examine garbage contents to obtain confidential information. This stolen information can include network diagrams, account login information, organizational charts, and financial data. Policies for shredding documents that contain this information should be implemented.

EXAMPLE

Neil's client sends him a revised printout of payroll information to be used in Neil's examination of the client's year-end financial statement. The client tells Neil to throw away the old documents that were sent. These payroll documents include salary amounts, Social Security numbers, and other personally identifiable information of the client's employees. Neil follows the client's instructions literally and simply tosses the old printout into the trash.

- Identity thieves, knowing that CPA firms receive many documents with confidential information, arrive in the evening and look through the trash dumpster outside the firm's office for any potentially useful information. They find the report and are able to sell the data contained in the report.

Malicious Software

Malicious software, also called malware, is any software that is designed to perform malicious acts. In many cases, this software is used to compromise a system to set up the data theft.

There are five classes of malware:

1. **Trojan horse.** Malware that disguises itself as a legitimate application while carrying out malicious actions.

EXAMPLE

Mary receives an email with the title "URGENT: IMMEDIATE UPDATE REQUIRED." Her email shows the message is from the software company that wrote the accounting package used in her organization. The email notes that a major security flaw has been discovered in their product that would allow unauthorized third parties access to all information in all of their accounting software packages and that the flaw is currently being actively exploited by parties that are now scanning the internet for vulnerable systems. The email adds that it is crucial that she apply the patch contained in the program that she will download from the link provided in the email immediately to avoid imminent unauthorized access to the organization's data. The link in the email shows up as "http://www.accountingvendor.com/updates" and Mary knows that "accountingvendor.com" is the domain used by the vendor that provides the software.

Mary, very concerned about stopping this threat to the organization as soon as possible, clicks the link and obtains the patch. When she runs the patch, the operating system asks her for permission to install and modify the software, to which Mary agrees. Mary now is sure she has saved the organization from an embarrassing security breach.

The email in question did not come from the vendor, as the "from" address was spoofed. According to the IT vendor Forcepoint (forcepoint.com/cyber-edu/spoofing), spoofing "is the act of disguising a communication from an unknown source as being from a known, trusted source" and "can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP) or Domain Name System (DNS) server." While the text on Mary's screen in her email program showed that the link went to her vendor's site, the actual HTML code in the email sent her browser to a wholly different site. The outsider tricked Mary into providing authorization for a program to be installed that, rather than patching the accounting system (which had no problems), installed malware into Mary's system and set up attacks on other computers inside the network that "trust" Mary's machine.

EXAMPLE

Wayne in ABC's accounts payable receives an email entitled "Overdue Invoice" to which is attached a Word document. The text of the email tells Wayne that the attached invoice has gone unpaid for over 120 days and the vendor (a major supplier to organizations like ABC) is threatening to take legal action against the organization. Wayne does not believe that any invoices should be unpaid from that vendor, so he opens up the Word document.

The document he opens up appears mainly as unreadable characters except for a box at the top that states "Open New Font necessary to read this document. Click here to obtain and install the font. If asked for permission to run the Word macro, please click yes." As Wayne needs to read the invoice to see what it is about, he clicks and then grants Word permission to run the macro. The system churns for about 30 seconds and then pops up an error message that the font could not be installed.

Wayne calls up the vendor to find out what is up. The vendor looks into ABC's account and finds that no outstanding invoices remain unpaid. The vendor's employee tells Wayne it must have been a system glitch and not to worry about it. Wayne mumbles about the incompetence of large bureaucratic organizations and then goes on about his work.

Six days later the users through ABC's network find they are unable to access most files on the server. As ABC begins to run down what the problem is, messages start popping up on machines throughout the organization that they have been infected with a ransomware program and a ransom of $30,000, payable in a specific cryptocurrency, must be paid or the key to decrypt their files will be destroyed.

What should Wayne have done to prevent the unfortunate series of events from occurring?

If Wayne's firm had implemented a phishing awareness training program, he would have known to question the email and to have contacted the vendor to confirm the email before opening the attachment. Training is critical to preventing phishing attacks.

---

2. **Virus.** Any malware that attaches itself to another application to replicate or distribute itself.

3. **Rootkit.** A set of tools that a hacker can use on a computer after he has managed to gain access and elevate his privileges to administrator. This is one of the hardest types of malware to remove, and in many cases only a reformat of the hard drive will completely remove it. Named after the root account, the most powerful account in UNIX-based operating systems (including Linux, iOS, MacOS and Android), these tools might include a backdoor for the hacker to access. But despite the UNIX-based reference used to name the tool, rootkits are an issue for a Windows-based system as well.

   The incident that brought rootkits to much more widespread attention was the attempt by Sony BMG to control music piracy in 2005 by installing a rootkit onto the computers of individuals who played various Sony music CDs on their computers. Sony's purpose was to detect attempts to burn copies of the CD and send data on the users back to Sony. The rootkit hid itself from any attempts to view the directory in Windows or by programs running under Windows, such as antivirus programs, rendering it very difficult to detect. As well, attempts to remove the rootkit would damage Windows, rendering the machine unbootable.[2]

   But far worse was the fact that the hidden directory could be used by other software (read malware) to have the Sony software hide their unauthorized operations as well. While a case study in how not to protect intellectual property and how to wildly mishandle a public relations issue, a Sony VP initially responded to the matter by saying in an NPR interview "Most people, I think, don't even know what a Rootkit is, so why should they care about it?"[3] But the key issue is to note that various mechanisms can be used to install such malware—including, in this case, something as apparently innocent as a user merely playing a legitimate audio CD on a computer on the network.

4. **Worm.** Any malware that replicates itself, meaning that it does not need another application or human interaction to propagate.

   Worms may be used as a secondary attack once the network firewall is breached. For instance, a worm may be installed on a machine by a Trojan program along with other malware. The worm then works inside the firewall to attack and install malware on other machines on the network.

   The "Eternal Blue" exploit was a worm that was used as part of the WannaCry ransomware attack. The exploit used a flaw in Microsoft's implementation of Server

---

[2] "Sony's DRM Rootkit: The Real Story," Schneier on Security, https://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html, November 11, 2005

[3] "Sony Music CDs Under Fire from Privacy Advocates," NPR Website, https://www.npr.org/templates/story/story.php?storyId=4989260, November 4, 2005

Messaging Block (SMB), the method used by Microsoft networks to handle networking. While organizations do not generally expose their network shares to the internet, once a single machine was infected via some other means, Eternal Blue allowed the ransomware to be installed rapidly on all machines in the network that had not been patched against the flaw. While Microsoft had released a patch in March 2017 that closed the exploit used by Eternal Blue, a large number of machines remained unpatched when the WannaCry ransomware attack began two months later.[4]

5. **Spyware.** Any malware that collects private user data, including browsing history or keyboard input.

   For organizations that CPAs work in, the ability of spyware to capture data and then send it to unauthorized third parties is a major exposure. In many cases, the spyware will be put in place first by a Trojan program that an attacker manages to trick one user to run, then by using a worm to place the spyware onto other machines inside the firewall due to their implied trust of first infected computer.

EXAMPLE

In the attack on Mary via the Trojan discussed earlier, spyware would be installed on Mary's machine that could report back Mary's keystrokes (via a keystroke logger) which would capture any data Mary entered into the machine. As well, the spyware could read any files that Mary can read, as well as report back items displayed on Mary's screen. But the ultimate goal is not merely to get the data Mary has direct access to since it's very likely she has only access to data needed to perform her job.

The malware package likely would include a worm that would use Mary's computer as a tool to attack other machines on the network, attempting to install malware on them more easily since it no longer has to evade the network firewall. As it moved to new computers with new permissions, the package would hope to eventually infect a party with high-level administrator access to sensitive data. As well, it very well may use rootkit technology to allow itself to hide from antivirus and antimalware tools.

The following are some of the actions a rootkit can take:

- Replacing default tools with compromised (Trojan) version
- Deleting all entries from the security log (log scrubbing)
- Installing a backdoor
- Inducing malicious kernel changes

Installing antivirus and antimalware software is the best defense against malicious software. Most vendors package these two types of software together. Keeping antivirus and antimalware software up to date is vital. Ensuring that the latest virus and malware definitions are installed is critical.

---

[4] "An NSA-derived ransomware worm is shutting down computers worldwide," ArsTechnica, https://arstechnica.com/information-technology/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/, May 12, 2017

NOTE

One clue your systems may be infected with malware may evidence itself as a "problem" with your security software no longer automatically obtaining its updates. Malware authors are in a "cat and mouse" game with software security vendors, developing exploits and testing them against security software to ensure they aren't detected. Security software vendors become aware of these exploits and write code to deal with the new threats.

Because the malware authors are aware that the security software organizations are likely to update their software to detect and remove their software, they will often attempt to find a way to stop the software on the system from ever obtaining the update. For an overly simple example (since most security software would anticipate this attack), the software could write an entry in the host's file on the infected computer for the security software company's servers to ensure the requests for updates are sent to servers other than those of the security company.

Rogue Endpoints

You also must concern yourself with the possibility of rogue devices in the networks. Rogue devices are devices that are present that you do not control or manage. In some cases, these devices are benign, as in the case of an employee bringing his laptop to work and putting it on the network. In other cases, rogue endpoints are placed by malicious individuals.

EXAMPLE

A janitor is paid to plug a device into an open network port in the building that is behind a cabinet. The device is able to advertise itself on the network as the gateway to the internet to all devices except the actual gateway. By doing so, the device can inspect all traffic coming into and out of the organization over the internet.

Rogue Access Points

Rogue access points are those that you do not manage or control. There are two types: those that are connected to your wired network and those that are not. The ones that are connected to your wired network present a danger to your wired and wireless networks. They may be placed there purposefully by a hacker to gain access to the wired network or by your own users without your knowledge. In either case, they allow access to your wired network. Wireless intrusion prevention systems (WIPS) can be used to locate rogue access points and in some cases even locate them and shut them down.

