ACCOUNTING

CONTINUING EDUCATION

Advanced Cybersecurity Awareness in Accounting—What You Need to Know

(CYBA4)

KAPLAN

Advanced Cybersecurity Awareness in Accounting—What You Need to Know

(CYBA4)

Frank Castillo, CPA

KAPLAN®

ADVANCED CYBERSECURITY AWARENESS IN ACCOUNTING—WHAT YOU NEED TO KNOW (CYBA4)

Published in 2023 by Kaplan Financial Education.

Printed in the United States of America.

ISBN: 978-1-0788-3366-0

TABLE OF CONTENTS

NOTES

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, Unit 1 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. Notable data breaches that occurred during the last 10 years have involved 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, 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 (Intrusion Prevention System), IDS (Intrusion Detection System), and firewall systems mean NOTHING.

On that note, let’s review a “top 10” list for 2022, courtesy of Security Magazine.[1]

Top Data Breaches of 2022

10. SuperVPN, GeckoVPN, and ChatVPN Data Breach

A breach involving several widely used Android VPN services—SuperVPN, GeckoVPN, and ChatVPN—led to 21 million users having their information leaked. Full names, usernames, country names, billing details, email addresses, and randomly generated password strings were among the information available.

[1] https://www.securitymagazine.com/articles/98716-the-top-10-data-breaches-of-2022

9. Costa Rica Government Data Breach

In a high-profile cyberattack, the Conti ransomware gang breached the Costa Rican government. The threat group accessed the government's systems, stole highly valuable data, and demanded $20 million, forcing the Central American government to declare a state of emergency. A total of 670GB of data—or 90% of data accessed—was posted to a leak site weeks after.

8. Neopets Data Breach

In July, a database containing account information for 69 million users of the popular game Neopets was posted for sale on an online forum. Names, email addresses, zip codes, genders, and birth dates were among the available information. An investigation revealed that attackers had access to the Neopets IT systems from January 3, 2021, until July 19, 2022, a total of 18 months.

7. Twitter Data Breach

Twitter suffered a data breach that affected 5.4 million accounts, including phone numbers and email addresses. According to several reports, the data was collected in December 2021 using a Twitter API vulnerability disclosed in a bug bounty program that allowed people to submit phone numbers and email addresses into the API to retrieve the associated Twitter ID. Using this ID, the threat actors could then retrieve public information about the account to create a user record containing both private and public information.

6. Uber Data Breach

While the data breach occurred in 2016 and was revealed in 2017, Uber admitted it covered up a data breach that affected 57 million users. The rideshare company paid $100,000 to the threat actors to ensure the information wasn't made public. The security breach is highly significant—Joe Sullivan, Uber's former chief security officer, was found guilty of actively hiding the breach from the U.S. Federal Trade Commission (FTC) and concealing a felony. According to the Department of Justice (DOJ), Sullivan took several steps to prevent the FTC from finding out and arranged to pay off the hackers in exchange for them signing nondisclosure agreements. It is the first time an executive faces criminal prosecution for charges related to a data breach, and this could affect data breach reporting compliance.

5. Twilio Data Breach

U.S. messaging giant Twilio confirmed in August that cybercriminals accessed data that belonged to 125 customers after a phishing attack. The attackers tricked company employees into handing in login credentials by masquerading as IT department workers. Current and former employees recently reported receiving text messages purporting to be from the IT department. Typical text bodies suggested that the employee's passwords had expired, their schedule had changed, and they needed to log in to a URL the attacker controled. According to Twilio, other companies confirmed that they were subject to similar attacks and have coordinated a response to the threat actors, including collaborating with carriers to stop the malicious messages, registrars, and hosting providers to shut down the malicious URLs. The company confirmed that 209 customers—out of a total customer base of over 270,000—and 93 Authy end users—out of approximately 75 million total users—had accounts that were impacted by the incident. There is no evidence that the malicious actors accessed Twilio customers' console account credentials, authentication tokens, or API keys, the company said.

4. DoorDash Data Breach

In August, food delivery giant DoorDash confirmed a data breach involving 4.9 million customers, workers, and merchants that exposed personal information. In a blog post, the company, a third-party vendor, was the target of a sophisticated phishing campaign and certain personal information maintained by DoorDash was affected. DoorDash said the attackers accessed the names, email addresses, delivery addresses, and phone numbers of DoorDash customers. For a "smaller subset" of users, hackers accessed partial payment card information, including card type and the last four digits of the card number.

3. Optus Data Breach

In September, Australian telecommunications company Optus, which has 9.7 million subscribers, suffered a massive data breach that exposed names, dates of birth, phone numbers, and email addresses. A group of customers may have had physical addresses and personally identifiable information (PII) like driving licenses and passport numbers leaked. According to several reports, state-sponsored hacking groups or criminal organizations breached the company's firewall to obtain sensitive information.

2. LAUSD Data Breach

Russian-speaking hacking group Vice Society leaked 500GB of information from the Los Angeles Unified School District (LAUSD) after the U.S.'s second-largest school district failed to pay an unspecified ransom by October 4th. The data contains personal identifying information, including passport details, Social Security numbers and tax forms, contact and legal documents, financial reports with bank account details, health information, conviction reports, and psychological assessments of students.

1. Medibank Data Breach

Medibank Private Ltd, one of the largest health insurance providers in Australia, confirmed that data belonging to 9.7 million past and present customers, including 1.8 million international customers, had been accessed by an unauthorized party. Medibank said it would *not* pay the ransom demands, saying, "We believe there is only a limited chance paying a ransom would ensure the return of our customers' data and prevent it from being published."

> ***COMMENTARY***
>
> 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 “CIA,” which is the acronym for Confidentiality, Integrity, and Availability.
- **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.

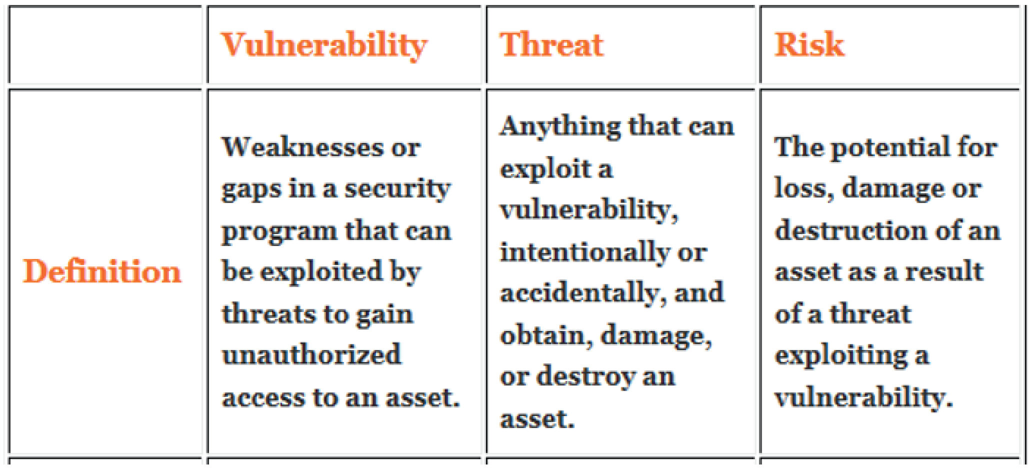
Examples of the threat actors include both internal and external actors and include the following:

- Internal actors
  - Government spy
  - Vendor/subvendors (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.



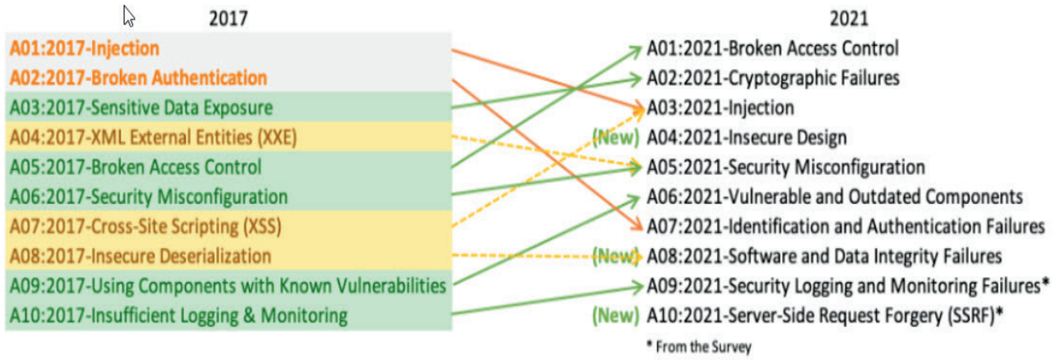
	Vulnerability	Threat	Risk
Definition	Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.	Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.	The potential for loss, damage or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

Vulnerabilities

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/).

OWASP Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021 (current version).


2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

A01:2021-Broken Access Control moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.

A02:2021-Cryptographic Failures shifts up one position to #2, previously known as Sensitive Data Exposure, which was a broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography, which often leads to sensitive data exposure or system compromise.

A03:2021-Injection slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.

A04:2021-Insecure Design is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.

A05:2021-Security Misconfiguration moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.

A06:2021-Vulnerable and Outdated Components was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.

A07:2021-Identification and Authentication Failures was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.

A08:2021-Software and Data Integrity Failures is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.

A09:2021-Security Logging and Monitoring Failures was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.

A10:2021-Server-Side Request Forgery is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

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 unique 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). California's new privacy law, the Consumer Privacy Rights Act ("CPRA"), includes PII category updates and an additional class of PII, which is defined as "sensitive PII."

  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.

- **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 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.

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 https://www.cpaportal.com/security, the actual HTML code in the email directs James to a different site (https://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.

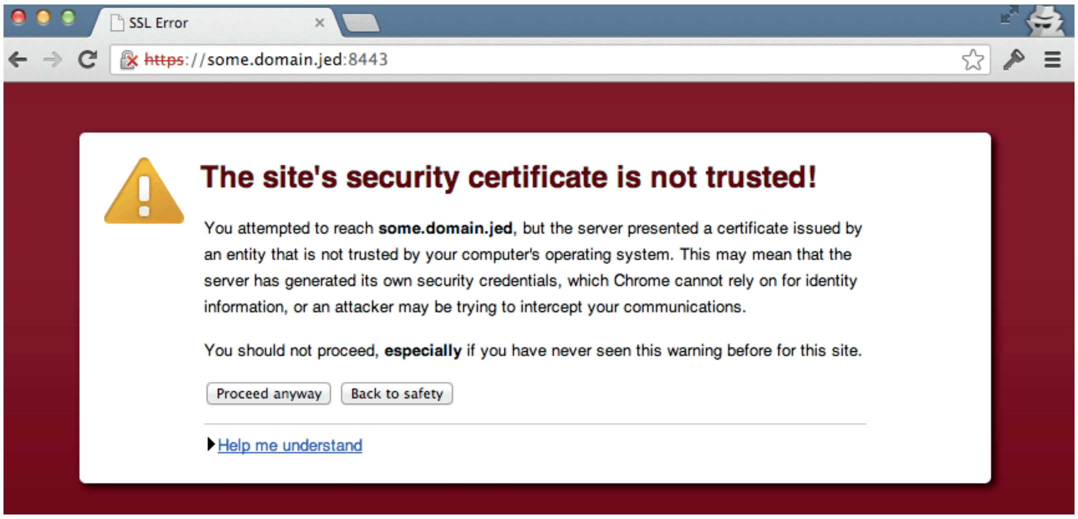
  It may be useful to think of DNS as being like the contacts application on your phone. You can dial your son, Harry, by just telling the phone to call Harry. What the phone does is look up Harry in your contacts list and then send the carrier the actual number that must be dialed to reach Harry. Pharming 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/



The site's security certificate is not trusted!

You attempted to reach **some.domain.jed**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

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://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. TLS 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.

- **Pretexting.** Pretexting is a type of social engineering technique where the attacker creates a scenario where the victim feels compelled to comply under false pretenses. Typically, the attacker will impersonate someone in a powerful position to persuade the victim to follow their orders. During this type of social engineering attack, a bad actor may impersonate police officers, higher-ups within the company, auditors, investigators, or any other persona they believe will help them get the information they seek.
- **Baiting.** Baiting puts something enticing or curious in front of the victim to lure them into the social engineering trap. A baiting scheme could offer a free music download or gift card in an attempt to trick the user into providing credentials. A social engineer may hand out free USB drives to users at a conference. The user may believe they are just getting a free storage device, but the attacker could have loaded it with remote access malware, which infects the computer when plugged in.
- **Tailgating.** Tailgating is a simplistic social engineering attack used to gain physical access to access an unauthorized location. Tailgating is achieved by closely following an authorized user into the area without being noticed by the authorized user. An attacker may tailgate another individual by quickly sticking their foot or another object into the door right before the door is completely shut and locked.
- **Piggybacking.** Piggybacking is exceptionally similar to tailgating. The main difference between the two is that, in a piggybacking scenario, the authorized user is aware and allows the other individual to "piggyback" off their credentials. An authorized user may feel compelled by kindness to hold a secure door open for a woman holding what appears to be heavy boxes or for a person claiming to be a new employee who has forgotten his access badge.

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 general 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 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]

[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

[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

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

Additional threats include:[5]

- ***Adware:*** unwanted software that displays advertisements on your screen. Adware collects personal information from you to serve you with more personalized ads.
- ***Ransomware:*** designed to encrypt your files and block access to them until a ransom is paid.
- ***Keyloggers:*** keep track of your keystrokes on your keyboard and record them on a log. This information is used to gain unauthorized access to your accounts.

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.

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.

[5] https://www.titanfile.com/blog/types-of-computer-malware/

> 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.

Recent threats and statistics for 2022:

- – A 26 million request per second HTTPS DDoS attacks that Cloudflare automatically detected and mitigated.
- – Attacks against Ukraine and Russia continue. Broadcast Media companies in the Ukraine were the most targeted in Q2 by DDoS attacks. In fact, all the top five most attacked industries are all in online/Internet media, publishing, and broadcasting.
- – Application-layer DDoS attacks are on the rise. Organizations in the US were the most targeted, followed by Cyprus, Hong Kong, and China.

> **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.[6]

- **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.

[6] "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

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 (2021) update from the National Institute of Standards and Technology (NIST) for both general industry and ePHI (electronic protected health information).

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.[7] 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.[8] When systems sharing these resources

[7] 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

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

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 VM (by modifying the VM virtual memory), the attacker can affect all the VMs, hypervisor, and potentially other programs on that machine.
- **Data remanence.** 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 ("TOCTOU" 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 personal 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.

Recent Legislation

On June 21, 2022, U.S. President Joe Biden signed two cybersecurity bills into law. The latest in a series of efforts to improve the nation's cybersecurity, the new legislation is intended to build skills and experience among the federal cyber workforce and promote coordination on security issues at all levels of government.

The State and Local Government Cybersecurity Act of 2021 is designed to improve coordination between the Cybersecurity and Infrastructure Security Agency (CISA) and state, local, tribal, and territorial governments. Under the new law, these bodies will be able to share security tools, procedures, and information more easily.

Under the second new cybersecurity law, the Federal Rotational Cyber Workforce Program Act of 2021, U.S. government employees in IT, cybersecurity, and related fields will be able to rotate through roles across agencies, enabling them to gain new skills and experience in a variety of job functions.

Cybersecurity Act of 2015

On December 18, 2015, President Obama signed into law a $1.1 trillion omnibus spending bill that contained the Cybersecurity Act of 2015 (the "Act"), a compromise bill based on competing cybersecurity information sharing bills that passed the House and Senate earlier this year. The Act creates a voluntary cybersecurity information sharing process designed to encourage public and private sector entities to share cyber threat information.

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 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 Personal Information Protection and Electronic Documents Act (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. PIPEDA was updated in 2021 in several areas that include: guidelines for obtaining meaningful consent, enhanced breach reporting requirements, more robust safeguards over data, and new policy statements relating to online behavioral advertising.

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 was rolled out by the Basel Committee on Banking Supervision—then a consortium of central banks from 28 countries, shortly after the credit crisis of 2008. Although the voluntary implementation deadline for the new rules was originally 2015, the date for implementation stood at January 1, 2022. The Basel III reforms have now been integrated into the consolidated Basel Framework.[9]

PCI DSS ("PCI")

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.

