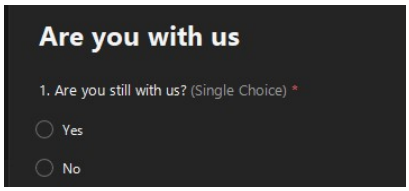
Advanced Cybersecurity Awareness in Accounting—What You Need to Know

(CYBA4)

KAPLAN

Tips for a Successful Experience

- **Technical Difficulty?** Try refreshing your page, reconnecting to the class, or rebooting (chat the moderator if you do this, so they can keep track of your presence). Also, logging in under your company's VPN may cause technical difficulty. Turn off your pop up blocker! Tech Support Team 866.265.1561 Option 1 then Option 2
- **Earning CPE:** Throughout the presentation a presence manager will pop up to check your attendance. Answer the questions with the appropriate response to record your attendance. Credit is earned by acknowledging 75% of these pop-ups per hour.



- **Chats:** You may be asked to reply to the moderator in the chat box to confirm attendance. Please be aware of any chats.
- **Questions:** Use the Chat box to ask any questions you may have about today's webcast. Someone is available to assist with your technology related concerns. The instructor will address your content related questions during the presentation or follow up after.
- **Once you are logged in please do not log out even during breaks.**

Unit 1

Cybersecurity Awareness and Data Safeguarding

KAPLAN

Audience

CPAs, accountants, and financial professionals within firms that provide audit, tax, financial statement compilation, and/or consulting services or within large companies who consult with IT service organizations

Objectives

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

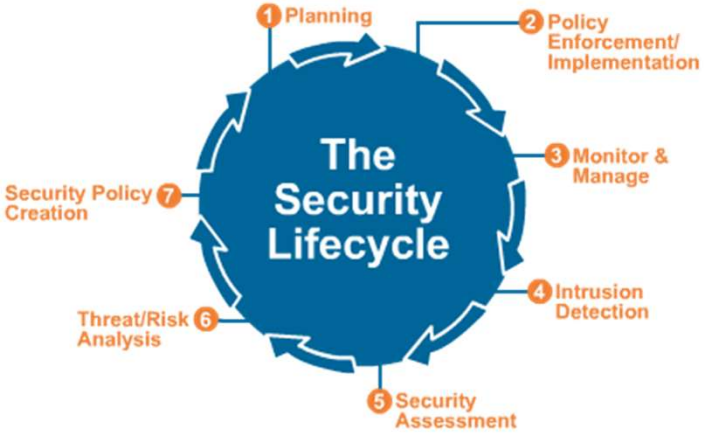
Topics

- Safeguarding Client Data
- Major Cybersecurity Threats (Social Engineering, Ransomware, Phishing, Fraud, Hackers)
- Third-Party Assurance (SOC, PCI, HITRUST)
- AICPA Cybersecurity Toolkit
- AICPA Professional Code of Conduct Disclosing Information to a Third-Party Service Provider (1.700.040)

Introduction

Organizations have an increasing need to demonstrate that they have to evaluate security threats, mitigate their vulnerabilities measure, and manage security risk.

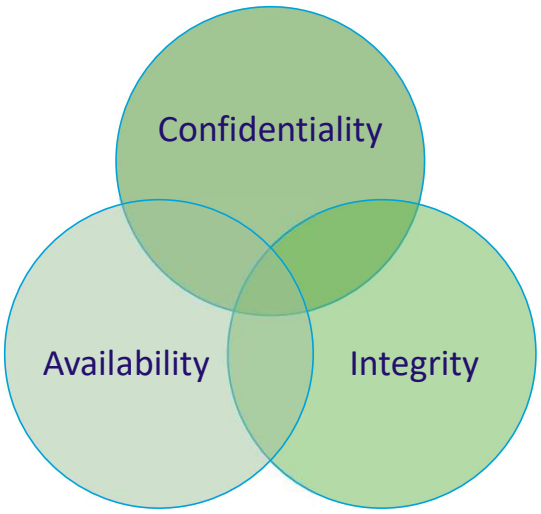
CPAs are often on the forefront of an organization's security program, by either controlling the budget, running the security program implementation, or testing.



Question

- Does anyone know what CIA stands for?