EXAMPLE

Katy is a CPA in the tax department of a CPA firm. Katy is looking for ways to economize, and the bill she is getting for wireless data on her phone bothers Katy. She knows that her phone can use Wi-Fi to access the internet, thus eliminating the need to access her carrier's wireless network. Since Katy spends long hours at the office during tax season, if she had access to Wi-Fi at her desk, she is sure she could greatly reduce the cost of her phone.

Unfortunately for Katy, her firm does not have Wi-Fi access in the building, so Katy brings in a wireless router she got at an online auction site. Her tech friend tells her how to configure it as an access point only rather than as a router, so she plugs the cord from the wall that was wired into her computer into the router. She then uses a network cable she also obtained at the online auction site to plug her computer into her infrastructure router.

Her tech friend told her she should set up security on the router, but Katy found that page confusing and the router worked just fine with her phone with the security just turned off, so Katy figured it was no big deal.

Now Katy is able to stream music from the internet to her phone that she listens to with her wireless headphones doing all of that tax work the first part of the year with no data charges. She can relax enough to enjoy the view of the park just outside her third-floor window.

General Attacks on Servers

Servers contain critical and sensitive assets and perform mission-critical services for the network. There are fewer of them but for this reason they receive the lion's share of attention from malicious individuals. The following are some issues that can impact any device but that are most commonly directed at servers:

- **DoS.** When attackers overwhelm a device with enough requests to degrade the performance of the targeted device, a denial-of-service attack ("DoS") has occurred. Some popular DoS attacks include Ping of Death, UPF flooding, SYN floods, fraggle, and teardrop attacks.

- **DDoS.** A distributed DoS (DDoS) attack is a DoS attack that is carried out from multiple attack locations. The initial attack is on vulnerable devices that are infected with malware-based software agents. The vulnerable devices, called zombies, become botnets, which then carry out the attack. Because of the distributed nature of the attack, identifying all the attacking botnets is virtually impossible. The botnets also help to hide the original source of the attack.

EXAMPLE

DDoS primarily affects servers exposed to the internet since that's what the botnets can reach. However, it can be used to effectively push an entity off the internet and has been used as part of extortion schemes (pay us, or your site goes dark). Companies exist (such as Cloudflare) that will, for a fee, insulate servers from these attacks using various mechanisms including simply being able to bring extra bandwidth to bear if necessary, to allow a system to continue to operate.

But there is another exposure—a machine or device inside an organization may end up becoming part of a botnet that participates in a DDoS attack. The packets coming from the organization's IP may be noticed by the internet service provider (ISP) providing access to the organization who may take the organization off their system until the organization is able to find and remove the offending machine(s).

- **Buffer overflow.** Buffers are locations in system memory that are used to store information. This attack involves the malicious individual inputting more data than the buffer is expecting. When the amount of data that is submitted to an application is larger than the buffer can handle, a buffer overflow occurs. This type of attack is possible typically because of poorly written application or operating system code, and it can result in an injection of malicious code.

  How does that result in running malicious code? After all, when the buffer overflows, the data overwrites items it shouldn't and when things aren't expected, computer systems crash, right? Well, while we consider it a crash, it rarely is like a car crash where the car then stops and can't be operated.

  The processor generally continues to execute instructions—most often whatever happens to be where the processor gets sent due to the unexpected conditions. When attackers discover a buffer overflow crash, they study what actually happens at the instant of the crash with the processor and then work to create conditions where the processor will end up not just with random gibberish, but rather with code that accomplishes the specific tasks the attacker wishes to accomplish—often to allow the attacker to access data or install software. If all operating systems and applications are updated with the latest service packs and patches, these attacks typically will fail since most vendors patch these flaws as they are made aware of them. In addition, programmers should properly test all applications to check for overflow conditions. Finally, input validation routines should be utilized by programmers to ensure that the data submitted is not too large for the buffer.

  Unfortunately, it's difficult to ensure that no conditions for buffer overflow exist in nontrivial code, so new overflow issues are being discovered each month. Many of the patches included in vendor patches (including Microsoft's "patch Tuesday" patches for Windows that come out most months) are meant to deal with errors such as buffer overflow issues. Attackers study patches as they are issued in order to determine what vulnerabilities remain unmitigated.

  Why would attackers care about problems that have been fixed? They care because many organizations do not immediately apply patches when they are released. Patching an operating system always carries risks—systems (at least those not yet attacked to exploit the flaw) were operating just fine before the patch and there's a small, but not zero, risk that applying the patch will cause the systems to cease to function. Attackers are betting enough unpatched systems will remain when they develop their attack to make developing the attack profitable.

  Of course, excessively delaying patching a system carries risks. The breach of Equifax's systems which exposed highly personal information of more than 140 million individuals was made possible due to a failure to apply patches that were

released more than two months prior to the breach.[5] Kaseya, SolarWinds, and SysAid offer automated patch management solutions.

- **Mobile code.** Software that is transmitted across a network to be executed on a local system is called mobile code. Examples of mobile code include ActiveX controls, Java applets, and JavaScript code. While mobile code includes security controls, malicious mobile code can be used to bypass access controls. For security Java implements sandboxes, and ActiveX uses digital code signatures.

  Note that mobile code is code and thus is subject to the buffer overflow vulnerability previously discussed. Thus, note that the more types of mobile code you allow systems to run, the larger the exposure a system will have to exploit. Clearly, there are advantages to running mobile code. But types of code that the organization does not actually run likely should not be enabled.

- **Emanations.** Electromagnetic signals that are emitted by an electronic device are called emanations. Attackers can target certain devices or transmission media to eavesdrop on communication without having physical access to the device or medium.

  Initiated by the United States and United Kingdom, the TEMPEST program researches ways to block or prevent emanations and standardizes the technologies used. Equipment that meets TEMPEST standards suppresses signal emanations using shielding material. Devices that meet TEMPEST standards usually implement an outer barrier or coating, called a Faraday cage or Faraday shield. TEMPEST devices are most often used in government, military, and law enforcement settings.

- **Backdoor/trapdoor.** A backdoor, or trapdoor, is a mechanism implemented in many devices or applications that gives the user who uses the backdoor unlimited access to the device or application. They can get there either by being implanted by malware or being installed by a developer during development. They are placed there during development to ease access into the program and sometimes they get forgotten and remain installed. Privileged backdoor accounts are the most common type of backdoor in use today. Code escrow is an alternative solution for developers who may still insist on a backdoor for contract issues such as client nonpayment and client license infractions.

Mobile Devices

With a mobile phone (maybe two) in each user's possession and the demand increasing to use these devices on the network, including the greater use of BYOD ("Bring Your Own Device" to work), mobile device security has become everyone's issue. With many of these devices connecting to and using public networks with little or no security, unique challenges are created for security professionals. Mobile device security is a top concern under multiple security frameworks with a recent (2018) update to NIST for both general industry and ePHI (electronic protected health information).

[5] "Equifax failed to patch security vulnerability in March: former CEO," Reuters, https://www.reuters.com/article/us-equifax-breach/equifax-failed-to-patch-security-vulnerability-in-march-former-ceo-idUSKCN1C71VY, October 2, 2017

The threats presented by the introduction of personal mobile devices (smartphones and tablets) to an organization's network include the following:

- Wi-Fi connectivity in open (unencrypted) hotspots
- Lost or stolen devices holding sensitive company data
- Web browsing in insecure locations
- Corrupt and malicious application downloads and installations
- Missing security updates

EXAMPLE

Hal finds it helpful to get out of the office in order to do research on accounting reporting issues undisturbed. He does so by going to his local coffee shop and using their Wi-Fi network. The Wi-Fi network at the coffee house is not secured.

Denise just likes to see what people are doing at the coffee house, including what they are sending over the internet. Denise installs software that turns on promiscuous mode on her network interface and is able to see all data being transmitted over the Wi-Fi network. While she won't be able to see any data sent via modes like SSL/TLS to separately encrypt the traffic, she will be able to read any other data being transmitted. That will include information about where packets are going to, which can itself be useful information. Certainly, she knows more about Hal than Hal probably believes is possible.

Any of these issues can lead to data exfiltration (unauthorized access/copying) from the device.

Network Appliances

Network appliances, many of which are based on Linux systems, may run an operating system or application that is less secure than it should be. Yes, vulnerabilities exist in the very devices designed to secure a network, including intrusion detection and prevention systems! Testing has shown that the following vulnerabilities are somewhat widespread:

- XSS scripting flaws allowing session hijacking
- Interfaces with no protection against brute-force password cracking
- Information about the product model and version that are exposed to unauthenticated users
- Cross-site request forgery flaws that allow attackers to access administration functions by tricking authenticated administrators into visiting malicious websites
- Hidden backdoors

For a specific example, Cisco in early 2018 disclosed a major vulnerability that attackers were attempting to exploit in their Adaptive Security Appliance products.[6] Issues with such devices are particularly troublesome, since by their very nature they are exposed directly to the internet. Thus, exploits generally will be subject to remote execution the attacker can be anywhere in the world and does not need physical access to the device.

Some might think that the failure of those who specialize in selling security solutions to be able to lock down their products means there's nothing that can be done. But that is taking the wrong lesson away from this fact.

Rather, what it tells us is that this is a complex problem with no single solution. An organization needs to have a number of different defenses, including those offered by security vendors. External vendors who offer a network security platform and a network traffic monitoring tool are a good choice. They are necessary but not sufficient, in and of themselves.

Attacks on Virtualization

In today's networks, virtualized devices have become commonplace. While virtualizing a device may seem like it is adding an additional layer of security, a number of vulnerabilities exist with the hosts, the virtual networks, and the management interfaces used to manage virtualization.

Virtual Hosts

Systems that are virtualized (guest systems) share the physical resources of a common host machine. Virtualization is the creation of a virtual—rather than actual—version of something, such as an operating system (OS), a server, a storage device, or network resources.