The PCI SSC released version 4.0 at the end of March 2022, although PCI DSS v3.2.1 will remain active for two years through March 2024. And the period of transition to when PCI 4.0 goes into full vigor in March 2025 is already underway.[10]

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.

[9] https://www.bis.org/bcbs/basel3.htm

[10] https://www.ispartnersllc.com/blog/pci-dss-version-4-0-launching-2020/#:~:text=is%20currently%20moving.-,PCI%204.0%20Compliance%20Date%3A%20March%2031%2C%202025,March%202025%20is%20already%20underway!

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.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere (including the United States), so long as they target or collect data related to citizens or residents (data subjects) of the countries that are in the EEA (European Economic Area).

The regulation went into effect on May 25, 2018. The GDPR levies harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

Brazil's General Law for the Protection of Personal Data (LGPD)

Brazil's data protection law (*Lei Geral de Proteção de Dados Pessoais* in Portuguese, or LGPD) came into effect in 2020. It contains provisions similar to the GDPR and aims to regulate the treatment of personal data of all individuals or natural persons in Brazil. That means, like the GDPR, even if your company isn't based in Brazil, if you process the data of Brazilian residents, it applies to you.

Companies and groups that do not follow the law's terms and directives may receive a fine such as 2% of their sales revenue, or even up to $50 million Brazilian Real (approximately $12 million USD).

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.[11]

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 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

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

> 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.

On March 9, 2022,[12] the Securities and Exchange Commission (SEC) proposed rules that would require public companies to make prescribed cybersecurity disclosures. The proposed rules would "strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting" by requiring:

(i). mandatory, material cybersecurity incident reporting, including updates about previously reported incidents; and

(ii). mandatory, ongoing disclosures on companies' governance, risk management, and strategy with respect to cybersecurity risks, including board cybersecurity expertise and board oversight of cybersecurity risks.

The proposed rules, if adopted, would codify and further expand on the SEC's previously issued interpretive guidance from 20113 and 2018,4 in which the SEC provided its views on how existing disclosure obligations would apply to cybersecurity risks and incidents, and how cybersecurity is a key element of enterprise risk management. The proposed rules also reflect the SEC's move toward a more prescriptive rule-making approach and away from the prior administration's principles-based approach. The public comment period for the proposed rules will remain open for 30 days following publication of the proposing release in the Federal Register or until May 9, 2022, whichever period is longer.

In explaining its approach to the proposed rules, the proposing release highlighted that current disclosures on cybersecurity risks and incidents remain "inconsistent, may not be timely, and can be difficult to locate." Given the increasing prevalence of cybersecurity incidents and attacks, as well as the significant impact such an attack may have on a company, the SEC believes "[c]onsistent, comparable, and decision-useful disclosures" would allow investors to better evaluate companies' "exposure to cybersecurity risks and incidents as well as their ability to manage and mitigate those risks and incidents."

The proposed rules evidence the SEC's continued focus on cybersecurity risk after several high-profile incidents and increasing cybersecurity attacks. In 2021, for example, the SEC charged at least two issuers with cybersecurity-related violations, demonstrating the shift to a more aggressive enforcement posture.

State Regulations: Privacy Law Updates

The U.S. has hundreds of sectoral data privacy and data security laws among its states. U.S. state attorney generals oversee data privacy laws governing the collection, storage, safeguarding, disposal, and use of personal data collected from their residents, especially regarding data breach notifications and the security of Social Security numbers. Some apply only to governmental entities, some apply only to private entities and others apply to both.

In addition to sectoral privacy laws, the U.S. is experiencing a massive push toward privacy legislation at the state level. That's because the federal government hasn't been able to find consensus on how to legislate broadly. Rather than wait, state lawmakers have felt pressure from consumers, consumer advocates, and even businesses to set their own rules. Of course, businesses would rather comply with one single federal standard than hire an attorney to look at every single statewide statute with which they must comply.

[12] https://www.sec.gov/rules/interp/2018/33-10459.pdf

California started the domino effect. While it's true that only one other state has been able to pass a comprehensive law to date, many states are trying. Even if their early bills have failed in previous legislative sessions, they serve as a reference point for where Republicans and Democrats agree to what must be amended before any deal can reach its final destination: the governor's desk.

Here's a breakdown of where things stand.[13]

California Consumer Privacy Act (CCPA)

The most comprehensive state data privacy legislation to date is the California Consumer Privacy Act (CCPA). Signed into law on June 28, 2018, it went into effect on January 1, 2020. The CCPA is cross-sector legislation that introduces important definitions and broad individual consumer rights and imposes substantial duties on entities or persons that collect personal information about or from a California resident. These duties include informing data subjects when and how data is collected and giving them the ability to access, correct, and delete such information. This notice must be disclosed in a privacy policy displayed on the entity's website that collects the data.

California Privacy Rights Act (CPRA)

The CPRA added the following to the CCPA:

- Right to rectification: This updates and adds to a consumer's right to correct inaccurate personal information.
- Right to restriction: This grants consumers the right to limit the use and disclosure of their sensitive personal information.
- Sensitive personally identifiable information: This updates the definition of personal information. Certain types of information, like a consumers' Social Security number, must be treated with special protections.

The CPRA also:

- Increases fines for breaches of children's data threefold.
- Expands breach liability beyond breaches of unencrypted data to disclosures of credentials (like an email address or password) that could lead to access to a consumers' account.
- Limits the duration of time a company may retain a consumers' information to only what's necessary and "proportionate" to the reason it was collected in the first place.
- Requires companies using third-party vendors to mandate contractually that those third parties exercise the same level of privacy protection to data shared with them as the first party.

The California Privacy Protection Agency will be empowered to fine transgressors, hold hearings about privacy violations, and clarify privacy guidelines. It's a five-member board, and it starts enforcing 6 months after the CPRA goes into effect on January 1, 2023.

[13] https://www.osano.com/articles/data-privacy-laws

Virginia's Consumer Data Protection Act (CDPA)

Virginia's Consumer Data Protection Act (CDPA) was passed on March 2, 2021. It grants Virginia consumers rights over their data and requires companies covered by the law to comply with rules on the data they collect, how it's treated and protected, and with whom it's shared.

The law contains some similarities to the EU General Data Protection Regulation's provisions and the California Consumer Privacy Act. It applies to entities that do business in Virginia or sell products and services targeted to Virginia residents and also do one of the following:

- Control or process the personal data of 100,000 or more consumers.
- Control or process the personal data of at least 25,000 consumers and earn 50% of their revenue by selling personal information.

The CDPA requires companies covered by the law to assist consumers in exercising their data rights by obtaining opt-in consent before processing their sensitive data, disclosing when their data will be sold, and allowing them to opt-out of it. It also requires companies to provide users with a clear privacy notice that includes a way for consumers to opt out of targeted advertising.

The CDPA becomes effective the same day as California's latest privacy law, the CPRA, which replaces its former iteration, the CCPA, on January 1, 2023. It's likely lawmakers will amend the law before then.

Colorado Privacy Act (CPA)

In June 2020, Colorado became the third U.S. state to pass a comprehensive privacy law. The Colorado Privacy Act grants Colorado residents rights over their data and places obligations on data controllers and processors. It contains some similarities to California's two privacy laws, the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), as well as Virginia's recently passed Consumer Data Protection Act (CDPA). It even borrows some terms and ideas from the EU's General Data Protection Regulation.

While there are similarities, such as some form of a right to opt-out, special protections for sensitive data and the adoption of some privacy-by-design principles, the significant differences are in the details.

The CPA applies to businesses that collect personal data from 100,000 Colorado residents or collect data from 25,000 Colorado residents and derive a portion of revenue from the sale of that data.

The law lists five rights granted to Colorado residents once the law becomes effective. They are:

1. The right to opt-out of targeted ads, the sale of their personal data or being profiled.
2. The right to access the data a company has collected about them.
3. The right to correct data that's been collected about them.
4. The right to request the data collected about them is deleted.
5. The right to data portability (that is, the right to take your data and move it to another company).

There are also 17 blanket exemptions within the law.

New York SHIELD Act

In July 2019, New York passed the Stop Hacks and Improve Electronic Data Security (SHIELD) Act. This law amends New York's existing data breach notification law and creates more data security requirements for companies that collect information on New York residents. The SHIELD Act went into effect in March of 2020. This law broadens the scope of consumer privacy and provides better protection for New York residents from data breaches of their personal information.

Utah Consumer Privacy Act[14]

The Utah Consumer Privacy Act (UCPA) is Utah's new data privacy law. Passed on March 25, 2022, the UCPA is slated to go into effect on December 31, 2023.

It lays out obligations for businesses that process personal data and data rights for Utah citizens.

In its overall framework, the Utah's data privacy bill is quite similar to the Colorado Privacy Act (CPA) and the Virginia Consumer Data Protection Act (VCDPA). That said, there are some notable differences, which we'll cover in greater detail as follows.

To be subject to the Utah Consumer Privacy Act, an entity (business or other organization) must:

- Have an annual revenue of at least $25 million
- Do business in Utah or market their product/service to Utah residents

Additionally, the entity must either:

- Process or control the data of at least 100,000 Utah residents OR
- Derive at least half its gross revenue from the sale of personal data and control the data of at least 25,000 consumers

The Connecticut Data Privacy Act (CTDPA)15

The Connecticut Data Privacy Act (CTDPA) was passed on May 10, 2022, and will go into force on July 1, 2023.

The CTDPA is similar in scope to other state privacy laws but, notably, it lacks an annual revenue threshold and exempts data that's only used for payment transactions.

To prepare for CTDPA compliance, businesses will need to implement a way to manage consent, fulfill privacy requests, and field consumer appeals. If engaging in risky data processing activities, they'll also need to conduct a data protection assessment.

Like all privacy laws, the first thing organizations should consider is whether or not they fall under the bill's scope. The first threshold for Connecticut's new privacy law is that an organization must do business in Connecticut (CT) or market goods or services to CT residents.

Additionally, the organization must:

- Collect, store, or sell personal data for 100,000 or more CT consumers (unless that data is only used in the context of payment transactions) OR

[14] https://transcend.io/blog/utah-consumer-privacy-act/

[15] https://iapp.org/news/a/connecticut-enacts-comprehensive-consumer-data-privacy-law/

- Process personal data for 25,000 of more consumers AND receive over 25% of annual gross revenue from selling personal data

Making payment transaction data exempt is one key way the CTDPA differs from other state privacy laws. This stipulation means that as long as businesses only use data from credit or debit card sales in that context (and they aren't processing data in other ways), the CTDPA doesn't apply.

Data Protection

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 always significant exposure for an unencrypted laptop, thumb drive, backup drive, smart phone, or similar device if it is lost or stolen. Let's look at an example of potential data loss in an Ohio location and then continue with a second data loss situation example:

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. 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 Private Companies Practice Section (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 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:

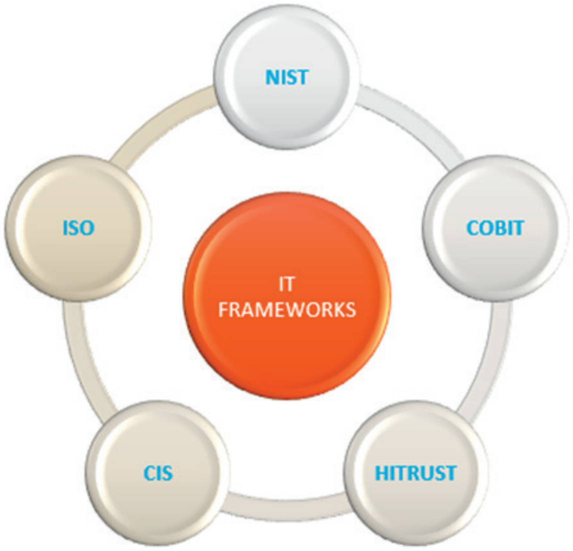
- Keep the number of administrative accounts to a minimum
- Administrators should use normal user accounts when performing routine operations

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.

Top Security Frameworks



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. COBIT 5 was published in 2012, and to include new technology and business trends in information and technology (I&T) such as digitization. COBIT 5 was updated to COBIT 2019 to incorporate these enhancements.

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. ISO 27001 is the central framework of the ISO 27000 series, which is a series of documents relating to various parts of information security management. ISO 27001 was last updated in 2022.

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 most recent version of NIST 800-53 is Revision 5. The Department of Defense (DOD) utilizes 800-171 to set standards for vendor and supplier compliance. NIST 800-171 is often used with the CMMC (Cybersecurity Maturity Model Certification) framework to carry out a security control assessment.

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.

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.[16]

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.[17]

- **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).
- **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.

[16] 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

[17] "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

Client Assessment: Cybersecurity Service Opportunities

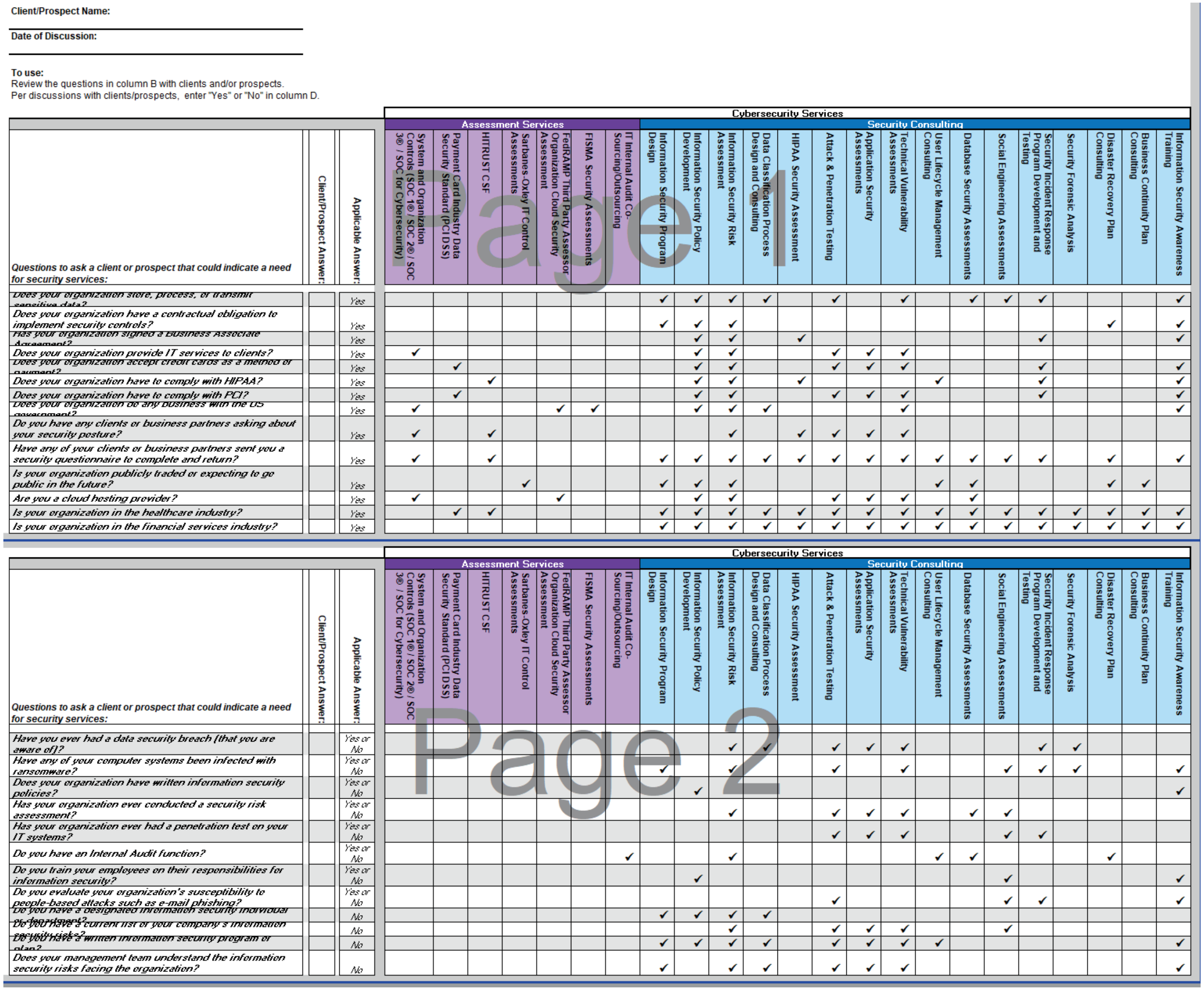
The AICPA makes available to accounting professionals a number of tools that can be used to enhance the range of services that can be provided to clients. One such tool is the Client Assessment: Cybersecurity Service Opportunities tool. This tool is used to generate engagement with the client to assess 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 several 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 to help offer perspective about how cybersecurity considerations fit with other business risks.
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.