Virtualization uses software that simulates hardware functionality in order to create a virtual system. This practice allows IT organizations to operate multiple operating systems, more than one virtual system, and various applications on a single server. The benefits of virtualization include greater efficiencies and economies of scale.[7] When systems sharing these resources have varying security requirements, security issues can arise. The following are some of these issues as well as some measures that can be taken to avoid them:

- **VM escape (Virtual Machine escape).** A virtual machine or "VM" is basically a software representation of a computer—there is no physical computer. A VM is an operating system or application that is installed on software, which allows a user to perform functions in a controlled environment; however, if the attacker can discover how his VM's virtual resources map to the physical resources, he will be able to conduct attacks directly on the real physical resources. When an attacker "breaks out" of a VM's normally isolated state and interacts directly with the hypervisor, it is called a VM escape attack. If she exploits the mapping of physical resources to each

[6] Dan Goodin, "That mega-vulnerability Cisco dropped is now under exploit," ArsTechnica, https://arstechnica.com/information-technology/2018/02/that-mega-vulnerability-cisco-dropped-is-now-under-exploit/, February 9, 2018

[7] https://searchservervirtualization.techtarget.com/definition/virtualization

VM (by modifying the VM virtual memory), the attacker can affect all the VMs, hypervisor, and potentially other programs on that machine.

- **Data remnants.** Cloud maintenance functions sometimes leave sensitive data inadvertently replicated in VM. Remnant data left in terminated VMs needs to be protected. When data is moved, data may be left behind, accessible to unauthorized users. Any remnant data in the old location should be destroyed, but with some removal methods, data remnants may remain. This can be a concern with sensitive and confidential information in both public and private clouds.

EXAMPLE

American Widgets has moved much of its accounting system to various hosted third-party locations. These services make use of virtualized cloud servers to hold the data.

If those servers carrying the virtualized hosted system have vulnerabilities like those described in this unit, the data in American Widgets systems could be at risk for exfiltration by unauthorized third parties.

Web Servers

Despite efforts to design secure web architecture, attacks on web-based systems still occur and still succeed.

Maintenance Hooks

Maintenance hooks are sets of instructions built into the code that allows someone who knows about the "backdoor" to use the instructions to connect and then view and edit the code without using the normal access controls. This is another term for backdoor, covered earlier in this section.

EXAMPLE

Arcadia Paper hired an outside developer to create a customized accounting system for the organization. The outside developer, who knows he is likely to be called if issues arise, created a backdoor which allows direct manipulation of data in the system bypassing the audit trail system that he had put in the system. In fact, the audit trail file could be modified through this vulnerability.

The developer could trigger this mode by leaving the username blank at the login screen and then pressing the backspace key five times. He thought this was a clever approach that no one would ever stumble upon.

Walter, a clerk in accounts payable, accidentally dropped a file folder on his desk. It landed on his keyboard, clipping the enter key and then resting on the password field. Walter saw the cursor drop to the password field and was able to see a set of screens he had not seen before. He noticed that this screen offered him options to directly change account balances, create new vendors, change vendors, create entries, etc. He also discovered that he was able to alter the record and the audit trail. He exited this mode and went back into the system using his standard login.

Walter stayed late that evening and attempted to find that screen again. He quickly figured out he could enter that mode by skipping the username field and then enter five backspaces. Walter, who was deeply in debt due to medical issues with his daughter, decided that he could use this newly found ability to help

offset the medical costs that, he rationalized, would have been covered if his employer hadn't skimped on the medical coverage provided to employees.

Time-of-Check/Time-of-Use Attacks

Time-of-check/time-of-use attacks, when successful, take advantage of the sequence of events that occur as a system completes common tasks, typically a security-related task such as verifying authorization to access a resource. They rely on knowledge of the dependencies present when a specific series of events occurs in multiprocessing systems. By attempting to insert himself between events and introduce changes, a hacker can gain control of the result.

A race condition is a term often confused with a time-of-check/time-of-use attack, although this is a different attack. In a race condition attack, the hacker inserts himself and introduces changes between instructions. The end game is to alter the order of execution of the instructions, thereby altering the outcome.

Insecure Direct Object References

This attack can come from an authorized user, meaning that the user has permission to use the application but is accessing information to which she should not have access, or it could come from an unauthorized user. Programs often use the actual name or key of an object when generating web pages. Verifying that a user is authorized, the target object is not always performed by the application. If successful, an insecure direct object reference flaw occurs. To prevent this problem, each direct object reference should undergo an access check. Code review of the application with this specific issue in mind is also recommended.

XSS

Cross-site scripting (XSS) occurs when an attacker locates a website's vulnerability and injects malicious code into the web application. Many websites allow and even incorporate user input into a web page to customize the web page. If a web application does not properly validate this input, one of two things could happen: The text may be rendered on the page, or a script may be executed when others visit the web page.

EXAMPLE

A CPA firm has a website on which they have installed a comments section for their articles which does not adequately work to prevent the injection of code via the comments. Such code will be executed by the browser of future clients that visit the site and be used against those clients.

When the problem is discovered, the firm will find itself with potential liability to those clients and certainly with a major public relations problem.

Cross-Site Request Forgery (CSRF)

A CSRF is an attack that causes an end user to execute unwanted actions on a web application in which he or she is currently authenticated. The attacker exploits the website's trust of the browser rather than the other way around (as with the XSS attack). The website assumes the request came from the user's browser and was made by the user. However, the request was planted in the user's browser. It usually gets there when a user follows a URL that already contains the code to be injected.

Click-Jacking

In this attack, the hacker crafts a transparent page or frame over a legitimate-looking page that entices the user to click something he trusts. When the user hits the seemingly trusted object, he is really clicking on a different and embedded URL. In many cases, the site or application may entice the user to enter sensitive information that could be used later by the attacker.

Session Takeover

Taking steps to protect against session hijacking involves proper session management. According to the hacksplaining.com website (www.hacksplaining.com/glossary/sessions), a session is a "stateful conversation between a website and a user agent, such as a browser" which acts as a shortcut authentication system. Hijacking can occur when a hacker is able to identify the unique session ID assigned to an authenticated user—no need for a hacker to figure out a password in this type of attack. Ensuring that the process used by the web server to generate these IDs is truly random is a critical step.

The hacker needs to identify or discover the session ID of the authenticated user and can do so using several methods:

- **Guessing the session ID.** By gathering samples of session IDs and using these as a bias for estimation, attempts can be made at guessing a valid ID assigned to another user's session.
- **Using a stolen session ID.** Session IDs can be stolen through XSS attacks and by gaining physical access to the cookie stored on a user's computer. Also, while SSL/TLS connections hide these IDs, many sites do not require an SSL/TLS connection using session ID cookies.

EXAMPLE

A firm has hired a developer who created a portal. Clients are assigned a session ID, but the developer decided to simply use an incrementing number for the session ID. Armed with information about what the current session IDs being generated are (perhaps by setting up a potential client account), an attacker could quickly determine potentially valid session IDs and grab the session of the next authenticated user.

Once the attacker takes over the session, the attacker would have the same access to information on the site as the client would—very possibly the client's tax returns and supporting documents that are currently loaded on the site.

Database Attacks

Much sensitive data resides in a database. An attack specific to the servers is made possible by a buffer overflow.

SQL Injection

SQL stands for "structured query language" and is a standardized text-based query language for obtaining information from a database that is in widespread use. Microsoft uses it for their database systems, and SQL is generally used on all UNIX-based systems. SQL databases are even found for many applications on smartphones (remember that iOS and Android OS are both UNIX variants).

When a hacker "injects" a SQL query as the input data to a form or dialogue box from the client to the application and due to a buffer overflow condition, the command is executed, and a SQL injection has occurred. This type of attack can result in reading sensitive data from the database, modifying database data, executing administrative operations on the database, recovering the content of a given file, and even issuing commands to the operating system.

By "injecting" SQL commands into the system (often as part of an input form) and then tricking the system into executing that text as a command (perhaps due to a buffer overflow condition or other flaw in the system), the attacker will be able to obtain some or all of the information that is in the database(s) that the system can access.

CYBERSECURITY STATE REGULATORY AND LEGAL RULES

Organizations, including accounting firms, that handle PII, ePHI, PHI, and other sensitive information, must comply with cybersecurity regulatory and legal rules at several levels, including federal laws, state laws, AICPA rules, and additional sets of regulations created by each state's board of accountancy. We will look at the first two types of regulation. Regulations created by each state's board of accountancy will be covered later in this course.

Federal Laws

Organizations in various industries must comply with relevant laws, regulations, and business rules as they apply to the industry. Ensuring compliance is a vital part of any organization's security initiative. Human resources, legal or external counsel, and senior management should be involved in this endeavor. Moreover, other internal and external entities may become stakeholders in the legal compliance and advocacy program. These two programs differ in these ways:

- Legal compliance ensures that an organization follows relevant laws, regulations, and business rules.
- Legal advocacy is the process carried out by or for an organization that aims to influence public policy and resource allocation decisions within political, economic, and social systems and institutions.

Involvement of human resources ensures that the organization is addressing all employment laws and regulations to protect its employees. When security policies are created to support these laws and regulations, human resources professionals can help ensure that individual rights are upheld while at the same time protecting organizational assets and liability. For example, an organization might display a screen at login (a "login banner") that informs users of the employer's rights to monitor, seize, and search organizational devices. Both the HR and legal departments should be involved in creating the statement that will be displayed to ensure that it includes all appropriate information.

An understanding of the relevant laws by the organization is required to ensure legal compliance. Financial, healthcare, industrial production and other business sectors are examples of industries that often have many federal, state, and local laws to consider. A few of the laws and regulations that must be considered by organizations are covered below.

Sarbanes-Oxley (SOX) Act

This law affects any organization that is publicly traded in the United States. More commonly known as the Sarbanes-Oxley (SOX) Act, the Public Company Accounting Reform and Investor Protection Act of 2002 regulates the accounting methods and financial reporting for the organizations and stipulates penalties and even jail time for noncomplying executive officers.

Health Insurance Portability and Accountability Act (HIPAA)

The Kennedy-Kassebaum Act, or HIPAA as it is also known, affects all healthcare facilities, health insurance companies, and healthcare clearinghouses which create and/or come into contact with PHI/ePHI (protected health information/electronic protected health information). HIPAA includes specific sections relating to privacy and security safeguards (the HIPAA Privacy Rule and the HIPAA Security Rule).

Officially, if a state law is "contrary" to HIPAA, HIPAA will be used. When state law is "more stringent" than HIPAA, both HIPAA and state law will be applied. The New York Department of Health has even published a HIPAA Preemption Chart which states that New York state law will, under certain circumstances, prevail over HIPAA.

HIPAA is enforced by the Office of Civil Rights of the Department of Health and Human Services.

Gramm-Leach-Bliley Act (GLBA) of 1999

Financial institutions, including banks, loan companies, insurance companies, investment companies, and credit card providers are the target of the Gramm-Leach-Bliley Act (GLBA) of 1999 which directly affects the security of PII. It provides guidelines for securing all financial information and prohibits sharing of financial information with third parties. GLBA is frequently used in conjunction with the FTC (Federal Trade Commission) Safeguards (security) and Red Flags (identity theft) rules. GLBA will also be preempted by state privacy laws under certain circumstances.

Computer Fraud and Abuse Act (CFAA)

This law defines “protected computers” and affects any entities that might engage in hacking of “protected computers.” Enacted in 1986 and amended in 1989, 1994, and 1996, the CFAA defines a “protected computer” as a computer used exclusively by a financial institution or the U.S. government or used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

The CFAA was updated in 2001 by the Uniting and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act; and in 2002 and in 2008 by the Identity Theft Enforcement and Restitution Act.

Most internet communications, ordinary computers and even smart phones have come under the jurisdiction of the law due to the interstate nature of most internet communication. For purposes of the law, hacking includes knowingly accessing a computer without authorization; intentionally accessing a computer to obtain financial records, U.S. government information, or protected computer information; and transmitting fraudulent commerce communication with the intent to extort.

Federal Privacy Act of 1974

Affecting any device that contains records used by a federal agency, the Federal Privacy Act of 1974 provides guidelines on collection, maintenance, use, and dissemination of PII about individuals that is maintained in systems of records by federal agencies on collecting, maintaining, using, and distributing PII.

Computer Security Act of 1987

While this act was superseded by the Federal Information Security Management Act (FISMA) of 2002, the Computer Security Act of 1987 was the first law written to require a formal computer security plan. Written to protect and defend any of the sensitive data in federal government systems and to provide security for that information, it also requires government agencies to train employees and identify sensitive systems.

Personal Information Protection and Electronic Documents Act (PIPEDA)

The act was written to address European Union (EU) concerns about the security of PII in Canada. Private-sector organizations that collect, use, and disclose personal information in the course of commercial business in Canada are covered by the PIPEDA. Consent is required when these entities collect, use, or disclose personal information. Personal information policies that are clear, understandable, and readily available are also required. Provincial laws (Quebec, British Columbia, etc.) relating to PII also apply under certain circumstances.

Basel II

While this act doesn't directly address cybersecurity, it is an important banking law that came about after numerous bank failures. Its main purpose is to protect against risks that banks and other financial institutions face. Basel II affects financial institutions and addresses minimum capital requirements, supervisory review, and market discipline. Basel III, Basel II's successor, will consider the emerging area of fintech, and will also address cybersecurity requirements for data storage as it is implemented in stages through 2022.

Payment Card Industry Data Security Standard (PCI DSS)

PCI is a framework and not a regulation. Organizations that handle cardholder information and process payments from the major credit cards (Visa, MasterCard, and Discover) are encouraged and sometimes required to comply with the standard, in order to continue to process such payments. Organizations can validate compliance by participating in annual voluntary third-party audits. Although PCI DSS is not a law, this standard has affected the adoption of several state laws. PCI is a security framework and is now on version 3.2.1 (May 2018). Version 4.0 is currently in the RFC (request for comment) phase and should be implemented in mid-2021.

Federal Information Security Management Act (FISMA) of 2002

This law superseded the Computer Security Act of 1987 and affects every federal agency. The Federal Information Security Management Act (FISMA) of 2002 requires each federal agency to develop, document, and implement an agency-wide information security program.

Economic Espionage Act of 1996

This law makes theft of a trade secret a federal crime and that trade secret does not need to be tangible to be protected by this act. The Economic Espionage Act of 1996 covers companies or individuals that have trade secrets and those who plan to use encryption technology for criminal activities. It also requires reports generated by the U.S. Sentencing Commission to provide specific information regarding encryption or scrambling technology that is used illegally.

USA PATRIOT Act

Amending several other laws, including FISA and the ECPA of 1986, the USA PATRIOT Act of 2001 affects law enforcement and intelligence agencies in the United States. It enhances the investigatory tools that law enforcement can use, including email communications, telephone records, internet communications, medical records, and financial records.

Although the USA PATRIOT Act does not restrict private citizens' use of investigatory tools, there are exceptions, such as the following:

- If the private citizen is acting as a government agent (even if not formally employed)

- If the private citizen conducts a search that would require law enforcement to have a warrant
- If the government is aware of the private citizen's search
- If the private citizen is performing a search to help the government

Health Care and Education Reconciliation Act of 2010

Affecting healthcare and educational organizations, this act increased some of the security measures that must be taken to protect healthcare information.

Securities and Exchange Commission

The SEC has issued Release No. 33-10459, effective February 28, 2018, that deals with disclosures on cybersecurity risk and incidents. The official guidance is very similar to the 2011 *CF Disclosure Guidance: Topic 21* issued by the Division of Corporate Finance staff.[8]

As the Commission notes in the preamble to the release:

> Given the frequency, magnitude, and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack. Crucial to a public company's ability to make any required disclosure of cybersecurity risks and incidents in the appropriate time frame are disclosure controls and procedures that provide an appropriate method of discerning the impact that such matters may have on the company and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality of such risks and incidents.

The release notes that issuers are required to provide timely information in their periodic reports regarding cybersecurity risks and incidents, including on their Forms 10K, 10-Q, and 20-F. The release provides that "companies must provide timely and ongoing information in these periodic reports regarding material cybersecurity risks and incidents that trigger disclosure obligations."

The release reminds issuers of their obligations under the Securities and Exchange Act. The release provides:

> Securities Act and Exchange Act registration statements must disclose all material facts required to be stated therein or necessary to make the statements therein not misleading. Companies should consider the adequacy of their cybersecurity-related disclosure, among other things, in

[8] See AICPA's take as well here: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity/comparison-of-sec-release-33-10459.pdf

> the context of Sections 11, 12, and 17 of the Securities Act, as well as Section 10(b) and Rule 10b-5 of the Exchange Act.

The release also discusses reporting on a current basis information on cybersecurity matters:

> In order to maintain the accuracy and completeness of effective shelf registration statements with respect to the costs and other consequences of material cybersecurity incidents, companies can provide current reports on Form 8-K or Form 6-K. Companies also frequently provide current reports on Form 8-K or Form 6-K to report the occurrence and consequences of cybersecurity incidents. The Commission encourages companies to continue to use Form 8-K or Form 6-K to disclose material information promptly, including disclosure pertaining to cybersecurity matters. This practice reduces the risk of selective disclosure, as well as the risk that trading in their securities on the basis of material nonpublic information may occur.

The Commission goes on to provide the following guidance to reporting entities on how to determine cybersecurity reporting obligations:

> In determining their disclosure obligations regarding cybersecurity risks and incidents, companies generally weigh, among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations. The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations. The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause. This includes harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.

Disclosure of cybersecurity risks and incidents can, if not properly handled, serve to increase the entity's exposure to attack and the Commission notes that it is not suggesting that a company must provide a "roadmap" for those seeking to break into the company's systems. But the guidance goes on to note that:

> Nevertheless, we expect companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences. Where a company has become aware of a cybersecurity incident or risk that would be material to its investors, we would expect it to make appropriate disclosure timely and sufficiently prior to the offer and sale of securities and to take steps to prevent directors and officers (and other corporate insiders who were aware of these matters) from trading its securities until investors have been appropriately informed about the incident or risk.

The SEC also warns companies that while there may be concerns about disclosures regarding an incident while it is under investigation, that:

> An ongoing internal or external investigation, which often can be lengthy, would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.

Also, companies are reminded of their duty to correct prior disclosures that the company determines were untrue at the time a statement was made or to update a disclosure if the company discovers it was materially inaccurate after it was made. Because of these duties, the Commission advises:

> Companies should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.

The Commission also discourages what might be viewed as "communicate nothing" very generic statements, noting:

> Companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors.

The Commission goes on to note that risks associated with cybersecurity and cybersecurity incidents may rise to the level of significant risks that require disclosure under Item 503(c) of Regulation S-K and Item 3.D of Form 20-F.

The release lists the following factors to be considered when evaluating cybersecurity disclosure:

- The occurrence of prior cybersecurity incidents, including their severity and frequency
- The probability of the occurrence and potential magnitude of cybersecurity incidents
- The adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks
- The aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third-party supplier and service provider risks
- The costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers
- The potential for reputational harm
- Existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies

- Litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents

The release provides that a company may need to disclose prior or ongoing cybersecurity incidents as part of its cybersecurity risk disclosure in order to put the risk in context:

> For example, if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident may occur. Instead, the company may need to discuss the occurrence of that cybersecurity incident and its consequences as part of a broader discussion of the types of potential cybersecurity incidents that pose particular risks to the company's business and operations. Past incidents involving suppliers, customers, competitors, and others may be relevant when crafting risk factor disclosure. In certain circumstances, this type of contextual disclosure may be necessary to effectively communicate cybersecurity risks to investors.

Under Rule 303 of Regulations S-K and Item 3.D of Form 20-F, the release notes may be required as part of management's discussion and analysis of a company's financial condition, changes in financial condition, and results of operations, to provide information on cybersecurity matters. The release states:

> In this context, the cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other matters, could inform a company's analysis. In addition, companies may consider the array of costs associated with cybersecurity issues, including, but not limited to, loss of intellectual property, the immediate costs of the incident, as well as the costs associated with implementing preventative measures, maintaining insurance, responding to litigation and regulatory investigations, preparing for and complying with proposed or current legislation, engaging in remediation efforts, addressing harm to reputation, and the loss of competitive advantage that may result.

The impact of these incidents on each of the company's reportable segments must also be considered per the release.