			Cybersecurity Services																						
			Assessment Services							Security Consulting															
Questions to ask a client or prospect that could indicate a need for security services:	Client/Prospect Answer:	Applicable Answer:	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	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*								✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

			Cybersecurity Services																						
			Assessment Services							Security Consulting															
Questions to ask a client or prospect that could indicate a need for security services:	Client/Prospect Answer:	Applicable Answer:	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	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 people-based attacks such as e-mail phishing?		*Yes or No*													✓					✓	✓				✓
Do you have a designated information security individual or department?		*No*								✓	✓	✓	✓												
Do you have a current list of your company's information security risks?		*No*										✓			✓	✓	✓			✓					
Do you have a written information security program or plan?		*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
  - Pretexting
  - Baiting

  - Tailgating
  - Piggybacking
  - DeepFakes
- 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 remanence
- 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:

- The State and Local Government Cybersecurity Act of 2021
- Federal Rotational Cyber Workforce Program Act of 2021
- Cybersecurity Act of 2015
- 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 & III
- 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
- General Data Protection Regulation (GDPR)
- Brazil's General Law for the Protection of Personal Data (LGPD)

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 California, Virginia, Colorado, New York, 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.

NOTES

UNIT

2

Cybersecurity Risk Management and Assurance

LEARNING OBJECTIVES

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

- Describe the CPA responsibilities and AICPA's cybersecurity risk management framework.
- Provide reasonable assurance to third-party consultants and cloud providers.
- Discuss cybersecurity basics, risk management, and best practices.

Risk management allows organizations to identify, measure, and control organizational risks. Threat modeling will enable organizations to identify threats and potential attacks and implement the appropriate mitigations against these threats and attacks. These facets ensure that security controls that are implemented are in balance with the operations of the organization. Each organization must develop a well-rounded, customized security program that addresses the organization's needs while ensuring that the organization exercises due care and due diligence in its security plan.

This unit explains how to use risk management components to assess risks, implement controls for identified risks, monitor control effectiveness, and perform future risk assessments.

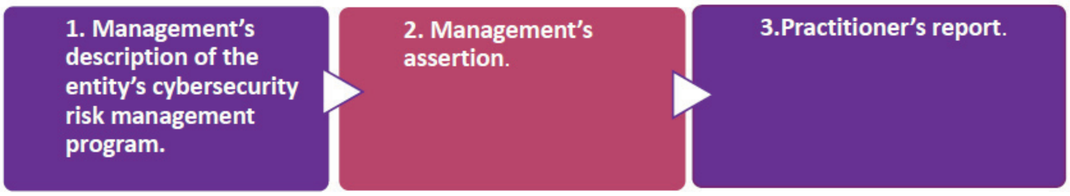
AICPA'S CYBERSECURITY RISK MANAGEMENT FRAMEWORK

The AICPA Cybersecurity Risk Management Reporting Framework is a flexible framework for organizations to take a proactive cybersecurity risk management approach. This framework is intended for management to design and describe its cybersecurity risk management program and is a critical component of the new **SOC for Cybersecurity engagement**. We will look at the **SOC for Cybersecurity** and use it to assess a fictitious organization.

The SOC for Cybersecurity (Below From SOC for Cybersecurity: Information for CPAs)

SOC for Cybersecurity is an examination engagement performed in accordance with the AICPA's clarified attestation standards on an entity's cybersecurity risk management program. A cybersecurity risk management examination results in the issuance of a general-use cybersecurity report designed to meet a variety of potential users' needs. The cybersecurity risk management examination report includes the following three key components as shown in Figure 2.1.

Figure 2.1: SOC for Cybersecurity


1. Management's description of the entity's cybersecurity risk management program.
2. Management's assertion.
3.Practitioner's report.

1. **Management's description of the entity's cybersecurity risk management program.** The first component is a management-prepared narrative description of the entity's cybersecurity risk management program. This description is designed to provide information about how the entity identifies its information assets, the ways in which the entity manages the cybersecurity risks that threaten it, and the key security policies and processes implemented to protect the entity's information assets against those risks. The description provides the context needed for users to understand the conclusions expressed by management in its assertion and by the practitioner in his or her report. Management uses the *description criteria* to prepare and evaluate an entity's cybersecurity risk management program.

Description Criteria

DC1: The nature of the entity's business and operations, including the principal products or services the entity sells or provides and the methods they distribute

DC2: The principal types of sensitive information created, collected, transmitted, used, or stored by the entity

DC3: The entity's principal cybersecurity risk management program objectives (cybersecurity objectives) related to availability, confidentiality, the integrity of data, and integrity of processing

DC4: The process for establishing, maintaining, and approving cybersecurity objectives to support the achievement of the entity's objectives

DC5: Factors that have a significant effect on the entity's inherent cybersecurity risks, including the:

- characteristics of technologies, connection types, use of service providers, and delivery channels used by the entity;
- organizational and user characteristics; and
- environmental, technological, organizational, and other changes during the period covered by the description at the entity and its environment

DC6: For security incidents that (1) were identified during the 12-month period preceding the period end date of management's description and (2) resulted in a significant impairment of the entity's achievement of its cybersecurity objectives, disclosure of the following: (a) nature of the incident; (b) timing surrounding the incident; and (c) extent (or effect) of these incidents and their disposition

DC7: The process for establishing, maintaining, and communicating integrity and ethical values to support the functioning of the cybersecurity risk management program

DC8: The process for board oversight of the entity's cybersecurity risk management program

DC9: Established cybersecurity accountability and reporting lines

DC10: The process used to hire and develop competent individuals and contractors and to hold those individuals accountable for their cybersecurity responsibilities

DC11: The process for (1) identifying cybersecurity risks and environmental, technological, organizational and other changes that could have a significant effect on the entity's cybersecurity risk management program and (2) assessing the related risks to the achievement of the entity's cybersecurity objectives

DC12: The process for identifying, assessing, and managing the risks associated with vendors and business partners

DC13: The process for internally communicating relevant cybersecurity information necessary to support the functioning of the entity's cybersecurity risk management program, including (1) objectives and responsibilities for cybersecurity and (2) thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents requiring a response, remediation, or both

DC14: The process for communicating with external parties regarding matters affecting the functioning of the entity's cybersecurity risk management program

DC15: The process for conducting ongoing and periodic evaluations of the operating effectiveness of key control activities and other components of internal control related to cybersecurity

DC16: The process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective actions, including management and the board of directors, as appropriate

DC17: The process for developing a response to assessed risks, including the design and implementation of control processes

DC18: A summary of the entity's IT infrastructure and its network architectural characteristics

> **DC19:** The key security policies and processes implemented and operated to address the entity's cybersecurity risks, including those addressing the following:
>
> - Prevention of intentional and unintentional security events
> - Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents
> - Management of processing capacity to provide for continued operations during security, operational, and environmental events
> - Detection, mitigation, and recovery from environmental events and the use of backup procedures to support system availability
> - Identification of confidential information when received or created, determination of the retention period for that information, retention of the information for the specified period, and destruction of the information at the end of the retention period

2. **Management's assertion.** The second component is an assertion provided by management, which may be as of a point in time or for a specified period of time. Specifically, the assertion addresses whether (a) the description is presented in accordance with the description criteria and (b) the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria. The AICPA has developed control criteria for use when evaluating whether the controls within the program were effective to achieve the entity's cybersecurity objectives.
3. **Practitioner's report.** The third component is a practitioner's report, which contains an opinion that addresses both subject matters in the examination. Specifically, the opinion addresses whether (a) the description is presented in accordance with the description criteria and (b) the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

Activity 3—SOC for Cybersecurity Example

In this activity, you will use the SOC for Cybersecurity process to review the XYZ Manufacturing Company. Read the assertion of compliance by management (Part 1) and the description of its cybersecurity program (Part 3) contained in the course Appendix *"Illustrative Cybersecurity Risk Management Report*" and present your group's assessment of the sufficiency with which the organization complies.

PERFORMING QUANTITATIVE RISK MANAGEMENT

Once the risk analysis team is formed, it is time to actually start the risk analysis or assessment process. This process includes two different types of risk analysis: quantitative risk analysis and qualitative risk analysis. We will discuss these two methods in the following sections.

Quantitative Risk Analysis

A quantitative risk analysis attempts to assign monetary and numeric values to all facets of the risk analysis process. Equations are used to determine the total cost of various vulnerabilities, were each vulnerability to result in a breach. The most common equations are for single loss expectancy (SLE) and annual loss expectancy (ALE).

SLE represents the cost of an adverse event, were the event to occur a single time. In many cases, the occurrence of an event does not leave the asset without value. Sometimes the event only reduces the value of the asset by a percentage of its value. For example, the occurrence of a flood might reduce the value of the building only by half (50%). The value is called the exposure factor (EF).

To determine the SLE, you must know the asset value (AV) and the exposure factor (EF). The EF is the percent value or functionality of an asset that will be lost when a threat event occurs. The calculation for obtaining the SLE is as follows:

$$\textbf{SLE} = \textbf{AV} \times \textbf{EF}$$

For example, an organization has a web server farm with an AV of $150,000. If the risk assessment has determined that a power failure is a threat for the web server farm and the exposure factor for a power failure is 30%, the SLE for this event equals $50,000.

Average loss expectancy (ALE) is a value that takes into consideration the frequency with which the threat event typically occurs and then attempts to spread the cost of a single occurrence across the number of years that come between occurrences. The frequency with which the threat event typically occurs is called the average rate of occurrence (ARO). The ARO is a percentage. To arrive at the percentage, divide the number of years between occurrences into 1. For example, if the event typically occurs once every 5 years, the ARO is 20% or .20 (1 divided by 5).

Once the ARO and the SLA are known, then the ALE can be determined.

The calculation for obtaining the ALE is as follows:

$$\textbf{ALE} = \textbf{SLE} \times \textbf{ARO}$$

Using the previously mentioned example, if the risk assessment has determined that the ARO for the power failure of the web server farm is 20%, the ALE for this event equals $10,000 ($50,000 X .20).

Knowing the ALE helps to prevent selecting a control that costs more than the adverse event itself, were it to occur. If the annual cost of the control to protect the web server farm is more than the ALE, the organization could easily choose to accept the risk by not implementing the control. If the annual cost of the control to protect the web server farm is less than the ALE, the organization should consider implementing the control.

Although a quantitative risk analysis uses numeric values, a purely quantitative analysis cannot be achieved because some level of subjectivity is always part of the data. For example, what certainty do you have that damage from the power failure will be 30% of the asset? This type of estimate should be based on historical data, industry experience, and expert opinion.

An advantage of quantitative over qualitative risk analysis is that quantitative uses less guesswork than qualitative. Disadvantages of quantitative risk analysis include the difficulty of the equations, the time and effort needed to complete the analysis, and the level of data that must be gathered for the analysis.

Qualitative Risk Analysis

Qualitative risk analysis does not assign monetary and numeric values. In this approach, subject matter experts assess each threat based on two things: impact of the event, were it to occur, and the likelihood that the event will occur. A scoring system of some sort is used for this. After each threat has been scored, the threats and their scores might be entered as what is called a threat/risk matrix. It is a table that lists each threat and its score on booth impact and likelihood. By combining these scores, the threats or issues can be prioritized with regard to which are most serious.

Qualitative risk analysis techniques rely on intuition, experience, and best practice techniques. The specific approach in use might include brainstorming, focus groups, surveys, questionnaires, meetings, interviews, and the Delphi technique. The quality of the output of this process depends on the knowledge and skill of the SMEs.

The threat data is combined in a report to present to management. All levels of staff should be represented as part of the qualitative risk analysis, but it is vital that some participants in this process should have some expertise in risk analysis.

Advantages of qualitative over quantitative risk analysis include qualitative risk analysis prioritizes the risks and identifies areas for immediate improvement in addressing the threats. Disadvantages of qualitative risk analysis include all results are subjective and a dollar value is not provided for cost-benefit analysis or for budget help.

Most risk analysis includes some hybrid use of both quantitative and qualitative risk analyses. Most organizations favor using quantitative risk analysis for tangible assets and qualitative risk analysis for intangible assets.

Return on Investment (ROI)

The term "return on investment" (ROI) refers to the money gained or lost after an organization makes an investment. ROI is a necessary metric for evaluating security investments.

ROI is used to determine if selecting an action (in this case a security control) provides more benefit than its cost. In the security field, reduction in risk is the goal. But it is often hard to determine exactly how much an organization will save if it makes an investment. Some of the types of losses that can occur include the following:

- **Productivity loss.** When systems are down, people cannot work and productivity goes down. This includes downtime and repair time.
- **Revenue loss during outage.** When assets are down, especially if those assets involve ecommerce, money is lost. The organization loses money with each minute and hour that the asset is down. If the issue is the internet, the effect increases exponentially because that affects all organizational assets.
- **Data loss.** Lost data must be restored and that takes time as well. This adds to productivity loss because personnel must restore the data backup. If conditions are such where backups are also destroyed, it could be catastrophic.
- **Data compromise.** When data is either disclosed or modified in an unauthorized fashion, it has been compromised. Intellectual data, especially, must be secured with measures to ensure that it is protected.
- **Repair costs.** In many situations, especially disasters, hardware is damaged. Costs to replace hardware or costs incurred to employ services from vendors add up quickly.
- **Loss of reputation.** Regardless of the outcome of an event, when these events become publicly known, it is damaging to the reputation of the company. Partners and customers will doubt the technical skill of the organization. Recent security breaches at popular retail chains have resulted in customer reluctance to trust the stores with their data.

Here's an example to better understand how ROI fits in the risk analysis process. Suppose two companies are merging. One company uses mostly hosted applications from an outside vendor, while the other uses mostly desktop applications installed locally. When the merging project is started, the following goals for the merged systems are set:

- Ability to customize systems at each location
- Quick implementation along with an immediate ROI
- Administrative-level control over all products by internal IT staff

One manager states that the local desktop applications are the best solution. The CIO argues that security will be best maintained by continuing to use outsourced applications because of a current staff shortage to support the desktop applications. The best way to resolve this issue is to:

1. Calculate the time to deploy and support local desktop application systems for the staff shortage.
2. Compare the costs to the ROI costs minus the costs of outsourcing applications.
3. Present the document numbers to management for a final decision.

There is a degree of uncertainty and subjectivity involved in calculating ROI, but the question of how to measure it should be somewhat easier. The most effective measures are likely to be those you already are using because they will enable you to compare security projects with all other projects. Two popular methods are payback and net present value (NPV).

Payback

Payback is a simple calculation that compares ALE against the expected savings as a result of an investment. Let's use the earlier example of the server that results in a $10,000 ALE. The organization may want to deploy a power backup if it can be purchased for less than $10,000. However, if that power backup costs a bit more, the organization might be willing to still invest in the device if it is projected to provide protection for more than one year with some type of guarantee.

Net Present Value (NPV)

Net present value (NPV) considers the fact that money spent today is worth more than savings realized tomorrow. In the previous example, the organization may purchase a power backup that comes with a five-year warranty. To calculate NPV, you need to know the discount rate, which determines how much less money is worth in the future. For our example, we'll use a discount rate of 15%. Now to the calculation: You divide the yearly savings ($10,000) by 1.15 (that is 1 plus the discount rate) to the power of the number of years you want to analyze. So this is what the calculation would look like for the first year:

$$\text{NPV} = \$10{,}000 \,/\, (1.15) = \$8{,}696 \text{ (rounded up)}$$

The result is the savings expected in today's dollar value. For each year, you could then recalculate NPV by raising the 1.15 value to the year number. The calculation for the second year would be:

$$\text{NPV} = \$10{,}000 \,/\, (1.15)^2 = \$7{,}165 \text{ (rounded up)}$$

If you're trying to weigh costs and benefits, and the costs are immediate but the benefits are long term, NPV can provide a more accurate measure of whether a project is truly worthwhile.