The release also reminds companies that cybersecurity issues can create required disclosures of material impacts arising from such incidents as they affect a company's products, services, relationships with customers or suppliers, or competitive conditions, as well as require disclosure of material legal proceedings arising from these incidents.

In the area of financial statement disclosures, the release notes that incidents and their related risks may affect the statements. For example, cybersecurity incidents may result in the following:

- Expenses related to investigation, breach notification, remediation and litigation, including the costs of legal and other professional services

- Loss of revenue, providing customers with incentives or a loss of customer relationship assets value
- Claims related to warranties, breach of contract, product recall/replacement, indemnification of counterparties, and insurance premium increases
- Diminished future cash flows, impairment of intellectual, intangible, or other assets
- Recognition of liabilities
- Increased financing costs

The Commission expects that a company's financial reporting and control systems would be designed to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cybersecurity incident would be incorporated into its financial statements on a timely basis as the information becomes available.

With regard to the board of directors and their oversight of these issues, the Commission states:

> A company must include a description of how the board administers its risk oversight function. To the extent cybersecurity risks are material to a company's business, we believe this discussion should include the nature of the board's role in overseeing the management of that risk.
>
> In addition, we believe disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area.

The release goes on to discuss the implications of cybersecurity risks to the design and effectiveness of disclosure controls and procedures and imposes responsibilities on the company's principal executive officer and principal financial officer in this area:

> Exchange Act Rules 13a-14 and 15d-14 require a company's principal executive officer and principal financial officer to make certifications regarding the design and effectiveness of disclosure controls and procedures, and Item 307 of Regulation S-K and Item 15(a) of the Exchange Act Form 20-F require companies to disclose conclusions on the effectiveness of disclosure controls and procedures. These certifications and disclosures should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. In addition, to the extent cybersecurity risks or incidents pose a risk to a company's ability to record, process, summarize, and report information that is required to be disclosed in filings, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective.

The release points out that information regarding cybersecurity incidents can lead to issues regarding insider trading. Specifically, information about a company's

cybersecurity risks and incidents may be material nonpublic information, and directors, officers, and other corporate insiders will violate the antifraud provisions if they trade the company's securities in breach of their duty of trust or confidence while in possession of that material nonpublic information.

State Regulations

Of course, state regulations vary and change often. The National Association of State Legislatures, through their website, lists Cybersecurity Legislation of 2017. From the website, they say the following in this regard:

> States are addressing cybersecurity through various initiatives, such as providing more funding for improved security measures, requiring government agencies or businesses to implement specific types of security practices, increasing penalties for computer crimes, addressing threats to critical infrastructure, and more.

2018 Introductions

According the National Council of State Legislatures ("NCSL"), at least 31 states have introduced bills or resolutions to amend existing laws related to cybersecurity. Some of the key areas of legislative activity include the following:

- Requiring free credit freezes for victims of data breaches
- Broadening the definition of "personal information" for breach notification requirements
- Implementing separate beach notification regulations for student information breaches

2018 Enactments

At least 18 states enacted legislation in 2018.

Note: *Please check individual legislative websites for the most current status, summaries, and versions of bill text.*

2018 Cybersecurity Laws Enacted

Highlights

In 2019, New York state enacted 23 NYCRR 500, GDPR-modeled cybersecurity regulation that requires organizations in the financial industry (insurance, banks, money service businesses) that are both regulated by the Department of Financial Services (DFS) and meet certain criteria to comply. Organizations that come under the purview of this law must assess their security risks and develop policies for data protection including classification, governance, access controls, external testing, system monitoring, and incident response.

Alabama and South Dakota, the final two states without laws relating to breaches and breach notification requirements, enacted cybersecurity laws during 2018 (the Alabama Data Breach Notification Act of 2018 [S.B. 318] and the South Dakota Breach Notification Law [S.B. 62]). In order to avoid a state referendum, California's Governor Brown signed the California Consumer Privacy Act of 2018 (SB 1121) into law in September, paving the way for enhanced consumer privacy rights and new obligations on certain firms doing business in the state. South Carolina enacted the Insurance Data Security Act, which places cybersecurity protection and response requirements on certain state insurance licensees. And in Ohio, the state enacted its novel Cybersecurity Safe Harbor Act, which provides certain defenses for eligible organizations in the event of a breach based on approved criteria such as compliance with a recognized security framework.

In 2018 state case law developments, the Pennsylvania Supreme Court ruled that employers have a duty to safeguard employee personal data from breaches.

Recent years have seen a flurry of additional state privacy law updates, with expansion of the definition of personal information to include **biometric data**: Arizona, Arkansas, Colorado, Illinois, Iowa, Louisiana, Maryland (2018), Massachusetts (pending), Nebraska, New Mexico (2017), New York (New York SHIELD Act), North Carolina, Oregon, Washington state (2019/2020), Wisconsin (2016 or earlier); new regulations on **data brokers**: California's CCPA, Illinois (pending); **geolocation data defined as regulated personal data**: California, New Jersey (pending).

Security Breach Notification Laws (The National Association of State Legislatures Through Their Website)

All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have also enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.

Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/information brokers, government entities, etc.); definitions of "personal information" (e.g., name combined with SSN, driver's license or state ID, account numbers, biometric data such as fingerprints, DNA, retinal scans, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).

Specifics of the Security Breach Notification Laws for each state are found at this link (as state cybersecurity laws are updated frequently, carefully check the "last updated" date on this website):

- http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

A key item to notice is that the **laws generally grant protection to encrypted data if a device is lost—that is, certain notifications are not required as long as the encryption key has not been lost or stolen**. CPAs, especially in public practice, will likely have client data in various forms they have received.

Ohio enacted the Ohio Data Protection Act, Senate Bill 220, in November 2018. This law offers firms which do business in Ohio a safe harbor defense from certain litigation relating to several types of security incidents if the firm maintains a "higher level of cybersecurity" by incorporating one of seven commonly used information security frameworks.

There is significant exposure for an unencrypted laptop, thumb drive, backup drive, smart phone, or similar device if it is lost or stolen.

EXAMPLE

Jessica is an Ohio CPA working for a firm with an Ohio office location. She has gone out to a client's office (also located in Ohio) to get a copy of the client's accounting database loaded onto a 128GB USB flash drive. Jessica has not encrypted the flash drive. She will use the information in the database as part of the examination of the client's financial statements. Jessica has loaded numerous client information on the drive—generally complete copies of the accounting data including information on employees from the payroll system.

Jessica erases the data from the drive once she has transferred the data onto her firm's network back at the office. She does so because she wants to ensure no data would be lost from those clients if the drive were to be lost or stolen.

Jessica stops at the gas station on the way back to the office. When she pulls her wallet out of her purse, the flash drive falls to the ground. When she arrives at the office, she notices that the flash drive is missing.

All 50 states have data breach laws, and most would require Jessica to notify clients and state authorities of the breach details, including the loss of personally identifiable information, within a certain time frame.

Additionally, flash drives do not actually write over files when data is erased. In fact, due to issues with the limited number of times that data can be written to a location on the drive, the drive's firmware will likely not write over any of the old client data files until it has written to every other location on the drive. Thus, Jessica's firm must also notify every other client whose data may have at some time been on that drive.

What could Jessica's firm have done to prevent this scenario from occurring?

Jessica's facts include several Ohio contacts, which would allow her the Ohio Data Protection Act's safe harbor protection if her firm had undergone a prior cybersecurity risk assessment under one of several security frameworks—her firm should have arranged for a risk assessment to receive the benefits of this safe harbor, which could include at least a partial defense to any litigation resulting from Jessica's actions.

All states allow at least a partial data breach defense if the data involved in a breach has been encrypted without a loss of the encryption key. Controls should have been in place to require that any client data be encrypted on all devices.

EXAMPLE

AWC, a professional business organization, has irreplaceable detailed data on its members on an unencrypted hard drive that has failed. Having no backups, AWC looks to hire an outside contractor located across the country to attempt to recover the data on the drive. The outside contractor has told the organization it is likely the data can be recovered in a relatively cost-effective manner, but they will need the drive.

AWC uses an overnight delivery service to get the drive to the vendor as soon as possible. When they call late the next day to see how the recovery is going, the vendor tells them they have not received any drive. When AWC contacts the delivery service, they find that the service shows the drive being taken in for delivery, but no other information on the drive is in their system. Further investigation proves fruitless.

AWC, under most state laws, will need to notify state authorities of the breach, as well as inform each member of this potential loss of their personal data.

Regulations Created by State Boards of Accountancy

Most state boards of accountancy either explicitly or implicitly incorporate the AICPA Code of Conduct into their regulations, so looking at the requirements for a CPA to use a third-party service provider without getting permission of each client is helpful.

Scenario 1 – Identifying the Difference: When is Notification Required?

As a group, examine the following three scenarios and identify in which scenario breach notification is required and which entities must receive notification. Utilize the link provided to research each state's security breach notification law found at the link following link. For purposes of this exercise, assume that the laws noted on the website are in effect and valid.

http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

- A laptop is lost in New York that contains client data including names combined with SSN and driver's license numbers. The data was encrypted, and the key was stored on the device.
- A thumb device was stolen in North Carolina that stores 1,200 client account numbers, SSNs, and addresses. The data was not encrypted, and the decryption key has not been lost or stolen.
- An external hard drive is missing at the office in Florida. It is unknown at this time whether it was lost or stolen. It contained encrypted client data including names and addresses. The key was not stored in the drive.

LIMIT CYBERSECURITY RISKS BY APPLYING CORE PRINCIPLES

While cyber threats appear to be insurmountable at times, there are basic principles that when followed can help to prevent the occurrence of data breaches and reduce their impact of those breaches when they do occur. We will look at some of those principles. After that we will look at the use of the Client Assessment: Cybersecurity Service Opportunities form, which can be used to identify service opportunities that might be available with a client. This form, a part of the PCPS Cybersecurity Toolkit, can be used to assess a client for adherence to basic core cybersecurity principles.

Core Cybersecurity Principles

When implementing security and managing risk, there are several important security principles and terms that you must keep in mind. We will take a look at these.

CIA

The three fundamentals of security are confidentiality, integrity, and availability (CIA), often referred to as the CIA triad. Most security issues result in a violation of at least one component of the CIA triad. Understanding these three security principles will help security professionals ensure that the security controls and mechanisms implemented protect at least one of these principles.

Fulfilling at least one of the security principles of the CIA triad is the purpose of every security control that is put into place by an organization. Understanding how to circumvent these security principles is just as important as understanding how to provide them.

A balanced security approach should be implemented to ensure that all three facets are considered when security controls are implemented. When implementing any control, you should identify the risk that the control addresses. For example, RAID (Redundant Array of Independent Disks) addresses data availability, file hashes address data integrity, and encryption addresses data confidentiality. A balanced approach ensures that no facet of the CIA triad is ignored:

1. **Confidentiality.** To ensure confidentiality, you must prevent the disclosure of data or information to unauthorized entities. As part of confidentiality, the sensitivity level of data must be determined before putting any access controls in place. Data with a higher sensitivity level will have more access controls in place than data at a lower sensitivity level. Identification, authentication, and authorization can be used to maintain data confidentiality.

   The opposite of confidentiality is disclosure. Encryption is probably the most popular example of a control that provides confidentiality. But encryption by itself is not sufficient to protect confidentiality—at some point the ability to decrypt data will be provided to a party.

   As crucial as making sure the data is strongly encrypted is ensuring that only authorized parties will have access to the key to decrypt the data—and authenticating the party authorized to decrypt data is far more technically difficult than providing strong encryption.

EXAMPLE

Christopher is working with payroll information for ABC Company. He needs to transmit information about the company's employees, including personally identifiable information and sensitive payroll information, to the third-party administrator handling the retirement plans for the company. He notices a file transfer service that promises secure transfers, pointing out they use unbreakable AES 256 encryption on the data in transit. The product is also easy to use, allowing the recipient to merely click a link in an email the service will be sent to the recipient to have the data delivered in fully readable and usable form.

Christopher decides to use this system to transfer the highly sensitive payroll information. Unfortunately for Christopher, an unauthorized party intercepts the email with the link. Since the unauthorized party has the address and the link has been authenticated, the third party is able to decrypt the unbreakable AES 256 encryption automatically and conveniently by the transfer service.

EXAMPLE

Christopher is aware of the interception issue, so he looks further at the service. Christopher implements a control that requires the recipient to enter a separate passcode. Believing this will solve the problem, he creates a long, complex password.

Christopher uploads the file with the password to be sent to the third-party administrator. He then sends a second email that contains the password. Unfortunately, since he used the same method to send the password and the encrypted file, the same unauthorized party is able to capture both emails.

Christopher should have called the administrator and told her the password verbally. This technique delivers the password under a different method which is more secure and is described as an "out of band" communication.

Christopher, recognizing the issues, arranges to deliver the complex password to the third party via other means. Now the party that intercepts the email is missing the item he/she needs to access the unencrypted data. Assuming the password is sufficiently complex, it should be effectively impossible for the third party to be able to access that information unless other flaws exist in the file transfer service.

2. **Integrity.** Integrity, the second part of the CIA triad, ensures that data is protected from unauthorized modification or data corruption. The goal of integrity is to preserve the consistency of data, including data stored in files, databases, systems, and networks.

   Maintaining the integrity of the data consists of several components: the quality, accuracy, completeness, and continuity of the data. Data that is either incomplete or inaccurate cannot serve the purpose for which it is being collected and stored. For example, if a bank has the wrong address of a customer, then sensitive data such as bank account numbers can be mailed to the wrong person. Organizations should continually verify the information that they store is the most up to date,

   The opposite of integrity is corruption. An access control list (ACL) is an example of a control that helps to provide integrity. An access control list for a file system provides various levels of permissions that a user must possess to access or change the file.

   Similarly, system logs provide audit trials revealing changes to the database. These audit trials help assure the integrity of the data, as even those who are authorized to make changes will find their actions recorded. The log file should be writable by the program and will also contain controls, such as computed signatures to allow the program to determine if the file has been altered.

3. **Availability.** Availability means ensuring that data is accessible when and where it is needed. Only individuals who need access to data should be allowed access to that data. The two main areas where availability is affected are when attacks disable and/or cripple operations and the loss of service occurring during and after disasters. Each system should be assessed on its criticality to organizational operations. Controls should be implemented based on each system's criticality level.

   In order for data to be useful, it must be available to the intended users. Organizations experience availability issues when drives or servers are damaged.

Systems are down. Hackers or bad actors are sometimes involved in attacks that affect availability. A denial-of-service attack occurs when the hacker takes over the organization's information systems and blocks the organization or their users' access to their data. Again, in this scenario, securing systems with authentication, strong passwords, and firewalls can prevent bad actors from accessing their systems.

Availability is the opposite of destruction or isolation. Fault-tolerant technologies, such as RAID or redundant sites, are examples of controls that help to improve availability. But CPAs should remember that fault-tolerant is not the same as fault free—for instance, while a RAID 5 arrangement will survive the loss of one drive, if a second drive fails before a new drive is installed in the array *and* the system is rebuilt, data loss will still occur. That can be a real problem if the firm, believing RAID 5 solved data loss problems- has no other backup of the data. Backing up data to the cloud or to an external offline device ensures that the data is available in the event there is a failure in hardware where the data is stored.

With regard to data availability, being a strong believer in Murphy's Law (anything that can go wrong will go wrong at the worst possible moment) is helpful when designing a system to achieve high availability. Organizations should have disaster recovery plans in place to respond timely and restore operations with minimal disruption.

EXAMPLE

Evans and Johnson, CPAs, arrives at their offices on April 10 with plans to prepare client extensions for tax season beginning that morning. They discover that the server that contains all of their tax files, including the entire file system, has failed. The firm is a modern paperless firm and for security reasons do not store paper files.

If Evans and Johnson had a recent backup of their files, perhaps in the cloud, it would have been immediately available. However, if no recent backup exists or the only existing backup is from six months earlier, the firm may be facing a problem that could result in the ultimate failure of the organization.

Defense-in-Depth

A defense-in-depth strategy refers to the practice of using multiple layers of security between data and the resources on which it resides and possible attackers. The first layer of a good defense-in-depth strategy is appropriate access control strategies. Access controls exist in all areas of an information systems (IS) infrastructure (more commonly referred to as an IT infrastructure), but a defense-in-depth strategy goes beyond access control.

Job Rotation

Job rotation ensures that more than one person fulfills the job tasks of a single position within an organization. This job rotation ensures that more than one person is capable of performing those tasks providing redundancy. It is also an important tool in helping an organization to recognize when fraudulent activities have occurred.

Auditors should recognize that this control is one that has been applied to accounting systems well before they were ever placed on computers. But too often what we easily recognize as a risk in a client's systems, we blithely accept in our own organizations.

Separation of Duties

Separation of duties ensures that one person is not capable of compromising organizational security. Any activities that are identified as high risk should be divided into individual tasks, which can then be allocated to different personnel or departments. When an organization implements adequate separation of duties, collusion between two or more personnel would be required to carry out fraud against the organization. *Split knowledge*, a variation of separation of duties, ensures that no single employee knows all the details to perform a task. An example would be two individuals knowing parts of a safe combination. Another variation is dual control, which requires that two employees must be available to complete a specific task to complete the job. An example of this is two managers being required to turn keys simultaneously in separate locations to launch a missile.

We just need to recognize that this same separation of duties concept applies not just to accounting information but all aspects of our information systems.

Principle of Least Privilege

The principle of least privilege prescribes that a user or process is given only the minimum access privilege needed to perform tasks and their duties. Its main purpose is to ensure that users are only authorized to perform the tasks they need to perform. To properly implement the least privilege principle, organizations must identify all users' jobs and restrict users only to the identified privileges.

Authentication

This control requires users to provide additional information beyond a password before they can gain access to systems. Two-factor authentication requires a user to enter something they know (password) and something they have, such as a code from a cell phone. Multifactor includes an additional step, often times a biometric scan of a finger, face, handprint, or iris.

EXAMPLE

Mary is using an administrator account on her work computer since that's how her Windows machine came configured out of the box and she figured it was better to have fewer restrictions on her account so she can easily access it. After all, she has work to do and having to deal with the computer getting in her way isn't what clients are paying her for.

Mary falls victim to a malware laden website, which surreptitiously installed malware on her system. That program, now running using the administrator rights on Mary's computer and is able to install additional programs. The malware also accesses various restricted areas on the firm's network computers, obtaining confidential client information, not only on Mary's clients, but also on clients for all other members of the firm.

If Mary had been running a normal user account rather than an administrative-level account, it is very likely the attempted installation of the malware would have been thwarted immediately.

Need-to-Know Principle

The need-to-know principle is closely associated with the concept of least privilege. Although least privilege seeks to reduce rights or privileges (actions) to a minimum, the need-to-know principle applies to the access of information assets (data). This concept prescribes that users are ONLY given access to the resources required to perform their job and the specific access right (full control, read, write etc.) should be kept to the minimum required by their job. A common implementation of the least privilege is when a systems administrator is issued both an administrative-level account and a normal user account. In most day-to-day functions, the administrator should use his normal user account. When the systems administrator needs to perform administrative-level tasks, he should use the administrative-level account. If the administrator uses his administrative-level account while performing routine tasks, he risks compromising the security of the system and user accountability.

EXAMPLE

Christopher, our friend from the payroll department discussed earlier, needs access to payroll information to be able to do his job. But he almost certainly does not need access to detailed information on accounts payable or the ability to rummage through the entire general ledger of the organization. Thus, in a well-designed system, Christopher's access would be limited to those needed to fulfill his payroll functions.

Similarly, someone in accounts payable should generally not need complete access to the payroll data of the company. That person's access should, instead, be limited to those items necessary to handle their accounts payable responsibilities.

One problem in many organizations (especially smaller ones) is that the simplest approach is to just allow all members of the accounting department access to all data. Doing the work to limit access generally requires someone with knowledge of each person's detailed job responsibilities learning the system's configuration options and adjusting them to fit the organization's needs. Most CPAs recognize the issue immediately for accounting records—but the same principle applies to other information on the network. After all, if Christopher can gain access to detailed information about the technical details of products under development, he could misuse (e.g., sell to a competitor) that information even though it's not accounting information.