Total Cost of Ownership

While some risks are hard to anticipate and calculate, such as the loss of a key employee, risks are everywhere and not all can be addressed with insurance. Total cost of ownership (TCO) measures the overall costs associated with undergoing the organizational risk management process. Costs might include insurance premiums, financing, administrative costs, and any losses incurred.

TCO should be compared to the overall company revenues and asset base and provide a way to track an organization's risk-related costs over time as compared to the overall organization growth rate. It may also be helpful to compare TCO to industry baselines that are available from trade groups and industry organizations. Obtaining relevant and comparable risk-related data should be obtained from related business and industry experts. For example, a financial organization should not compare its risk TCO to TCOs of organizations in the healthcare field.

The advantages to calculating TCO are as follows:

- Discovering inconsistencies in their risk management approach
- Identifying areas where managing a particular risk is excessive as compared to similar risks managed elsewhere
- Generating direct cost savings by highlighting risk management process inefficiency

However, the most relevant risk TCO data, such as data on a direct competitor, is often difficult to find because many direct competitors protect this sensitive data. Trade bodies and industry standard bodies can often help alleviate this problem. Keep in mind that if the TCO process is viewed as a cost-cutting measure, it will meet resistance in some quarters.

Some of the guidelines an organization should keep in mind when determining risk TCO are as follows:

- Break down costs into categories including risk financing, risk administration, risk compliance costs, and self-insured losses in the framework.
- Express category costs as a percentage of overall organizational revenue.
- In each category, include data from trade bodies for comparison with each category's figures.
- Identify reasons for any differences between your organization's numbers and industry figures.
- Select target goals for each category.
- Remember these basic rules when calculating and analyzing risk TCO.
  - Don't overemphasize industry data. Industry benchmarks may not always be truly comparable to your organization's data.
  - Cover some minor risks within the organization.
  - The complex nature of risk management may call for risk management software to aid in decisions.
  - Stress risk management's importance in the budget process. It is not merely a cost.
  - Savings from the process (risk TCO) do not occur immediately. It occurs over time.
  - Some risk calls for outside help. External specialists and insurance brokers may be needed.

Approaches to Handling Risk

Risk reduction is the process of applying security measures or controls in response to risk analysis. This decision will rest partly on the organization's risk appetite or how much risk the organization can withstand on its own. There are four basic strategies:

1. **Avoid.** Avoiding is the process of halting the activity that is causing the vulnerability. The avoid strategy may also involve choosing an alternative that is not as risky. While not useful against all threats, in some cases, it is the perfect strategy. An example of avoidance is discontinuing the use of an application that is found to have a coding vulnerability.

   In some cases, this strategy may not be available to you. For example, you might have a web application that is found to have a coding vulnerability, but you can't discontinue the use of it now because it is making money for the organization and developing a new application or fixing bathe code will take time. In this case, you would need to find a way to mitigate it, perhaps by installing a web application firewall between the application and the internet.

   Consider the following scenario: A company is in negotiations to acquire another company for $64,000,000. Due diligence activities have uncovered systemic security issues in the flagship product of the company being purchased. A complete product rewrite because of the security issues is estimated to cost $10,500,000. In this case, the company is paying $74,500,000 for the other company. This might alter the decision to move forward and avoid the purchase.

2. **Transfer.** The transfer strategy passes the risk on to a third party, including insurance companies. While insurance is the clearest example of transferring, outsourcing certain functions to a provider would also be considered transferring *if* the service-level agreement (SLA) with a third party includes this provision. Otherwise, the risk could still rest with the original organization. Legal counsel should be used to ensure that the contract provides the level of protection needed.

   Consider the following scenario: A small business has decided to reduce costs by outsourcing the help desk. Initially, this will be run as a short-term trial. If it works, the system will be expanded and form part of the day-to-day business. Two main business risks for the initial trial have been raised:

   - Management has no experience with setting up offshore outsourcing.
   - Additional international laws and regulations must be considered by an organization that has no global experience.

   In this situation, it is best to transfer the initial risks by engaging a consulting company to handle the short-term setup and test.

3. **Mitigate.** This strategy selects a control or set of controls that while not eliminating the risk reduces the risk to a level that is acceptable to the company. This is the most common strategy employed and includes measures such as implementing intrusion detection systems (IDSs), intrusion prevention systems (IPSs) and firewalls.

   Consider the following scenario:

   Your company's database server experiences a security incident on average two times a year, costing the company $6,400 in downtime per occurrence. The database server is scheduled to be decommissioned in five years. The cost of implementing a database activity monitor (DAM) to reduce these incidents would be $46,000 initially, plus $2,000 a year for maintenance. The cost of the security incident is calculated as follows:

($6,400 per occurrence × 2 per year) × 5 years = $64,000

The cost to prevent the problem is calculated as follows:

$46,000 software cost + ($2,000 maintenance × 5 years) = $56,000

In this situation, the mitigation (implementing the software) is cheaper than accepting the risk.

4. **Accept.** This strategy amounts to making the decision to do nothing and live with the risk. Consider this example:

   Your company's firewall is aging and experiences an outage on average one time a year, costing the company $4,500 in downtime per occurrence. The firewall is scheduled to be decommissioned in two years. The cost of repairing the firewall to reduce these incidents would be $10,000. The cost of the security incident is calculated as follows:

   ($4,500 per occurrence × 1 time per year) × 2 years = $9,000

   The cost to prevent the problem is calculated as follows:

   $10,000 repair cost = $10,000

   In this situation, mitigation (repairing) is more expensive than accepting the risk.

REASONABLE ASSURANCE AND THIRD-PARTY RISKS

The more well-known security breaches that have occurred have resulted from a compromise of privileged accounts held by third-party contractors and vendors (the Target and Home Depot breaches, for example). We will look at the AICPA Professional Code of Conduct, Disclosing Information to a Third-Party Service Provide, and the use of the PCPS Cybersecurity Toolkit.

AICPA Professional Code of Conduct, Disclosing Information to a Third-Party Service Provider – As you learned earlier, most of the accountancy boards 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 the permission of each client would be helpful. The relevant requirement is found at 1.700.040 "Disclosing Information to a Third-Party Service Provider," which is on page 126 of the Code. It reads as follows:

> **1.700.040, Disclosing Information to a Third-Party Service Provider**
>
> **.01** – When a member uses a third-party service provider to assist the member in providing professional services, threats to compliance with the "Confidential Client Information Rule" [1.700.001] may exist.
>
> **.02** – Clients may not expect the member to use a third-party service provider to assist the member in providing the professional services. Therefore, before disclosing confidential client information to a third-party service provider, the member should do one of the following:
>
> Enter into a contractual agreement with the third-party service provider to maintain the confidentiality of the information and provide reasonable assurance that the third-party service provider has appropriate procedures in place to prevent the unauthorized

> release of confidential information to others. The nature and extent of procedures necessary to obtain reasonable assurance depends on the facts and circumstances, including the extent of publicly available information of the third-party service provider’s controls and procedures to safeguard confidential client information.
>
> Obtain specific consent from the client before disclosing confidential client information to the third-party service provider.
>
> **.03** – Refer to the “Use of a Third-Party Service Provider” interpretation [1.150.040] of the “Integrity and Objectivity Rule” [1.100.001] and the “Use of a Third-Party Service Provider” interpretation [1.300.040] of the “General Standards Rule” [1.300.001] for additional guidance. [Prior reference: paragraphs .001–.002 of ET section 391]

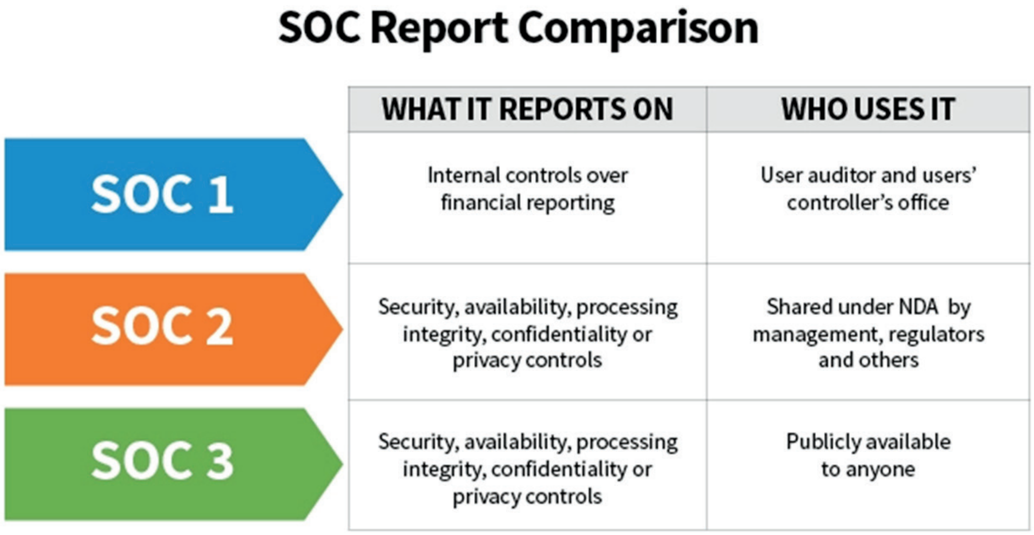
A nonauthoritative basis-for-conclusions document that summarizes considerations that were deemed significant in the development of this interpretation is available at www.aicpa.org/InterestAreas/ProfessionalEthics/Resources/Tools/DownloadableDocuments/BasisforConclusionsOutsourcing.pdf.

In addition, nonauthoritative sample client disclosure language that could be used to fulfill the requirement discussed in this interpretation is also available at http://www.aicpa.org/InterestAreas/ProfessionalEthics/Resources/Tools/DownloadableDocuments/Sample_Disclosure_Notification.pdf.

If the CPA makes use of a third-party service provider to assist the CPA in providing professional services (like a cloud service providing accounting systems and related items), that would trigger the requirements to have the written agreement and obtain “reasonable assurance” (a term that has a specific meaning in accounting literature—**it’s the level of assurance provided by an audit or SOC report**) that the third-party provider has adequate systems in place to prevent unauthorized disclosure (which necessarily includes unauthorized access to systems).

SOC Reports

Let’s look at five types of SOC reports. The first three have been around for some time.



SOC Report Comparison

	WHAT IT REPORTS ON	WHO USES IT
SOC 1	Internal controls over financial reporting	User auditor and users’ controller’s office
SOC 2	Security, availability, processing integrity, confidentiality or privacy controls	Shared under NDA by management, regulators and others
SOC 3	Security, availability, processing integrity, confidentiality or privacy controls	Publicly available to anyone

1. **SOC 1:**
   - What it reports on? Internal controls over financial reporting.
   - Who uses it? User auditors and users' controller's office.
2. **SOC 2:**
   - What it reports on—Security, availability, processing integrity, confidentiality, or privacy controls.
   - Who uses it? Management, regulators, and others. Shared under NDA (Nondisclosure Agreement).
3. **SOC 3:**
   - What it reports on—Security, availability, processing integrity, confidentiality, or privacy controls.
   - Who uses it? Publicly available to anyone.
4. **(SOC) for Cybersecurity:**

   To address a market need, the AICPA has developed a cybersecurity risk management reporting framework that assists organizations as they communicate relevant and useful information about the effectiveness of their cybersecurity risk management programs. The framework is a key component of a new System and Organization Controls (SOC) for cybersecurity engagement, through which a CPA reports on an organization's enterprise-wide cybersecurity risk management program. This information can help senior management, boards of directors, analysts, investors and business partners gain a better understanding of organizations' efforts.

   The SOC for Cybersecurity is covered earlier. The SOC for Cybersecurity (below from SOC for Cybersecurity: Information for CPAs).
5. **SOC for Supply Chain:**

   This newly added member of the SOC Reporting family is a risk management and reporting framework which tests controls relating to vendors and third-party suppliers.

PCPS Cybersecurity Toolkit

The AICPA's PCPS (Private Companies Practice Section) Cybersecurity Toolkit is a collection of learning resources, staff training tools, and tools to use with clients to assess their needs for cybersecurity services. Together, these tools will help your firm analyze your service opportunities and assist in building a cybersecurity practice.

The toolkit includes many of the documents we have discussed and utilized in class already. Specifically, it includes (from the AICPA website):

- **Tool for Understanding Cybersecurity**

  A CPA's Introduction to Cybersecurity **(for AICPA members)**
  This guide provides a general overview of cybersecurity. What is it? What are the threats to your firm and your clients? And what best practices should your firm implement to protect against cyber threats?

  Learning Matrix **(for AICPA members)**
  Cybersecurity is comprised of numerous facets. Learn more about the key areas as well as the resources available for further research.

Service Opportunity Grid **(for AICPA members)**
Numerous service opportunities relate to cybersecurity. Consider which of these opportunities may fit with your firm by reviewing the key considerations of each opportunity.

Cybersecurity PowerPoint **(for PCPS members)**
Host an internal meeting for your staff on the basics of cybersecurity, why it's important and how your firm is approaching the applicable issues. Use this template for your firm's practices and to share cybersecurity basics with your clients.

Client FAQs **(for PCPS members)**
Help your clients address some of the top cybersecurity questions they may have with this co-brandable FAQ document.

- **Tools for Implementation Considerations**

  Service Implementation Checklist (for PCPS members).

  Interested in implementing a cybersecurity advisory service line? Follow this step-by-step guide to get your new service offering up and running.

  Client Assessment Template (for PCPS members).

  Use this document to facilitate a discussion with your client about their needs. Review all potential opportunities using the document linked previously or see only applicable options based on your discussion with this Excel document.

  Client Communication Template (for PCPS members).

  Let your client know what new services you have to offer which may be of service to their organization using this customizable template.

- **Tools for Reporting**

  SOC for Cybersecurity: Engagement Overview **(for AICPA members)**
  Learn about the new SOC for Cybersecurity engagement developed by the AICPA for firms to use in assisting organizations with communicating their cybersecurity positions. This document provides an overview of what you need to know.

Additional PCPS Resources

PCPS has even more resources to dive into cybersecurity!

- HACKED! Building defenses against and responses to intrusion
- CPA cybersecurity checklist
- Building a business model for cybersecurity
- The Professional Ethics Executive Committee (PEEC) has answered some of your questions about independence when providing cybersecurity services. Check out these Frequently Asked Questions.
- AICPA Cybersecurity Risk Management Framework
- Cybersecurity Resource Center
- Information Management and Technology Assurance Resources

Activity 4—Let's Manage Your Company's Risk: What Should You Do?

In this activity, you will use the provided data to perform a quantitative risk assessment.

Your organization has gathered the following information about the vulnerability of the database server cluster. These servers are required for the ecommerce application to function. There are two servers in the cluster but only one has a backup power system. If a loss of power occurs, only one of the servers will be online, reducing availability by half. If total unavailability were to occur, it would cost the company $5,000 an hour in lost sales.

Historical figures indicate that power outages in your area occur once every other year. When they occur, they last an average of 5 hours. The company could purchase a second backup power system for a cost of $6,400. Should the company mitigate the risk or accept the risk?

- AV: $5,000 an hour in sales
- EF: .5
- SLE: $2,500 an hour * 5 hour = $12,500
- ARO: (1 div by 2) = .5
- ALE: $6,250
- Cost of the system: $6,400
- ROI of control: $6,250 – $6,400 = –$150
- **Accept the Risk is the Answer**

Final Review—Best Practices for Cybersecurity

We covered *AICPA's Cybersecurity Risk Management Framework*, which is intended for management to use to design and describe its cybersecurity risk management program and is a key component of the new SOC for Cybersecurity engagement.