Organizational rules that support the principle of least privilege include the following:

- Keep the number of administrative accounts to a minimum
- Administrators should use normal user accounts when performing routine operations

To more easily support the least privilege and need-to-know principles, users should be divided into groups to facilitate the confinement of information to a single group or area. This process is referred to as *compartmentalization*.

Security Frameworks

Adopting an IT security framework is key to clearly defining information security controls in an enterprise environment. There is some overlap in controls and complexity in these frameworks. In some highly regulated industries, some frameworks are either required (financial, government) or recommended (health care). Organizations must tailor these frameworks to work with their objectives, operations, and risks.

COBIT

Control Objectives for Information and Related Technology (COBIT®) was developed in the 90s by the IT organization ISACA®. It is primarily focused on reducing IT and business risk, while achieving goals. It is often used to meet Sarbanes-Oxley (SOX) rules.

ISO 27000 Series

ISO 27000 services was developed by the International Organization for Standards. The framework is divided up into standards based on content and can be applied to all industries and organization sizes. ISO 27000 is particularly helpful for cloud computing, secure storage, and digital evidence collection.

NIST

The National Institute of Standards and Technology (NIST) has been building an extensive collection of information security standards and best practices documentation. Government agencies use NIST 800-53 to comply with the Federal Information Processing Standards (FIPS) requirements. The Department of Defense (DOD) utilizes 800-171 to set standards for vendor and supplier compliance.

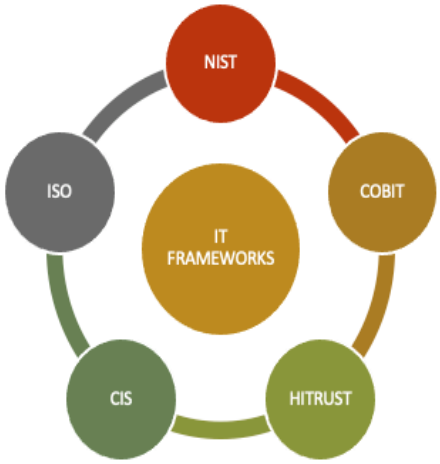
CIS Controls

This framework provides a list of technical controls and best practice configurations that can be applied in any environment, though it does not address risk management. It is used to harden technical infrastructure and increase resilience.

HITRUST

This framework was specifically developed to assist covered entities and business associates in the health care industry with compliance with the HIPAA privacy rule and HITECH security rules.

Top Security Frameworks



Recommendations From AICPA

In the publication, *A CPA's Introduction to Cybersecurity*, the AICPA offers additional recommendations.

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

- **Risk assessment.** This involves identifying and analyzing events that can negatively impact an organization's operations, employees, customers, and assets. The organization must then make decisions based on its ability to treat those risks. Organizations can do any of the following regarding identified risks:
  - Ignore (do nothing)
  - Accept (absorb the risk as part of business strategy and plan)
  - Mitigate (take measures to reduce the risk)
  - Transfer (outsource the risk)
  - Share (with a third party)
  - Avoid (stop or end the activity that is the source of the risk)

  Conduct a cybersecurity risk assessment to determine the firm's susceptibility to IT vulnerabilities, identifying the most critical areas to address.

  This step is similar to the brainstorming of possible ways accounting systems could be open to fraud in an auditing engagement. The mere act of going through

considering your exposures will bring the key issues to the surface. Technologically astute CPAs will recognize specific obvious vulnerabilities to systems (such as passwords placed on Post-It notes on monitors).

When assessing risks, people are just as important as your IT systems, and those people include the organization's customers/clients, vendors, and contractors who have any interaction with your systems.

EXAMPLE

Seagate is a large manufacturer of mass storage devices with sophisticated IT controls over its business aspects. Highly sensitive information was exfiltrated from their payroll systems.

In early 2016, an employee in Seagate's payroll department received an email claiming to be from the company CEO. The email appeared to be a genuine Seagate electronic communication, asking the employee to send the CEO a PDF of the W-2s for all of the organization's employees.

The employee complied with the bogus request and replied with an attached PDF with all of the organization's W-2s for its employees for 2015.[9]

Seagate was not the only organization targeted. This particular phishing incident has continued to occur. The IRS issued public warnings about this ruse in 2018.[10]

- **Account for sensitive data.** Identify the nature and type of data being stored by firm associates on your IT systems. Create an inventory and classify the data according to sensitivity (proprietary, private, confidential, public) in order to employ measures sufficient to protect that data. Do not forget to include data stored on laptops, removable drives, mobile devices, wearables, cloud-based services with third parties, and even hard copy printed records.

- **Require strong passwords.** Make sure that all users of the firm's IT systems have been trained in proper password security techniques. Also, ensure that laptops, servers, and other devices have been hardened with security software and password protections relating to length, composition, the maximum number of login attempts, etc.

- **Multifactor authentication.** This is an authentication method in which a user is granted access to something only after successfully presenting two or more pieces of evidence to an authentication mechanism: something you know (example: passcode), something you have (example: smart card), and something you are (example: fingerprint).

---

[9] Brian Krebs, "Seagate Phish Exposes All Employee W-2's," Krebs on Security, https://krebsonsecurity.com/2016/03/seagate-phish-exposes-all-employee-w-2s/, March 6, 2016

[10] "IRS, States and Tax Industry Warn Employers to Beware of Form W-2 Scam; Tax Season Could Bring New Surge in Phishing Scheme," IRS Website, https://www.irs.gov/newsroom/irs-states-and-tax-industry-warn-employers-to-beware-of-form-w-2-scam-tax-season-could-bring-new-surge-in-phishing-scheme, January 17, 2018

- **Update software.** Keep operating systems updated to the latest version and install any security patches. Do not 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. Ensure that security software such as antivirus, malware protection, and desktop firewall software is patched and updated to avoid the latest cybersecurity threats.

- **Security audits.** Periodically assess security measures around a firm's IT systems to confirm that they fall within the guidelines of a baseline program established by the firm. This can be performed internally and externally—external or third-party audits of IT systems include risk identification and performing tests of compliance and fitness of IT systems.

- **Monitor problems.** Implement a security monitoring system to provide alerts of any potential issues to respond promptly. Security monitoring should include intrusion prevention/detection systems and a review of security logs from servers, databases, critical software applications, and firewalls. Security monitoring and alerting should be automated if possible, and studies of the alerts should be conducted in near-real/real time. Many firms choose to outsource security monitoring to third-party organizations that specialize in this service.

Client Assessment: Cybersecurity Service Opportunities

The AICPA makes available to accounting professionals a number of tools that can be used to enhance the range of services that can be provided to clients. One such tool is the Client Assessment: Cybersecurity Service Opportunities tool. This tool is used to generate engagement with the client to assess how your firm can help them enhance their security efforts.

You might be asking yourself, "Why would a CPA or accounting firm get involved in cybersecurity issues and what do CPAs have to offer in this regard?" The AICPA Guide to Cybersecurity describes five compelling reasons why it makes sense for CPA firms to provide cybersecurity capabilities and advice:

1. CPAs are risk specialists. 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.

3. CPAs offer perspectives about how cybersecurity considerations fit with other business risks.

4. 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. CPAs are required to implement controls related to data security to protect client files. It is important for CPAs to remind the clients of the importance of labeling and protecting sensitive

information and to suggest and evaluate appropriate cybersecurity controls over such data.

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

6. 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 role in which they must decide how to direct company resources toward things like cybersecurity. CPA firms that offer cybersecurity services can provide the C-level CPA with a resource that can speak the right language to assist in making a business case for investment in cybersecurity resources.

The instructions of the tool are as follows:

> Below is a list of questions firms can ask a client or prospect regarding the organization's information security efforts. Checkmarks in cells under the cybersecurity services indicate the potential services a firm could provide to the client based on the client's answer and their specific situation. Column F indicates the client response that would potentially invoke service opportunities. This list is not all-inclusive and is intended as a guide to aid in preparation for the client/prospect meeting and assist the practitioner in determining the most applicable opportunities for each client's need. For a description of the opportunities, refer to the Cybersecurity Service Opportunity Grid, a separate document in the toolkit.

Client/Prospect Name:

Date of Discussion:

To use:
Review the questions in column B with clients and/or prospects.
Per discussions with clients/prospects, enter "Yes" or "No" in column D.

Questions to ask a client or prospect that could indicate a need for security services:	Client/Prospect Answer:	Applicable Answer:	Assessment Services: System and Organization Controls (SOC 1® / SOC 2® / SOC 3® / SOC for Cybersecurity)	Payment Card Industry Data Security Standard (PCI DSS)	HITRUST CSF	Sarbanes-Oxley IT Control Assessments	FedRAMP Third Party Assessor Organization Cloud Security Assessment	FISMA Security Assessments	IT Internal Audit Co-Sourcing/Outsourcing	Cybersecurity Services: Security Consulting: Information Security Program Design	Information Security Policy Development	Information Security Risk Assessment	Data Classification Process Design and Consulting	HIPAA Security Assessment	Attack & Penetration Testing	Application Security Assessments	Technical Vulnerability Assessments	User Lifecycle Management Consulting	Database Security Assessments	Social Engineering Assessments	Security Incident Response Program Development and Testing	Security Forensic Analysis	Disaster Recovery Plan Consulting	Business Continuity Plan Consulting	Information Security Awareness Training
Does your organization store, process, or transmit sensitive data?		Yes								✓	✓	✓	✓		✓		✓		✓	✓	✓				✓
Does your organization have a contractual obligation to implement security controls?		Yes								✓	✓	✓										✓			✓
Has your organization signed a business associate agreement?		Yes									✓	✓	✓	✓								✓			✓
Does your organization provide IT services to clients?		Yes		✓							✓	✓	✓		✓	✓	✓	✓							
Does your organization accept credit cards as a method of payment?		Yes			✓						✓	✓	✓		✓	✓	✓					✓			✓
Does your organization have to comply with HIPAA?		Yes				✓					✓	✓	✓	✓				✓				✓			✓
Does your organization have to comply with PCI?		Yes			✓						✓	✓	✓		✓	✓	✓					✓			✓
Does your organization do any business with the US government?		Yes					✓	✓			✓	✓	✓	✓				✓							✓
Do you have any clients or business partners asking about your security posture?		Yes		✓								✓			✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
Have any of your clients or business partners sent you a security questionnaire to complete and return?		Yes		✓		✓					✓	✓	✓	✓	✓	✓	✓	✓		✓		✓			✓
Is your organization publicly traded or expecting to go public in the future?		Yes								✓	✓	✓						✓	✓					✓	✓
Are you a cloud hosting provider?		Yes		✓			✓				✓	✓	✓		✓	✓	✓	✓							✓
Is your organization in the healthcare industry?		Yes				✓					✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓
Is your organization in the financial services industry?		Yes									✓	✓	✓		✓	✓	✓	✓		✓	✓	✓			✓

Questions to ask a client or prospect that could indicate a need for security services:	Client/Prospect Answer:	Applicable Answer:	Assessment Services: System and Organization Controls (SOC 1® / SOC 2® / SOC 3® / SOC for Cybersecurity)	Payment Card Industry Data Security Standard (PCI DSS)	HITRUST CSF	Sarbanes-Oxley IT Control Assessments	FedRAMP Third Party Assessor Organization Cloud Security Assessment	FISMA Security Assessments	IT Internal Audit Co-Sourcing/Outsourcing	Cybersecurity Services: Security Consulting: Information Security Program Design	Information Security Policy Development	Information Security Risk Assessment	Data Classification Process Design and Consulting	HIPAA Security Assessment	Attack & Penetration Testing	Application Security Assessments	Technical Vulnerability Assessments	User Lifecycle Management Consulting	Database Security Assessments	Social Engineering Assessments	Security Incident Response Program Development and Testing	Security Forensic Analysis	Disaster Recovery Plan Consulting	Business Continuity Plan Consulting	Information Security Awareness Training
Have you ever had a data security breach (that you are aware of)?		Yes or No										✓			✓	✓					✓				
Have any of your computer systems been infected with ransomware?		Yes or No										✓			✓					✓	✓				✓
Does your organization have written information security policies?		Yes or No									✓						✓	✓							✓
Has your organization ever conducted a security risk assessment?		Yes or No										✓				✓	✓		✓	✓					
Has your organization ever had a penetration test on your IT systems?		Yes or No													✓	✓	✓		✓		✓				
Do you have an Internal Audit function?		Yes or No							✓			✓						✓				✓			
Do you train your employees on their responsibilities for information security?		Yes or No									✓								✓	✓					✓
Do you evaluate your organization's susceptibility to phishing emails?		Yes or No													✓				✓	✓					✓
Do you have a designated information security manager (or equivalent)?		No									✓		✓												
Do you have a current risk or your company's information security program?		No											✓				✓			✓					
Do you have a written information security program or policies?		No									✓		✓				✓	✓							✓
Does your management team understand the information security risks facing the organization?		No										✓			✓		✓								

The questions that are used to gather information about the client are as follows:

- Does your organization store, process, or transmit sensitive data?
- Does your organization have a contractual obligation to implement security controls?
- Has your organization signed a business associate agreement?
- Does your organization provide IT services to clients?
- Does your organization accept credit cards as a method of payment?
- Does your organization have to comply with HIPAA?
- Does your organization have to comply with PCI?
- Does your organization do any business with the U.S. government?
- Do you have any clients or business partners asking about your security posture?
- Have any of your clients or business partners sent you a security questionnaire to complete and return?
- Is your organization publicly traded or expecting to go public in the future?
- Are you a cloud hosting provider?
- Is your organization in the healthcare industry?
- Is your organization in the financial services industry?
- Have you ever had a data security breach (that you are aware of)?
- Have any of your computer systems been infected with ransomware?
- Does your organization have written information security policies?
- Has your organization ever conducted a security risk assessment?
- Has your organization ever had a penetration test on your IT systems?
- Do you have an Internal Audit function?
- Do you train your employees on their responsibilities for information security?
- Do you evaluate your organization's susceptibility to people-based attacks such as email phishing?
- Do you have a designated information security individual or department?
- Do you have a current list of your company's information security risks?

- Do you have a written information security program or plan?
- Does your management team understand the information security risks facing the organization?

The answer to each item leads to an opportunity to help the client and solicit a firm's service contract. On the right side of the form are assessment services and security consulting services that might be selected as appropriate to address each unaddressed concern.

Activity 2 – When Does the Principle Apply?

In this activity, assess each given scenario and identify the cybersecurity principle at work based on the scenario's controls.

After an employee was fired from a small company for defrauding the company by creating false invoices payable to himself and the organization decides to separate the accounts receivable and accounts payable functions (separation of duties).

A real estate firm recently suffered the theft of several laptops when the cleaning service mistakenly left the front door unlocked. After this occurred, a decision was made to install locks on all interior doors (defense-in-depth).

When a contractor's account was compromised with a phishing attack, the account was used to delete important client information by a malicious individual. After an account review process, the contractor's ability to delete data was removed (least privilege).

Final Review – Principles, Regulation, and Rules

The *Cybersecurity Threat Landscape* covers the cybersecurity landscape and recent breaches. The most problematic aspects of many of these breaches are as follows:

- Organizations have the resources and the means to prevent security breaches.
- Organizations need to apply the same amount of effort to prevent breaches as they do to manage the public relations response to a breach. There have been what many see as unacceptable delays in announcing these breaches. In some cases, the breach information was not disclosed for months—months during which untold damage can be done to those whose lives are affected.

We also discussed hackers and their motivations, and we found that they want one of four things:

- Financial gain
- Disruption
- Geopolitical change
- Notoriety

Later we explored data types that can be monetized or used to support attacks on data types that can be monetized. Those data types are as follows:

- Credit card data
- Personally identifiable information (PII)
- Trade secrets
- Personal financial information
- Personal health information (PHI)

To better understand the methods used, we also looked at types of attacks, including the following:

- Social engineering threats
  - Phishing
  - Pharming
  - Shoulder surfing
  - Identity theft
  - Dumpster diving
- Malicious software
  - Trojan horse
  - Virus
  - Rootkit
  - Worm
  - Spyware
- Rogue endpoints
  - Rogue access points
- General attacks on servers
  - DoS
  - DDoS
  - Buffer overflow

  - Mobile code
  - Emanations
  - Backdoor/trapdoor
- Network appliances
  - XSS scripting flaws
  - Interfaces with no protection against brute-force password cracking
  - Information about the product model and version that are exposed to unauthenticated users
  - Cross-site request forgery
  - Hidden backdoors
- Attacks on virtualization
  - VM escape
  - Data remnants
- Web servers
  - Maintenance hooks
  - Time-of-check/time-of-use attacks
  - Insecure direct object references
  - Cross-site scripting (XSS)
  - Cross-site request forgery (CSRF)
  - Click-jacking
  - Session takeover
- Database attacks
  - SQL injection

In *Cybersecurity State Regulatory and Legal Rules*, we covered cybersecurity laws and security frameworks. Among the federal and foreign laws and security frameworks we examined are the following:

- Sarbanes-Oxley (SOX) Act

- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA) of 1999
- Computer Fraud and Abuse Act (CFAA)
- Federal Privacy Act of 1974
- Computer Security Act of 1987
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Basel II
- Payment Card Industry Data Security Standard (PCI DSS)
- Federal Information Security Management Act (FISMA) of 2002
- Economic Espionage Act of 1996
- USA PATRIOT Act
- Health Care and Education Reconciliation Act of 2010

We also looked at state regulations that vary and change often.

All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have also enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information (security breach laws). Some have unique insurance, privacy, or safe harbor aspects, including South Carolina, California, and Ohio.

In *Limit Cybersecurity Risks by Applying Core Principles*, we learned about cybersecurity principles and when to apply them. Among the concepts we covered that should guide security efforts are as follows:

- CIA
- Defense-in-depth
- Job rotation
- Separation of duties
- Principle of least privilege
- Need-to-know principle

We also discussed recommendations from the AICPA as covered in the publication (AICPA's Introduction to Cybersecurity). These included the following:

- Conduct risk assessments

- Account for sensitive data
- Require strong passwords
- Update software
- Audit security measures
- Monitor problems

We also looked at the Client Assessment: Cybersecurity Service Opportunities form from the AICPA. This tool is used to generate engagement with the client to assess how your firm can help them enhance their security efforts.

Finally, we ended with five compelling reasons why it makes sense for CPA firms to provide cybersecurity capabilities and advice:

1. CPAs are risk specialists. CPA firms understand business and financial risk.
2. CPAs understand business. Accounting is the language of business.
3. CPAs realize the importance of securing their clients' information. CPA firms are regularly handling and processing sensitive information for their clients, such as tax returns, audit records, and Social Security numbers.
4. CPAs design, implement, and assess controls.
5. CPAs are often in company leadership positions.

Take Advantage of Diversified Learning Solutions

We are a leading provider of continuing professional education (CPE) courses to Fortune 500 companies across the globe, CPA firms of all sizes, and state CPA societies across the country, as well as CPA associations and other financial organizations. Our efficient and flexible approach offers an array of customized cutting-edge content to meet your needs and satisfy the priorities of your business. Select from live classes, live webinars, conferences, or online training, including Nano courses, based on your preferred method of learning.

Meet your CPE requirements, increase productivity, and stay up-to-date with relevant industry trends and mandatory regulations with collaborative live or online learning.

Live Training Topics	Online Training Topics
Accounting and Auditing	**Accounting and Auditing**
Employee Benefit Plans	**Business Law**
Ethics	**Business Management and Organization**
Information Technology	**Economics**
Governmental and Not-For-Profit	**Ethics**
Non-Technical (including Professional Development)	**Finance**
Tax	**Information Technology**
	Management Services and Decision Making
	Personal and Professional Development
	Tax

"We have enjoyed [your] programs and have found the content to be an excellent learning tool, not only for current accounting and management issues, but also how these issues apply to our company and affect how our business is managed."

—Debbie Y.

KAPLAN®