You also learned that the SOC for Cybersecurity is an examination engagement performed in accordance with the AICPA's clarified attestation standards on an entity's cybersecurity risk management program. It includes the following three key components:

1. Management's description of the entity's cybersecurity risk management program
2. Management's assertion
3. Practitioner's report

In *Performing Quantitative Risk Management*, you learned about risk management, both qualitative and quantitative. You learned the following fundamental values used in a quantitative risk assessment:

- **Asset value (AV).** Represents the asset value.
- **Exposure factor (EF).** Represents the percentage reduction in the value of the asset by the event.
- **Single loss expectancy (SLE).** Represents the cost of an adverse event, were the event to occur a single time (SLE = AV × EF).

- **Average rate of occurrence (ARO).** The frequency with which the threat event typically occurs (expressed as a percent).
- **Average loss expectancy (ALE).** A value that takes into consideration the frequency with which the threat event typically occurs and then attempts to spread the cost of a single occurrence across the number of years that comes between occurrences (ALE = SLE × ARO).

You also learned about additional concepts used in the risk management process such as the following:

- **Return on investment (ROI)** refers to the money gained or lost after an organization makes an investment.
- **Payback** compares ALE against the expected savings as a result of an investment.
- **Net present value (NPV)** considers the fact that money spent today is worth more than savings realized tomorrow.
- **Total cost of ownership (TCO)** measures the overall costs associated with undergoing the organizational risk management process.

You also learned about the following approaches to handling risk:

- **Avoid.** Halt the activity that is causing the vulnerability.
- **Transfer.** Pass the risk on to a third party, including insurance companies.
- **Mitigate.** Select a control or set of controls that while not eliminating the risk, reduce the risk to a level that is acceptable to the company.
- **Accept.** Make the decision to do nothing and live with the risk.

In *Reasonable Assurance and Third-Party Risks*, we covered the AICPA Professional Code of Conduct, Disclosing Information to a Third-Party Service Provider.

You also learned about the four types of SOC reports:

- SOC 1
- SOC 2
- SOC 3
- (SOC) for Cybersecurity
- (SOC) for Supply Chain

Finally, we covered the components that make up the PCPS Cybersecurity Toolkit:

- Exploring Cybersecurity Guide (for AICPA members)
- Learning Matrix (for AICPA members)
- Service Opportunity Grid (for AICPA members)
- Cybersecurity PowerPoint (for PCPS members)
- Client FAQs (for PCPS members)
- Service Implementation Checklist (for PCPS members)
- Client Assessment Template (for PCPS members)
- Client Communication Template (for PCPS members)
- SOC for Cybersecurity: Engagement Overview (for AICPA members)

CONCLUSION

Billions of data records are improperly accessed or stolen each year. Ensuring that your organization is properly advised on cybersecurity and auditing skills can mitigate or prevent data breaches. Knowledge of cybersecurity basics, awareness, and risk mitigation can also help to prevent data breaches or to minimize their impact.

APPENDIX

Illustrative Cybersecurity Risk Management Report[18]

SECTION 1—ASSERTION OF THE MANAGEMENT OF XYZ MANUFACTURING

Introduction

We have prepared the attached XYZ Manufacturing's Description of its Cybersecurity Risk Management Program throughout the period January 1, 20X1, to December 31, 20X1 (description), based on the criteria for a description of an entity's cybersecurity risk management program identified in the AICPA Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program (description criteria). An entity's cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented. We have established XYZ Manufacturing's cybersecurity objectives, which are presented on page XX of the description. We have also identified the risks that would prevent those objectives from being achieved and have designed, implemented, and operated controls to address those risks.

Inherent Limitations

There are inherent limitations in any system of internal controls, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

[18] Please note that this is an example of SOC for Cybersecurity.

Examples of inherent limitations in an entity's cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

ASSERTION Example

We assert that the description throughout the period January 1, 2017, to December 31, 2017, is presented in accordance with the description criteria. We have performed an evaluation of the effectiveness of the controls included within the cybersecurity risk management program throughout the period January 1, 2017, to December 31, 2017, using the criteria for security, availability, and confidentiality set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) (control criteria). Based on this evaluation, we assert that the controls were effective throughout the period January 1, 2017, to December 31, 2017, to achieve the entity's cybersecurity objectives based on the control criteria.

SECTION 2—INDEPENDENT ACCOUNTANT'S REPORT

To Management of XYZ Manufacturing:

Scope

We have examined the accompanying XYZ Manufacturing's Description of its Cybersecurity Risk Management throughout the period January 1, 20X1, to December 31, 20X1 (description), based on the description criteria noted below. We have also examined the effectiveness of the controls within that program to achieve the entity's cybersecurity objectives based on the control criteria noted below.

The criteria used to prepare the description are the AICPA's Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program (description criteria); the criteria used to evaluate whether the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives are the criteria for security, availability, and confidentiality set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) (control criteria).

An entity's cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that were not prevented.

Entity's Responsibilities

XYZ Manufacturing's management is responsible for the following:

- Establishing the entity's cybersecurity objectives, which are presented on page XX of the description
- Designing, implementing, and operating the cybersecurity risk management program, including the controls within that program, to achieve the entity's cybersecurity objectives
- Preparing the accompanying description of the entity's cybersecurity risk management program
- Providing an assertion about whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether controls within the cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives

When preparing its assertion titled Assertion of the Management of XYZ Manufacturing, management is responsible for (a) selecting and identifying in its assertion, the description criteria and the control criteria and (b) having a reasonable basis for its assertion about whether the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives by performing an assessment of the effectiveness of those controls based on the control criteria. The description of the entity's cybersecurity risk management program and management's assertion accompany this report.

Accountant's Responsibilities

Our responsibility is to express an opinion, based on our examination, about whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria of:

- obtaining an understanding of the entity's cybersecurity objectives and its cybersecurity risk management program;
- assessing the risks that the description was not presented in accordance with the description criteria and that the controls within that program were not effective; and
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria and whether the controls were effective.

Our examination also included performing such other procedures as we considered necessary in the circumstances. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in a cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects,

- the description of XYZ Manufacturing's cybersecurity risk management program throughout the period January 1, 20X1, to December 31, 20X1, is presented in accordance with the description criteria and
- the controls within that program were effective throughout the period January 1, 20X1, to December 31, 20X1, to achieve the entity's cybersecurity objectives based on the control criteria.

Baker, Jones, and Eagle, CPAs Athens, Georgia March 1, 20X2.

SECTION 3—XYZ MANUFACTURING'S DESCRIPTION OF ITS CYBERSECURITY RISK MANAGEMENT PROGRAM

Nature of Business and Operations

DC1: The nature of the entity's business and operations, including the principal products or services the entity sells or provides and the methods they distribute.

XYZ Manufacturing (XYZ or the Company) is a leading manufacturer, distributor, and retailer of reproduction consumer products, and objects from various historical periods, with an emphasis on classical Greece, ancient Rome, and medieval Europe. The Company's products allow consumers to emulate a noncontemporary lifestyle in one or more facets of their lives. Merchandise is provided across a broad range of categories, including kitchen and dining, furniture, bedding and bath, lighting solutions, and arts, crafts, and sewing. The Company operates through three key segments: manufacturing (30% of revenue), online retail (40% of income), and wholesale (30% of revenue). XYZ's online retail and wholesale operations offer products manufactured by the Company and sourced under contract from other manufacturers. Online retail also offers products sourced from other wholesalers.

The Company serves its primary markets of North America and Europe from its headquarters in Athens, Georgia, Rome, and Italy, respectively, and has major operating facilities throughout the U.S. and Europe. Manufacturing is located in Shanghai, China. In 2015, the Company entered into a joint venture with UVW Trading of Hong Kong to expand into Asian markets, where the Company's products hold strong appeal from a novelty perspective. Commercial carriers provide distribution.

Nature of Information at Risk

DC2: The principal types of sensitive information created, collected, transmitted, used, or stored by the entity.

The Company creates, obtains, distributes, uses, and stores a wide variety of information in its operations. In addition to information common to the operation of entities similar to XYZ, such as regulatory compliance information and personnel records, the Company uses the following information:

- Financial information, which is used for both internal and external reporting purposes. Internal financial information and external financial information, prior to publication, are considered confidential and are treated as insider information.
- Confidential sales information, including customer lists, confidential wholesale pricing information, and order information.
- Payment card information used in online retail and wholesale transactions, including cardholder names and card numbers. This information may be retained for customer convenience on XYZ systems for ease of ordering.
- Online retail customer profile information, used to provide customers with a personalized lifestyle experience.
- Confidential product information, including product specifications, new design ideas, and branding strategies.
- Proprietary information provided by business partners, including manufacturing data, sales and pricing information, and licensed designs.
- Confidential employee information.

Cybersecurity Risk Management Program Objectives (Cybersecurity Objectives)

DC3: The entity's principal cybersecurity risk management program objectives (cybersecurity objectives) related to availability, confidentiality, the integrity of data, and integrity of processing.

Under the direction of the XYZ board of directors, management establishes the objectives of the Company. Based on these objectives, management also establishes specific objectives for its cybersecurity risk management program. Because substantially all Company operations involve the use of IT, the Company makes no distinction between information security and cybersecurity.

XYZ Manufacturing's cybersecurity objectives are the following:

- **Availability.** Enabling timely, reliable, and continuous access to and use of information and systems to support operations and to provide the following:
  - Online retail store availability 24-hours a day year-round
  - Customer experiences related to system response and dropped transactions meeting benchmarks established by management
  - Manufacturing system availability during scheduled shifts
  - Timely information from the enterprise resource planning (ERP) system to suppliers and management to support decision-making

    - Wholesale online, field sales support, and customer service center systems availability as committed
    - Accurate product availability and delivery information
        - Support the delivery of products to customers as committed
        - Comply with applicable laws and regulations
        - Safeguard assets
- **Confidentiality.** Protecting information from unauthorized access and disclosure, including means for protecting proprietary information and personal information subject to privacy requirements, to safeguard the following:
    - Employee and customer information, including credit card information, in accordance with laws, regulations, and card brand requirements
    - Confidential corporate data related to sales and financial reporting
    - Confidential business transactions related to the information of business partners and others
    - The intellectual property of the Company, its business partners, and others
- **Integrity of data.** Guarding against improper capture, modification, or destruction of information to support the following:
    - The preparation of reliable:
        - Financial and nonfinancial information for external reporting purposes
        - Information for internal use
    - Nonrepudiation authenticity of transactions from online systems
    - The completeness, accuracy, and timeliness of manufacturing, delivery of goods, and information processing
    - Management, in holding employees, vendor and business partner employees, and customers accountable for their actions
    - The storage, processing, and disclosure of information, including personal and third-party information
- **Integrity of processing.** Guarding against improper use, modification, or destruction of systems in order to support the following:
    - The accuracy, completeness, and reliability of product delivery and transaction processing
    - The manufacture of goods to product specifications
    - The efficient operation of production
    - The safeguarding of the life and health of employees in production facilities

Guarding Against the Improper Use or Misuse of Processing Capabilities That Could Be Used to Impair the Security or Operations of External Parties

DC4: The process for establishing, maintaining, and approving cybersecurity objectives to support the achievement of the entity's objectives.

With the support of management and outside resources engaged by the board, the Company's board of directors reviews and updates its formal business strategy annually. Based on that strategy, management and the board annually establish or update the Company's overall business objectives, including objectives over operations, compliance, and reporting. At the completion of this process, the overall objectives are approved.

Upon approval of the Company's business strategy and overall objectives, management uses a top-down approach to establish or update specific business objectives for business units and functions, including information technology, within the organization. This process includes budgeting resources and establishing metrics for the achievement of the objectives. At the completion of this process, the specific business objectives and the budget is submitted to the board for approval.

As part of the development of specific business objectives, the chief information security officer (CISO) updates the Company's cybersecurity objectives with the business units' objectives and other functional areas. These cybersecurity objectives are then approved by the Company's executive management, including the CEO, COO, CFO, chief risk officer (CRO), general counsel (GC), and the CIO.

The Company's cybersecurity risk management program is based on specifications outlined in the National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity" (NIST cybersecurity framework) and International Standardization Organization and International Electrotechnical Commission (ISO/IEC) standards. The Company's portfolio of security controls is based on ISO/IEC controls and, for systems containing cardholder information, the Payment Card Industry Data Security Standards.

Factors That Have a Significant Effect on Inherent Cybersecurity Risks

DC5: Factors that have a significant effect on the entity's inherent cybersecurity risks, including the (1) characteristics of technologies, connection types, use of service providers, and delivery channels used by the entity; (2) organizational and user characteristics; and (3) environmental, technological, organizational, and other changes during the period covered by the description at the entity and its environment.

Technologies, Connection Types, Service Providers, and Delivery Channels

The Company uses the following technologies, connection types, service providers, and delivery channels:

- An integrated ERP system is used to manage manufacturing, wholesale, and retail operations. The ERP system is interfaced with the manufacturing, wholesale, and online retail systems to provide an integrated IT environment.
- Online retail operations are supported by a software-as-a-service (SaaS) cloud provider. The integrated solution permits the Company to design and maintain its retail site effectively and efficiently. Online wholesale operations are supported through a third-party system that interfaces with the ERP system. The system is hosted on a network of virtual servers hosted in XYZ's primary data center.
- Wholesale call center services are outsourced with the call center's systems interfaced with the ERP system to facilitate ordering and problem resolution. The interface with the call center is over a virtual network connection. Custom-developed software is used to interface the call center system to the ERP interface.

- Field sales automation is provided through the use of company-owned tablet devices running third-party software customized for the Company. Tablets access the ERP system through a virtual private network (VPN) system.
- Manufacturing is controlled through a network of midrange systems running widely used manufacturing system software. This software is modified and maintained by Company IT personnel.
- All connectivity to external users occurs through defined access points managed by routers. Routers are also used to segment the network within the Company.
- Transmissions to vendors and other third parties are sent through defined secure channels.

Organizational and User Characteristics

The Company's IT function is headed by a chief information officer (CIO) and is divided into application services, technology services, and information security. The Company uses a centralized organizational model to support company applications and technology. The online retail and call center vendor relationships are managed by designated personnel in technology services reporting to the chief technology officer (CTO). The information security group is headed by the chief information security officer (CISO) and consists of security architecture and technical support, application security, and the security operations center personnel. Security operations center personnel are primarily responsible for user administration, second-level security support, security event monitoring, security incident response, and management.

Users of the system primarily consist of the following:

- Consumers whose access is restricted to the online retail system provided by the vendor.
- Wholesale customers whose employees have access to catalog information, order status, order functionality, and account functionality through the wholesale system's internet module. Customer personnel are assigned user IDs via a master customer account that is also used to administer the accounts. Customer personnel accounts are assigned defined roles established by the Company.
- UVW personnel whose access is similar to wholesale customer access.
- Call center service organization personnel, who access the wholesale system through assigned user accounts that are restricted to a defined call center role.
- All XYZ employees, who are assigned unique user IDs that grant them default company access and email access, except for manufacturing line personnel in Shanghai who are not granted access.
- Product vendors, who are granted limited access to the ERP system to pick up purchase orders and inquire about the status of invoices. This access is provided through a module of the ERP system through a vendor account and password.

Although IT assets are located in all countries of operation, the Company does not deem any countries to be of higher risk than others.

Environmental, Technological, Organizational, and Other Changes During the Period

In December of 2016, the Company added manufacturing operations in Shanghai, China, through the acquisition of an established brass foundry. At the time of the acquisition, the foundry ran its business operations using off-the-shelf software on a local area network. The

Company completed migration of all foundry data processes to the ERP system in March of the current year.

The Company is in the process of finishing its new manufacturing facility and upgrading manufacturing and foundry equipment as part of a modernization program. This program is modernizing foundry floor equipment, replacing existing manual equipment with new equipment that uses leading industrial control systems. These systems will be integrated with the ERP system to enhance production operations and reporting. The new facility is expected to be operational by November. The process for adding new system components related to this change is subject to the cybersecurity risk management program, and controls over those components are implemented as part of the change management process.

DC6: For security incidents that (1) were identified during the 12-month period preceding the period end date of management's description and (2) resulted in a significant impairment of the entity's achievement of its cybersecurity objectives, disclosure of the following: (a) nature of the incident, (b) timing surrounding the incident, and (c) extent (or effect) of these incidents and their disposition.

XYZ utilizes a number of manual and automated security monitoring capabilities to identify security events in the environment. During the period under assessment, the Company experienced an incident that compromised sensitive data from a SQL injection attack on a web application. The attack was detected approximately 66 hours after the event and was remediated within 5 days of detection. XYZ Manufacturing incurred costs related to the notification of and credit monitoring for affected parties (commercial customer information and personally identifiable information of retail customers) and fees associated with the retention of outside cybersecurity expertise to conduct a forensic investigation of the affected systems and later, an independent evaluation of security measures to ensure that remediation actions were sufficient to address the identified threats. The incident was fully resolved and remediated, and XYZ has made the necessary adjustments to its systems and processes and the affected service provider systems and processes to reduce the likelihood that similar incidents could reoccur.

Cybersecurity Risk Governance Structure

DC7: The process for establishing, maintaining, and communicating integrity and ethical values to support the functioning of the cybersecurity risk management program.

Management sets the organizational tone through policies, a code of ethics, a commitment to hiring competent employees, and the development of reward structures that promote an effective internal control and governance structure. The board of directors meets quarterly with members of executive management to review financial and operational performance, including the entity's cybersecurity risk management program. Employees are required to sign the employee handbook upon hire, acknowledging their acceptance and adherence to the Company's policies and code of conduct. Such policies and the code of conduct have been designed to promote integrity and ethical values throughout the workplace. The information security policy includes information about the following:

- Information privacy, confidentiality, and acceptable use
- Electronic communications
- Data management
- Disclosure

DC8: The process for board oversight of the entity's cybersecurity risk management program.

The XYZ board of directors includes various outside directors with industry knowledge and experience, including one board member who is a former IT director of an S&P 100 company with over 15 years of experience in IT and cybersecurity, and serves as the board's subject matter expert on cybersecurity matters. Additionally, the XYZ CISO joins the quarterly board meeting to present an overview of the Company's cybersecurity risk management program, including the entity's risk governance and committee's activities. The board provided feedback and action items and is actively engaged in overseeing this key business risk.

The risk governance committee was established to coordinate the entity's risk assessment and management efforts and its units. The committee, which the CRO chairs and consists of the CISO, CCO, external specialists, and IT and business line personnel, ensures that (a) cybersecurity risks arising from both internal and external sources are identified and evaluated; (b) controls are properly designed and implemented to address all areas as appropriate; and (c) controls operate effectively to achieve the entity's cybersecurity objectives. Areas evaluated include systems development, computer operations, program changes, and access to programs and data.

As part of the CISO's quarterly presentations, the results of the XYZ information security team's program assessments are presented and discussed, as well as any corrective action needed as a result of the evaluations. The presentations also include summaries of the Company's vendor and business partner oversight program. Under the program, Company personnel perform an annual review of vendor and business partner relationships to evaluate whether the Company complies with industry standards and best practices.

DC9: Established cybersecurity accountability and reporting lines.

Under the direction of the risk governance committee, the CISO is responsible for overseeing the cybersecurity risk management program and executing the entity's strategy and other decisions agreed upon by executive management and the board of directors. The CISO reports administratively to the CIO, with an escalation point to the CEO. The CISO presents a quarterly cybersecurity update to the board of directors to report the entity's cybersecurity risk management program.

The CISO also chairs the information security committee. The information security team, which consists of representatives from all departments in XYZ, is a centralized team of cybersecurity practitioners, subject matter experts, and IT personnel who support the information security operations of the organization (such as systems administrators, software engineers, network engineers, and security analysts). The duties, responsibilities, and hierarchy of employees on the information security team are defined in a role matrix and form the entity's cybersecurity risk management program's foundation.

The information security committee defines and approves the strategy, policies, and standards underlying the entity's cybersecurity risk management program. The annual risk assessment results, periodic internal audits, and quarterly external independent assessments are provided to the CISO and the information security committee throughout the year to continuously adapt the program to align with new and emerging threats and potential vulnerabilities. The risk governance committee oversees the activities of the information security committee.

Alongside the CISO is the CTO who also reports administratively to the CIO but with an escalation point to the CEO. The CTO is responsible for managing the technology and resources that support the internal operations of the company. This includes overseeing policy and processes regarding relationships with vendors and business partners that may contribute to the cybersecurity risk management program. These policies and procedures are administered through the vendor and business partner oversight program discussed later.

DC10: The process used to hire and develop competent individuals and contractors and to hold those individuals accountable for their cybersecurity responsibilities.

Applicants with a role in the cybersecurity risk management program are hired based on their ability to satisfy the job duties and responsibilities of the position and fulfill the goals and expectations of the entity.

They are evaluated on their education level, the merits of their past experience, a positive performance history, and knowledge of relevant cybersecurity controls and processes. Before employment, all applicants must also pass a thorough background check.

Upon hiring, employees are required to sign the employee handbook, acknowledging their acceptance of and adherence to the Company's policies and any associated confidentiality and nondisclosure agreements.

Upon hiring and annually after that, all employees must complete training courses covering basic information security practices that support an effective cybersecurity risk management program's functioning. Employees with job responsibilities that fall directly within the cybersecurity risk management program (such as IT personnel, IT management, and internal auditors) have minimum training and continuing education requirements each year.

Employees in the cybersecurity risk management program are encouraged to maintain an active role in relevant cybersecurity information sharing forums, special interest groups, and professional associations to stay up to date on new and emerging cybersecurity risks that may impact the entity or its operating environment.

Contractors must follow the same onboarding process as employees and are subject to the same background checks and security awareness training requirements as employees. Employees' and contractors' compliance with security awareness training requirements is monitored regularly by human resources.

XYZ has established an entity-wide hierarchy and reporting structure that is codified within an organizational chart maintained on the corporate intranet by human resources. XYZ has prepared a role matrix for employees and managers who have roles within the cybersecurity risk management program. The role matrix defines key job duties and responsibilities in the context of the overall program. Additional information security responsibilities and practices for certain roles within the entity are described in the Company's information security policy and the employee handbook.

All employees go through an annual performance review cycle. At the beginning of each calendar year, employees and their immediate supervisors establish goals and expectations for their job performance over the upcoming year based on the job duties and responsibilities described in the role matrix.

Employees then receive mid-year and year-end performance reviews from their supervisors that assess the employees' performance against the agreed-upon goals and expectations. Based on the results of their performance review, employees receive merit increases in compensation and are eligible for bonuses and promotions, respective of their seniority, experience, and position within the organization.

Employees whose performance is not aligned with established goals and expectations for job performance, or who are not fulfilling their job responsibilities, may be referred to human resources by their supervisor to develop a performance enhancement plan.

If an employee violates any statute of the employee handbook or the Company's policies, or otherwise acts in a manner deemed contrary to the Company's mission and objectives, whether purposefully or not, the employee is subject to sanctions up to and including termination of employment.

Cybersecurity Risk Assessment Process

DC11: The process for (1) identifying cybersecurity risks and environmental, technological, organizational, and other changes that could have a significant effect on the entity's cybersecurity risk management program and (2) assessing the related risks to the achievement of the entity's cybersecurity objectives.

XYZ maintains a detailed inventory of all information systems, including manufacturing and industrial control systems. All such assets are assigned ownership by a designated department or team within the entity and prioritized based on the asset's business value and criticality to the organization. Information and data assets are subject to the data management policy that defines parameters for the ownership, classification, security, storage, and retention of data. Software and hardware assets are subject to the information systems management policy that defines parameters for the acquisition, development, maintenance, security, and disposal of information system assets.

On an annual basis, the information security team performs a risk assessment that identifies internal and external cyber threats and vulnerabilities to the organization. Information system assets are analyzed to identify associated threats to those assets and vulnerabilities that may be exploited. The resulting risks are then scored based on their likelihood and potential impact to the organization. The assessment includes consideration of the inherent and residual risks that may reside with external parties and the cybersecurity controls to address those risks. Specific policies and procedures are in place to assess and manage the requisition and engagement of vendors or business partners cyber threats and vulnerabilities such relationships may present.

Results of the risk assessment are evaluated by relevant management against criteria for risk acceptance to identify new or existing protective measures and develop or enhance information security policies and procedures.

Internal audit conducts periodic cybersecurity assessments that include working with process owners and IT support personnel to identify specific security threats and vulnerabilities and to identify how the associated risks are being addressed. Additionally, quarterly vulnerability assessments and penetration tests are performed by an external party to identify specific technical threats and vulnerabilities.

DC12: The process for identifying, assessing, and managing the risks associated with vendors and business partners.

XYZ considers the inherent risk of working with vendors and business partners as part of the information security team's annual risk assessment. Internal and external cyber threats and vulnerabilities are identified and assessed based on the likelihood that they could prevent the entity from achieving its cybersecurity objectives. Specific policies and procedures are in place to assess and manage the requisition and engagement of vendors. Consideration is given to the cyber threats and vulnerabilities such relationships may present and whether XYZ's controls reduce such risks to a level consistent with XYZ's cybersecurity objectives and risk acceptance.

XYZ has established a tiering system in which each vendor is assigned a tier (1–3) based upon the inherent risk of the goods and services the vendor provides, the overall operational significance of the vendor to achieving XYZ's business objectives, and the sensitivity of data that resides within the vendor's environment. Business partners are evaluated using the same tiering structure based on the cybersecurity risk associated with each business partner.

The entity's vendor and business partner oversight program requires that all contracts with vendors or business partners clearly address (a) the size, scope, and nature of services being provided; (b) the hardware, software, and information requirements related to the provision of such services; (c) the responsibilities of each party; (d) the requirements for information security to meet XYZ's standards; (e) the ability to perform independent audits of the effectiveness of internal control processes; and (f) the requirement to obtain and review a third-party attestation report.

Disclosure of any confidential or personally identifiable information (PII) to a vendor or business partner is provided only on an as-needed basis and only if the vendor or business partner has enacted appropriate information security and privacy controls. All vendors and business partners with access to confidential information are subject to confidentiality, and privacy agreements and other contractual confidentiality provisions, which must be signed and acknowledged before access to XYZ's systems and data is granted.

The vendor and business partner oversight team ensures that XYZ and its vendors and business partners stay current with existing contractual obligations, information security and privacy regulations, certification compliance requirements, and industry standards. The vendor and business partner oversight team performs an ongoing annual review of vendor and business partner relationships to (a) reevaluate the services provided and any cybersecurity threats and vulnerabilities arising from the relationship; (b) consider whether the assessed risks are being addressed appropriately by each party's contractual agreements, information security controls, and processes; and (c) evaluate whether the entity's vendor and business partner oversight program complies with industry standards and best practices. The review process includes obtaining security questionnaires, conducting personnel interviews, performing walkthroughs, performing site visits, and conducting IT scanning and testing. In addition, when available, the review process may also include obtaining and reviewing third-party attestation reports.

The CISO and the information security team participate in cybersecurity information sharing forums, special interest groups, and professional associations to increase information sharing between knowledgeable parties and to stay up to date on changes in the regulatory, economic, and physical environment in which the Company operates. XYZ Manufacturing maintains communicative relationships with relevant governing and regulatory bodies to stay abreast of changes to laws and regulations that impact the organization as they arise. Internally, consideration of the entity's cybersecurity risk management program is an integral part of proposed changes to existing business lines or operations, the development or acquisition of new business lines or procedures, decisions about doing business in new geographies or markets, and the adoption of new technologies or processes throughout the business. The information security team, led by the CISO, is involved in the decision-making process related to changes that could impact the size, scope, or operational nature of the business. In this capacity, the team may perform ad hoc, focused risk assessments to identify new risks to the organization and associated impacts to be considered during the decision-making process. The team may also reevaluate the design of controls to ensure continued protection.

Additionally, on an annual basis, the information security team performs a full risk assessment that identifies internal and external cyber threats and vulnerabilities to the organization. During the annual risk assessment, the team considers both internal changes to XYZ operational processes (such as new or modified lines of business, new or modified operating procedures, new geographies or markets, new technologies or services used) and external changes (such as new or changing regulatory requirements, industry standards, economic circumstances, emerging risks) that could affect the entity. New controls are designed in response to identified threats and existing controls are assessed to ensure they reflect changes to the size, scope, and operational nature of the business.

Cybersecurity Communications and Quality of Cybersecurity Information

DC13: The process for internally communicating relevant cybersecurity information necessary to support the functioning of the entity's cybersecurity risk management program, including (1) objectives and responsibilities for cybersecurity and (2) thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents requiring a response, remediation, or both.

The internal communication of cybersecurity information for employees according to their role in the cybersecurity risk management program is described in the XYZ information security policy, which is available to all employees on the Company intranet. Additionally, the employee handbook identifies certain information security responsibilities and practices, depending on the employee's role within the organization. At the time of hiring, all employees must provide sign-off, acknowledging acceptance of and adherence to the Company's policies.

Upon hiring, and annually thereafter, all employees must successfully complete training courses covering basic information security practices that support the functioning of an effective cybersecurity risk management program. The training courses are designed to assist employees in identifying and responding to social engineering attacks (phishing, tailgating) and in avoiding inappropriate security practices (for example, writing down passwords or leaving sensitive material unattended). XYZ periodically assesses employees' awareness of corporate policy by attempting to tailgate into buildings, sending simulated phishing emails, and performing desk sweeps, among other tactics. If an employee is found to be violating Company policies, additional training is provided or other disciplinary actions are taken.

Employees with job responsibilities that fall directly within the cybersecurity risk management program (IT personnel, IT management, internal audit, and the like) have additional requirements to complete technical and job-specific training throughout the year. Additionally, those employees who have direct access to customer and employee data (for example, sales, customer service, human resources, IT helpdesk, and finance) will receive specific training around incident management, information handling, and data protection.

Training and other programs related to employee cybersecurity awareness incorporate materials developed internally by XYZ in collaboration with industry—and cybersecurity—focused vendors or business partners. These vendors or business partners provide expertise and tools to develop, perform, track, and test employees' compliance with cybersecurity awareness policies and standards.

XYZ has established a cybersecurity awareness program (CAP) that periodically distributes reminders of information security practices to all employees and sends internal communications to promote security awareness and to provide the latest security news. CAP is also responsible for (a) monitoring cybersecurity risk associated with vendors and business partners who have access to the entity's system, (b) monitoring forums and news sites for information regarding potential breaches, (c) reviewing vendors' and business partners' cybersecurity examination reports on an annual basis, and (d) maintaining ongoing, direct contact with vendors and business partners to address any issues identified.

On an annual basis, XYZ updates the cybersecurity training program and CAP to incorporate changes in the threat landscape and new tactics being executed by threat actors. XYZ also evaluates lessons learned from any previous incidents and incorporates changes into the programs as necessary.

An incident hotline is available to all employees to report information security events they have been involved in or witnessed (such as phishing attacks, malware, lost or stolen devices, and inappropriate information disclosure). XYZ receives a quarterly attestation from the outsourced call center that all hotline personnel have completed XYZ's CAP and are aware of defined policies related to information protection, data handling, and incident response.

The CISO presents a quarterly update to the board of directors to report on the state of the entity's cybersecurity risk management program. During the update, the CISO presents the status of ongoing efforts to develop and maintain the program in response to (a) prior security events at the organization, (b) changes in XYZ's operational procedures, (c) changes to legal and regulatory requirements affecting the organization, (d) results of audits and testing by internal and external parties, and (e) new and emerging cybersecurity risks to the organization.

DC14: The process for communicating with external parties regarding matters affecting the functioning of the entity's cybersecurity risk management program.

XYZ has a disclosure policy defining when, by whom, and to what extent external parties are informed of matters relevant to the functioning of XYZ's cybersecurity risk management program. All disclosures to external parties are made in accordance with applicable laws and regulations at the state and federal level. Any such legal requirements are considered in the development and maintenance of the disclosure policy during annual review. Employees are educated on the policies and procedures for reporting and disclosing cybersecurity incidents or events through the XYZ information security policy and XYZ employee handbook.

XYZ may become aware of matters affecting the functioning of the entity's cybersecurity risk management program via its existing monitoring processes, as well as via notification by third parties or law enforcement. When such matters arise, they are immediately reviewed by the XYZ risk governance committee to determine relevance and applicability. Where necessary or appropriate, the matter may be treated as a security incident and handled via XYZ's security incident response process, as described later.

As is typical business practice by most organizations, XYZ restricts communication of matters related to the functioning of XYZ's cybersecurity program to only those stakeholders and business partners who have a need to know such information. This information may be communicated via mediums appropriate to the nature of the information and the urgency of the situation, and may include conference calls, electronic mail, memoranda, or in-person meetings. In the rare instance when public disclosure of such matters would be necessary or appropriate, XYZ's legal counsel and corporate communications representative are responsible for jointly distributing and communicating such disclosure.

Monitoring of the Cybersecurity Risk Management Program

DC15: The process for conducting ongoing and periodic evaluations of the operating effectiveness of key control activities and other components of internal control related to cybersecurity.

XYZ uses several mechanisms to assess the ongoing effectiveness of internal controls designed to mitigate cybersecurity risks. Assessment and monitoring of the program are designed to meet the requirements of the NIST cybersecurity framework and ISO 27001.

Internal audit conducts periodic cybersecurity assessments and tests of internal controls that include (a) working with process owners and IT support personnel to identify specific security threats and vulnerabilities and how the associated risk is being addressed and (b) tests of the design, implementation, and operating effectiveness of internal controls that address cybersecurity risks.

Members of the internal audit team have the requisite knowledge of and experience with cybersecurity risks and controls. XYZ also uses external parties to independently evaluate the state of the cybersecurity risk management program. Quarterly vulnerability assessments and annual penetration tests are performed by an external service provider to identify specific technical threats and vulnerabilities and to benchmark the environment against leading cybersecurity practices. In addition, the entity obtains for its SaaS vendor an annual web application security assessment report. Every 2 years, XYZ engages a service provider to perform an independent assessment of the cybersecurity risk management program to evaluate alignment with leading industry practices and consistency with Company policies in order to identify gaps and potential opportunities for improvement.

Both internal and external evaluations are made using a risk-based approach that may vary the nature, timing, and extent of testing. The criteria for such evaluations, including the nature and frequency of such evaluations, are reviewed during the annual risk assessment and modified as needed, with consideration for changes to XYZ's operational processes, including changes to the size, scope, and operational nature of the business, recent security threats or incidents, new or emerging risks, and changes in industry standards.

DC16: The process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective actions, including management and the board of directors, as appropriate.

On a quarterly basis, the information security team performs a risk assessment update that identifies changes to internal and external cyber threats and vulnerabilities to the organization. Results are evaluated by the risk governance committee to identify whether new protective measures or enhanced information security policies and procedures are needed. The risk governance committee is also tasked with monitoring vulnerabilities, allocating resources to address them, and reprioritizing remediation initiatives, as necessary. Key performance indicators related to average closure time have also been defined and are monitored by the committee on a monthly basis.

The results of all monitoring activities, regardless of source, are entered into a vulnerability tracking system for evaluation and identification of remediation activities that may be needed. Identified vulnerabilities are assessed with regard to the likelihood and magnitude of exploitation. All vulnerabilities evaluated are identified for remediation or additional monitoring. Responsibilities for corrective action plans are assigned and completion dates determined. The information security committee reviews the list of open vulnerabilities on a monthly basis to monitor progress toward resolution and to identify trends and responses. On a quarterly basis, the risk governance committee and executive management receive summary reports of vulnerability management activities. In addition, the CISO presents cybersecurity risk management program results, including vulnerability management activities, to the board of directors during each of its regularly scheduled meetings.

Cybersecurity Control Activities

DC17: The process for developing a response to assessed risks, including the design and implementation of control processes.

A risk governance committee was established by XYZ to coordinate the risk assessment and management efforts of the entity and its units. The committee, which is chaired by the CRO and consists of the CISO, CCO, external specialists, IT and business line personnel, ensures that risks are evaluated and that controls are designed, implemented, and operated to address all areas, as appropriate, to detect, respond to, mitigate, and recover from security events based on the assessed risks. Areas for evaluation include systems development, computer operations, program changes, and access to programs and data. Implemented controls include preventive and detective controls, such as manual, automated, or IT-dependent controls based on the environment in which the entity operates, the nature and scope of the entity's operations, and its specific characteristics.

Business processes are documented in standard operating manuals; however, the risk governance committee also has business operations liaisons in each business area that are responsible for the ownership and documentation of key risk areas for the business operations. In 2014, the risk governance committee enhanced their key risk considerations for business areas to include specific consideration of cybersecurity risks.

The risk governance committee business liaisons annually revisit the risk assessments and validate the existence of controls to mitigate identified risks. The controls are captured in the Company's controls repository (CR), which is an inventory of the operations, risks, and controls associated with each business area. The CR is used to conduct quarterly self-assessments of controls and also serves as an input into the Company's annual controls maturity assessment, which is conducted by internal audit and reported to the risk governance committee.

The Company contracts for insurance coverage, including business disruptions, for risks which cannot be cost effectively mitigated through other techniques.

DC18: A summary of the entity's IT infrastructure and its network architectural characteristics.

XYZ employs both internally hosted and cloud-based applications to support its manufacturing, retail, and wholesale operations. Cloud-based applications are provided through an arrangement with ABC Cloud under a service contract whereby XYZ retains the responsibility for specific server configuration and operating system change management. And ABC Cloud provides server support and maintenance.

Company applications run primarily on UNIX family operating systems and use industry standard database management systems. The manufacturing system uses a proprietary midrange operating system supplied by a leading IT manufacturer. The application was developed in house using the integrated operating system database. Field sales application tablets use an industry standard operating system.

XYZ has segmented its ERP financial reporting systems from its externally facing retail, wholesale, and call center interfaces through the use of Cisco ASA firewalls, which are configured, managed, and supported by XYZ IT personnel. The firewall configurations and rules follow standards created by XYZ IT management under the direction of the CISO. All connectivity to external users occurs through defined access points protected by a redundant firewall complex. Firewalls are also used to segment the network within the Company.

Wholesale call center services are outsourced, with the call center's systems interfaced with the ERP system to facilitate ordering and problem resolution. The interface with the call center is over a virtual network connection. Custom-developed software is used to interface the call center system to the ERP interface.

The call center service provider facilities are reviewed annually by XYZ through their previously defined vendor and business partner oversight program. These vendor and business partner assessments focus on areas specific to the security configurations of the hosted applications, as well as to the network architecture related to XYZ's interfaces to the vendors.

ABC Cloud's SaaS is also reviewed annually through XYZ's vendor and business partner oversight program; however, given the nature of the responsibilities defined within the cloud agreement, XYZ configures its server settings in line with XYZ's corporate standards. XYZ has defined a standard build for cloud-based server configurations and uses that as the baseline from which servers are configured to support the SaaS environment. Also, monitoring of the configurations for adherence and compliance with defined standards is conducted by XYZ IT support personnel, as well as through the corporate internal audit and risk management teams.

Field sales automation is provided through the use of company-owned tablet devices running third-party software customized for the Company. Tablets access the ERP system through a cellular-based VPN system that uses two-factor, token-based authentication.

DC19: The key security policies and processes implemented and operated to address the entity's cybersecurity risks, including those addressing the following:

a. Prevention of intentional and unintentional security events

b. Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents

c. Management of processing capacity to provide for continued operations during security, operational, and environmental events

d. Detection, mitigation, and recovery from environmental events and the use of backup procedures to support system availability

e. Identification of confidential information when received or created, determination of the retention period for that information, retention of the information for a specified period, and destruction of the information at the end of the retention period

XYZ has defined a set of information security standards and policies that are under the direction and ownership of the CIO and implemented through the CISO. The standards and policies address the management and implementation of security controls, ranging from the physical security of facilities and equipment to the logical security at the data element layer. The information security policies and standards are designed to provide information to employees, contractors, and vendors that are aligned to their job or functional responsibilities, while also contemplating segregation of functions that may otherwise create a segregation of duties conflict.

Security policies are published on the Company's intranet, included in onboarding packages, and reiterated through annual training that all employees are required to take and acknowledge. Security policies related to relationships with vendors and business partners are enforced through contractual commitments and related service-level agreements (SLAs) and, where possible, are monitored for adherence through XYZ's vendor and business partner oversight program.

The key components of the XYZ information security policy are discussed in the following paragraphs.

Prevention of Intentional and Unintentional Security Events

The Company has the following processes in place to prevent intentional and unintentional security events:

Physical and Logical Access Provisioning, De-provisioning, and Transfers (including Remote Access)

XYZ employees are granted network access only after completing security awareness training. Users are granted access to XYZ systems and data based on their job role. Access requests are approved by the user's manager prior to access being granted. Upon termination, human resources send a notification through the ticketing system, which is routed to the user administration team to remove user account access for the terminated user. Human resources provide a weekly list of terminations, which is then cross-referenced against the user account list to identify any user accounts that have not been properly terminated. User accounts that are inactive for 60 days are automatically disabled. For access modifications, the user's manager is required to submit and approve an access request ticket via the ticketing system, which is routed to the user administration team for processing.

Authentication

Users are required to authenticate using a unique user ID and password before being granted access to the network. The network domain password policy is configured to include password minimum length, expiration intervals, complexity, history, and an invalid password account-lockout threshold. A new user's account password is set to pre-expire so that the password must be reset the first time a user logs in to the network.

Credentials Management

Access is granted based on role-based security profiles that provide segregation of duties and limit transaction access. XYZ application and data owners review access rights on a semiannual basis. On an annual basis, the roles and the transactions assigned to the roles must be reviewed.

Privileged User Management

Access to privileged user or super-user accounts is authorized by management. Users with privileged user accounts are provided with a standard (nonprivileged) user account for use on a daily basis (for email and personal productivity software) and are only permitted to use their super-user accounts when performing administrative tasks. All super-user account access is logged and monitored. On a quarterly basis, the user administration team performs an access review of privileged access.

Database Security

Database administrators are the only individuals that can access XYZ databases. All database access and activity are logged. Database account access is reviewed twice a year for continued appropriateness. Direct data changes require approval, which should be documented within the Company's ticketing system and handled via the change management process.

Data Loss Prevention (DLP)

The Company has a DLP solution that monitors and provides alerts about (and can take action regarding) the transmission or removal of confidential data outside of the Company or on BYOD devices. The DLP solution is configured to encrypt external storage devices and prevent the saving of sensitive data to removable media. Hard drives of all servers, workstations, and laptops are encrypted. XYZ Manufacturing and its vendors utilize transport layer security for encryption of transmissions across the internet to XYZ web servers and the email system. A VPN requiring multifactor authentication is used for all remote access to XYZ's internal network, ensuring that data is encrypted in transit when sent across the internet from a Company computer system. Site-to-site VPNs are also utilized with certain XYZ vendors to provide encrypted channels for communication between locations.

Data Destruction

Data that exceeds its retention period is removed from systems and all backup media. Data that is labeled as confidential is erased using secure deletion techniques approved by the U.S. government (multipass overwrite). All computer hard drives are required to be securely deleted before disposal and a certificate of destruction is obtained from the third-party organization that disposes of all computer equipment for XYZ.

Data Backup

Nightly incremental backups of all production servers and daily backups of production databases are conducted. Every month end, the Company is required to perform a full backup of the production servers. Backup tapes are encrypted and sent to a third-party vendor for storage. An automated backup system is implemented to monitor the completion of scheduled backups. When a backup job is not completed successfully, operations personnel create an incident ticket and assign personnel to resolve the failure.

Virus Detection and Prevention

Antivirus software is required to be installed on all XYZ servers, desktops, laptops, and email infrastructure and is centrally managed to ensure timely delivery of signature updates. The antivirus software settings are preconfigured for automatic updates and locked to prevent any user tampering or disabling. Email filtering software is in place to restrict and reject emails that contain certain malicious file types, including executable files. The Company's antivirus administrator is required to perform a quarterly inventory reconciliation against a system inventory list.

Firewalls and Perimeter Security

XYZ Manufacturing deploys enterprise firewalls at the perimeter of the network and in other strategic locations throughout the network in an active failover configuration. Only a minimal number of ports and services are allowed into the XYZ environment. All firewalls are managed using a centralized console and XYZ installs monitoring software on the firewalls to provide alerts when changes occur at the administrative level. Firewall rulesets are reviewed twice a year to ensure that they are appropriately configured.

Secure System Configuration

Configuration specifications are installed on all systems before they are implemented into production. Monthly vulnerability and configuration scans to validate that all systems remain configured in accordance with XYZ's security hardening standards are performed. When updates to existing standards are made, the changes are implemented on production systems.

Intrusion Prevention

A threat intelligence database is regularly updated. Packets identified by the threat intelligence database that meet a certain risk threshold or exhibit certain characteristics are automatically dropped and prevented from entering the XYZ network.

Change Management

A change approval board (CAB) that consists of representation from all IT departments within XYZ is in place. On a weekly basis, the CAB meets to review upcoming system and application changes, which are requested via the Company's online ticketing software. All changes are required to have a documented back-out plan. All changes are required to have a documented test plan.

All members of the CAB approve a change before it can be implemented. In the weekly CAB meeting, the previous week's changes are reviewed. A root cause analysis report is completed for any changes that did not go as planned before they can be reconsidered.

Application Changes

Change requestors submit a change request within the Company's ticketing system. An application analyst reviews the change request and develops a project change budget estimate. On a monthly basis, application change requests and associated budgets are reviewed and categorized by IT and the business owners and ranked according to priority. Development occurs in a development environment that is separate from the production environment, using test data. Once development is completed, user acceptance testing takes place. Once user acceptance testing is completed, the business owner who sponsored the change and the applicable application analyst are required to approve the change within the ticket. The IT operations team migrates changes into production after they have been approved by the CAB. Emergency changes are required to be documented and logged in the ticketing system after changes are completed, and the CAB conducts an after-action review to approve the changes retroactively.

Patch Management

When new patches are released, they are reviewed by a group of IT personnel, including a representative from the information security team. The team assigns a priority level to each patch. Patches that are assigned a rating of "critical" are applied to all affected systems within 7 days. Patches that are assigned a rating of "high" are applied to all affected systems within 30 days. Patches that are assigned a rating of "medium" are applied within 60 days. All other patches are applied in regular system updates that typically occur quarterly. Once assigned a patch criticality rating, a patch is assigned to the appropriate IT system administrator for evaluation and testing in the XYZ test lab. When testing is completed, a change ticket is entered in the ticketing system, and the patch is reviewed and approved by the CAB. The information security team is required to conduct vulnerability scanning of all systems monthly to ensure that patches are properly in place. Any missing patches are immediately ticketed, and a resolution is required within 5 business days.

Detection of Security Events, Identification of Security Incidents, Development of a Response to Those Incidents, and Implementation Activities to Mitigate and Recover from Identified Security Incidents

Due to the pervasive use of IT to conduct business operations and deliver products and services to customers, the ability to detect a security event in a timely manner is of significant importance. Accordingly, XYZ Manufacturing has defined formal key security policies and processes focused on identifying cybersecurity issues to detect security events. These policies and processes are focused on the following:

- Utilizing continuous security monitoring tools and programs to assist in identifying anomalies within the network and supporting infrastructure environment—inclusive of security event information relevant to third-party vendors
- Implementing security monitoring processes and procedures and other measures to identify anomalies in information flow, access, data communications, and the operation of business critical systems
- Analyzing anomalies to identify security events and to detect abnormal events or data movement using historical baseline or behavioral analytics data to determine what is considered to be abnormal
- Escalating identified security events that occur through the course of business operations and ongoing communications, both within and outside of the organization

Detection of Security Events

A dedicated security team is available 24/7. Administrative activity and supporting infrastructure components are monitored through manual analysis and automated alerts where risk-based security monitoring, or a triage approach, is performed based on inherent risk of the anomaly or security event detected and the potential impact that said event could have on the Company's business operating environment. Security monitoring procedures are documented and consistently followed; documentation updates are made to the relevant security monitoring procedures-related documentation when required or when significant procedures-related changes are made. Regular security monitoring and detection-based reporting capabilities with metrics are mapped to business drivers for security monitoring purposes. Vendor-related and custom signatures are updated regularly based on threat intelligence information gathered for security-detection purposes. Centrally stored or monitored logs are maintained, and correlation and alerting capabilities are performed on a limited basis when unusual activity is suspected based on the information gathered from the security incident and event management (SIEM) system.

Development of a Response Plan

The incident response sections of the Cybersecurity Incident Response and Recovery Plan (CIRP) includes tactical procedures to help "triage," contain, monitor, or eradicate a security incident, including procedures to do the following:

- Respond to, recover from, and restore normal business operations in a timely manner with minimal, or no, business interruption or loss of data.
- Continuously improve the cybersecurity risk management program to limit the likelihood and impact of future incidents based on lessons learned from the Company's own experiences and those of others.
- Communicate with employees, stakeholders, regulators, and other constituents in a structured manner about the nature of the security incident, impact to the organization and others (if applicable), and the corrective action taken to recover.

The incident response sections of the CIRP have been created based on a threat scenario risk assessment performed annually as part of the review of the plan. The plan is focused on responding to those threat scenarios that have the highest impact and likelihood of occurring based on the business and markets in which the Company operates and the current technology environment. The incident response sections of the CIRP include the following key information:

- Response plan owners (those who can activate the plan), team members, and contact information for plan owners and team members
- Defined criteria required to activate the response plan
- Target business and IT performance metrics for operating in a "business as usual" environment
- Linkage to the business impact analysis and critical path recovery items within the disaster recovery (DR) and business continuity (BC) plans
- Alternate internal and external communication and operating methods to use when primary methods are unavailable
- Communication plan for notifying internal stakeholders (including legal, human resources, marketing, and investor relations), retained service providers (external counsel, forensics investigators, and the like), and external stakeholders (such as customers, vendors, regulators, and law enforcement) to manage expectations and information disclosure as part of the overall response effort. The communication plan also includes communication templates for certain formal internal and external communications, including, but not limited to, internal IT outage notifications and public press releases.
- Facility recovery procedures providing linkage to the DR and BC plans regarding the hosted hot site facility located in Syracuse, NY, and the alternate call center located in Troy, MI
- Data response procedures providing linkage to the backup policies and procedures, as well as the DR plan, regarding offsite data storage and backup media
- Hardware and software access procedures enabling IT service and operations during response and recovery procedures
- Response and recovery metrics focused on the target response and recovery milestones to enable effective management, measurement, and monitoring of recovery activities
- Detailed incident response and recovery procedures to be executed based on the identification of the root cause, including operational steps to eradicate any infections, malicious code, unauthorized user accounts, and the like, and restore systems in accordance with priority and dependencies

It should also be noted that mitigating processes and controls are evaluated as part of the current CIRP-related processes and controls in place to detect and respond to security incidents and events. (These mitigation process and control factors may be directly related to the CIRP or may be part of other security monitoring related controls.)

The CIRP is reviewed annually and approved by the following members of management:

- CISO
- CIO
- CTO
- CRO
- GC
- Chief Marketing and Communications Officer
- Director, Security Operations
- Director, Crisis and Response Management

Implementation Activities to Mitigate and Recover From Identified Security Incident

The plan activation process begins when one or more of the incident response and recovery plan owners are informed of a cybersecurity event for which incident response is imminent or underway. The plan owner will ensure details about the cybersecurity event are clearly understood and documented to the extent necessary to enable future communications. This includes the identification of security monitoring or other mitigating processes and control factors, which may be present, and reduce the overall impact of the identified security event. Should the plan owner decide to activate the plan, he or she will convene an emergency meeting of the CIRP leadership team (including the CIO, CISO, CRO, GC, VP of human resources, and CFO) to determine the following:

- Immediate tasks
- Departments and functions required to carry out the plan based on the cybersecurity event
- The initial communication plan and the individual assigned to execute the plan

Once agreement is made, the leadership team is responsible for notifying members of their teams and others, including external advisors (such as investor relations and external general counsel) about the plan activation, initial decisions made, and assigned actions.

Once activated, XYZ considers the current cybersecurity event and its effects on systems and business operations. The Company refers to the appropriate sections of the BC and DR plans, as well as the relevant and applicable data backup logs, to identify the following:

- Where the IT systems and IT infrastructure affected by the cybersecurity event reside within the asset prioritization hierarchy
- Where the business operations affected by the cybersecurity incident or event reside within the operations prioritization hierarchy
- The planned alternative IT systems (such as the failover or load-balanced servers and network devices) and business processing activities (for instance, manual sales order forms) for the affected components of the environment
- The time prior to the cybersecurity incident or event from when the Company will be able to respond to and recover from (recovery point objective [RPO]) for the affected IT systems and IT infrastructure
- The maximum length of time until IT systems, IT infrastructure, and business processes affected by the cybersecurity incident or event is returned to normal business operation, after which significant negative impact may occur (recovery time objective [RTO])

For each IT asset (hardware and software, including virtualized assets) affected by the cybersecurity event, an evaluation will be made to determine the appropriate response and recovery actions, such as the following:

- Decommission and replace
- Reconfigure with enhancements (firmware updates, vendor patches, configuration changes)
- Reconfigure with no enhancements

Recognizing that the Company may not be able to complete the chosen recovery action in a timely manner in relation to the RTO, an alternative solution will be determined to enable a return to normal processing.

Data restoration is based on the activities outlined in the backup and recovery policies and procedures. The backup procedures apply to the following:

- Network devices—such as configurations, access control lists, and firmware
- Physical and virtual servers (DNS servers, email servers, FTP servers, application servers, database servers, web servers)—operating systems, application programs, and application data
- Networked file shares
- End user computing (desktops, laptops, tablets, mobile devices) and peripherals (such as printers and copy machines)
- Telephone and voicemail systems

XYZ Manufacturing leverages a global backup management solution to manage the backup processing and monitoring of all IT assets connected to the environment. The backup solution is connected to a virtual storage area network (SAN) and supplemented by real-time disk imaging to an offsite facility for the highest-value IT assets and data. Moderate- and lower-value information and IT assets are backed up to electronic, removable media and stored at a secure offsite facility for the period of time defined by the backup and recovery policies and procedures. Backup method and frequency is based on the volume and frequency of information processing and the importance of the data or IT asset.

Restoration of data, software, and configurations is made using the global backup management solution. Prior to restoring data, software, and configurations to the live environment, the Company will conduct tests in the security sandbox against the backup media to determine if the cybersecurity event is present. Based on results, the Company may seek to leverage an older backup or execute the eradication techniques that were successfully employed in the production environment.

Communications related to a cybersecurity event are governed by the CIRP leadership team. Throughout recovery efforts, XYZ will communicate to the extent possible, and as required, with employees, stakeholders, regulators, or law enforcement through formal written and verbal communications (email, press releases, mass voicemail) that are structured to be informative, easy to understand, and transparent and that address the following:

- Current understanding of the cybersecurity incident or event
- The known impact of the cybersecurity incident or event
- The current status of remedial action being taken in response to the cybersecurity incident or event communications are tailored to specific audiences (all employees, individuals of whom specific action is required, public domain), leveraging templates that have previously been created and preapproved by appropriate members of executive management and external advisors

Within 10 business days of returning to “business as usual,” the CIRP requires a formal meeting of the full cybersecurity incident response and recovery team. The purpose of the meeting (which may be held via teleconference, videoconference, or in person) is to discuss lessons learned from the event and additional actions required. Defined criteria are included within the CIRP to help determine the structure of the meeting, the documentation required, and the monitoring that will be performed to ensure any new correction action agreed upon or implemented since the occurrence of the cybersecurity incident or event continues to operate over a period of time. During the meeting, at a minimum, the following are discussed:

- Identified breakdown in processes or controls, if any
- Enhancements that may need to be made to the process for identifying security monitoring or other mitigating processes and control factors, which may be present in the

environment and reduce the overall impact of the identified security event, prior to plan activation

- Changes required to standard configurations and the status of changes to other comparable systems that have yet to be attacked (as well as confirmation that those systems have not been compromised)
- Changes to the CIRP or the response team that would benefit incident response or recovery capabilities
- Capital investments or additional operating expenses required to more effectively prevent or detect a similar cybersecurity incident or event
- Changes to business partner relationships that may enable better response or recovery actions to be taken for future cybersecurity incidents or events
- Changes to CIRP test scenarios

The meeting minutes from the discussion are documented and appended to the CIRP.

Once per quarter, as part of the crisis management and incident response readiness activities, formal tests of response and recovery procedures are performed. Tests are based on overall business-based scenarios that have been developed to confirm awareness of and education about the CIRP and related plans (such as the DR and BC), as well as to hone plan content in an effort to continuously improve response and recovery capabilities.

Tests performed during three of the four quarters are "tabletop" exercises in conference rooms, leveraging tele- and video conferencing as necessary to conduct a virtual simulation with the CIRP team and other stakeholders. Tests performed during the other quarter involve a real-life simulation where a simulated cybersecurity incident or event is triggered. Only the CIRP leadership team is initially aware of the simulation. XYZ executes the response and recovery plan in a "real-life" situation until the point when communication with internal and external stakeholders would be required. The Company then completes the simulation as if it were a real event. Test results produced from this simulated event are formally discussed; ongoing updates are made to the CIRP as deemed necessary.

Management of Processing Capacity to Provide for Continued Operations During Security, Operational, and Environmental Events

Policies and processes are implemented to address capacity management and include the use of the Information Technology Infrastructure Library (ITIL) IT service management framework for capacity management. Performance management and capacity monitoring tools are used to real-time information to the network operations centers. Alert levels are established based on asset priority and failover capability for the load-balanced and redundant components. Alerts may be in the form of a yellow or red color indicator on the operator console within the network operations centers. The automatic creation of a problem ticket in the service management system for investigation and resolution, or an automated text and email to the on-call IT operations lead, is acceptable.

Detection, Mitigation, and Recovery From Environmental Events and the Use of Backup Procedures to Support System Availability

Policies and processes are implemented to address the detection, mitigation, and recovery from environmental threats. The primary computer facility houses key IT infrastructure for the Company's integrated ERP system and midrange platforms supporting manufacturing software. The facility has been specifically designed to mitigate the risk of environmental threats to the computer hardware operations and include protection from fire and the loss or fluctuation of power, cooling, and humidity.

Fire suppression systems, in combination with smoke detection and handheld fire extinguishers, are installed throughout the Company's facilities. Preventive maintenance is performed annually along with required inspections. An uninterruptible power supply (UPS) system provides continuous conditioned power through its strings of batteries to all infrastructure hardware to control unanticipated power interruptions. Maintenance for the UPS and batteries is performed at least quarterly. Emergency generator systems are required to be installed within the secure perimeter of the data center facilities.

They are sized to provide 100% of the data center's electrical service in the event of a utility service failure. These generators have scheduled maintenance performed at least quarterly. The temperature and humidity inside the data center are controlled by dedicated air conditioning systems for computer hardware. These units act independently of any general building air conditioning. Maintenance is performed at least tri-annually. The data center environment, temperature, humidity, power, and fire prevention systems are required to be monitored through a building management system within the command operations center. Operations personnel man the facility 24 hours a day, 7 days a week.

Physical Access

Access to the computer facility entrances and to the network operations centers (including the raised floor areas) is controlled by the badge access reader system. Building access points are required to be locked at all hours except for the main entrance, which can be unlocked during normal business hours and manned by a security guard. At each facility entrance, visitors are required to provide relevant identification, such as name, representing company, and employee contact. All visitors receive a visitor badge and sign in on the visitor log. All personnel are required to display their badge at all times while in the facility. Visitors are escorted while in restricted-access areas of the facility; when leaving, they are required to sign out on the visitor log. Video cameras are monitored 24/7 and provide surveillance over the interior and exterior of the building. All camera activity is recorded on digital video and retained for at least 60 days.

Backup Media

Data and programs are backed up in accordance with defined schedules. The backup schedule, rotation schedule, and retention period of tapes at the offsite storage facility are determined based on business need. The offsite tape storage is located approximately 30 miles from the computer facility. Backup job failures are monitored and tracked to resolution through the incident management process. Monitoring tools established in the job scheduling and monitoring process are utilized to monitor backup jobs. Job monitoring tools are in place to automatically generate an incident ticket in the incident management system for backup failures. Tape management systems are used to manage tape activities in the data center. Features of these systems include onsite media inventory, offsite media inventory, picking list for the vault, distribution list for the vault, and scratch lists.

The tape management systems produce reports to facilitate tape movement between the tape racks and drives in the data center, as well as between the data center and the offsite facility. Tape rotation is monitored. Reports are reconciled daily, and discrepancies are evaluated and resolved. Periodic inventories of tapes located both onsite and at the offsite facility are required to be conducted. Backup media is periodically tested. Periodic testing of backup media is coordinated by the business continuity team and performed by the appropriate technology groups.

Alternate Processing

BC plans are in place for all major business units and updated on an annual basis. DR plans are in place to support BC plans covering the critical IT infrastructure and networking equipment. The DR plan is updated annually. The main data center is physically separated from business operating units and dedicated solely to processing functions. The DR plans are reviewed annually and tested at least once a year. During a testing exercise, locations that are part of the testing exercise access the DR location through VPNs to segregate the network and prevent interruption to production services.

All business units with RTOs of less than 72 hours participate in a DR exercise once every 3 years. Business units with RTOs of 48 hours or less participate in the recovery testing exercise on an annual basis. The results of the tests are documented and assembled into a problem and resolution log.

Identification of Confidential Information When Received or Created, Determination of the Retention Period for That Information, Retention of the Information for the Specified Period, and Destruction of the Information at the End of the Retention Period

Policies and processes are implemented to address capacity management and include the following.

Data Classification and Retention

The data classification and retention policy and relevant security and confidentiality policies describe how information is designated as confidential and ceases to be confidential. The handling, destruction, maintenance, storage, backup, distribution, and transmission of confidential information are documented in the data classification and retention policy, XYZ's general business terms, and in some cases, in customer and business partner-specific contracts and service-level agreements.

Confidential policies and processes have been implemented to limit access to logical input routines and physical input media to authorized individuals. Each type of confidential information is classified, handled, secured, retained, and disposed of. All nonpublic customer information is confidential. Data that carries a confidential classification is subject to the Company's information security policy, which defines protection requirements, access rights, and access restrictions, as well as retention and destruction requirements.

Customer, vendor, and business partner information is presumed to be confidential (as a default) unless obviously not.

As part of their standard process for establishing service levels and operational protocols with vendors or business partners such as ABC Cloud and UVW Trading, XYZ will evaluate data shared between the two organizations and agree on what is confidential. XYZ also requests that business partners disclose their security, data classification, and retention policies to ensure that XYZ's data is afforded the proper retention and information protection. The CISO, with the information security team, is responsible for maintaining and updating confidentiality, system security, and related policies.

At the time of hire or affiliation, the code of conduct and confidentiality agreements that employees are required to sign prohibit any disclosures, beyond the extent authorized, of information and other data to which the employee has been granted access. Individual manufacturing contracts also define how confidential information is authorized and rescinded. Signed nondisclosure agreements are required from third parties before information designated as confidential can be shared with them. XYZ's business partners are also subject to nondisclosure agreements or other contractual confidentiality provisions, as outlined in the business associate agreement. Customer contracts, service-level agreements, and vendor contracts are negotiated before performance or receipt of service and formally signed off on by management.

Logical Access

Customers, groups of individuals, or other entities are restricted from accessing confidential information, other than their own. Users, contractors, or vendors who have the ability to access confidential information are properly authorized or supervised, in line with the Company's employees. The information supervisor for a business unit determines whether users require access to confidential information to perform their specific job functions.

Data Retention

Retention periods, and policies for ensuring retention during the specified period and proper disposal of data at the end of the retention period, are also outlined in the data classification and retention policy. The retention period assigned to data is based on the (1) classification of the data, (2) regulatory requirements and legal statutes, and (3) the general requirements of the business.

During the designated retention period, XYZ ensures that backup media (whether offline or online) are stored in a protected environment for the duration of the designated document retention period. Computer backup media is included. When the retention period has ended, XYZ Manufacturing destroys the information securely. Electronic information and other information are disposed of securely by proven means.

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

www.kaplanfinancial.com | 332 Front Street South, Suite 501, La Crosse, WI 54601 | 800.824.8742