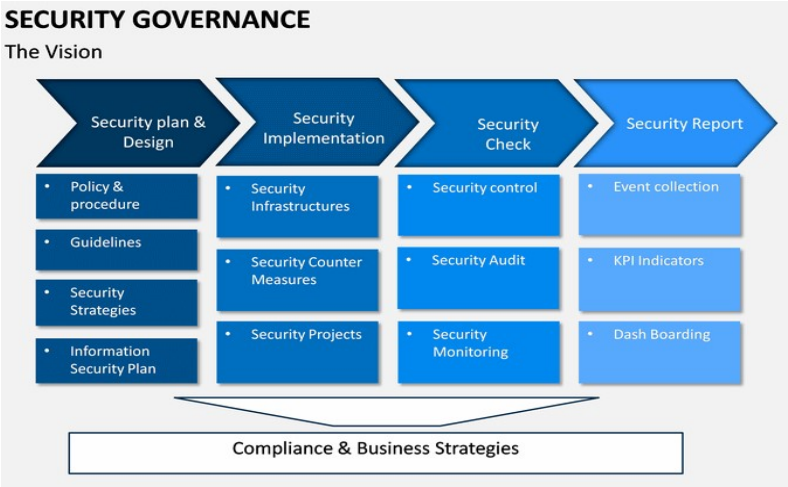
Answer



Information Security

Information security is comprised of a number of factors:

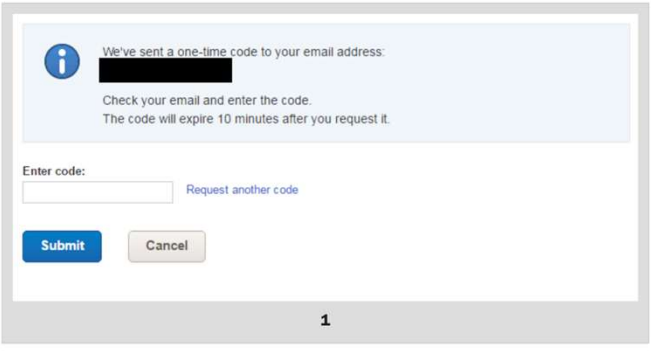
- Compliance
- Policies controls
- Relationship Management
- Incident response and management



Cybersecurity Threat Landscape

Polling Questions

- Do you use a password vault at work or at home?
- Do you use two-factor or multifactor authentication for work or personal use?



Question

Which of the following four passwords is the most secure?

a. Boat123

b. WTh!5Z

c. Into*48

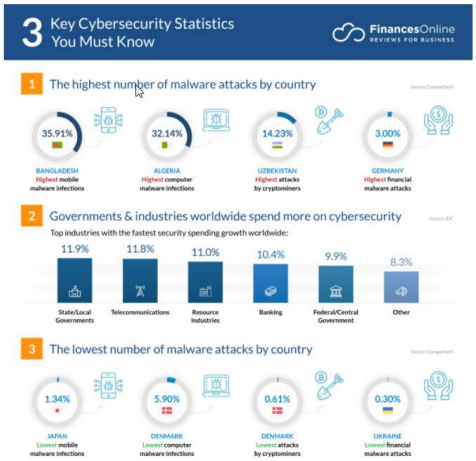
d. 123456

e. Not sure

Answer

c. Into*48

Cybersecurity Statistics: 2020/2021



https://financesonline.com/cybersecurity-statistics/

Top Data Breaches of 2021

Stripchat

- A database breach containing 200 million records belonging to Stripchat — an adult cam site was discovered. The database included 65 million user records that contained email addresses, IP addresses, the number of tips they gave to models, a timestamp of when the account was created and the last payment activity.
- Another database containing about 421,000 records for the platform's models, including usernames, gender, studio IDs, tip menus and prices, live status, and the model's "strip score."
- It was reported that the exposure could pose risks for both Stripchat viewers and models.

Raychat

- Iran business and social messaging application Raychat suffered a large data breach. Millions of its user records were exposed to the internet and then destroyed by a cyberattack involving a bot.
- The company stored its user data on a misconfigured MongoDB database, a NoSQL database used by companies who handle large volumes of user data. When misconfigured, the database can leave millions of documents vulnerable.
- NoSQL databases like Mongo are targets "for bot attacks operated by malicious actors who scan the internet for open and unprotected dbs [databases] and wipe their contents, with only a ransom note left."

Android

- In May, security researchers discovered the personal data of more than 100 million Android users exposed due to several misconfigurations of cloud services.
- Unprotected in real-time databases used by 23 apps, the downloads ranged from 10,000 to 10 million and included internal developer resources.
- Check Point researchers discovered anyone could access sensitive and personal information, including names, email addresses, dates of birth, chat messages, location, gender, passwords, photos, payment information, phone numbers and push notifications.

Top Data Breaches of 2021

SuperVPN, GeckoVPN and ChatVPN Data Breach

- A breach involving several widely used Android VPN services — SuperVPN, GeckVPN 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.

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.

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.
- 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.

Top Data Breaches of 2021

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.

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, 2022.
- The data contained 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.

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."

Cybersecurity Threat Landscape

- The organizations involved were large enough and had pockets deep enough to afford the very latest in technologies and the cyber skill sets required to properly deploy them. In other words, there really seemed to be no good excuse!
- Individuals are learning over time that most of these organizations seem to apply more resources to managing the public relations response to a breach rather than to assisting those they have harmed; their users, customers, vendors, and business partners.

Cybersecurity Threat Landscape

- There has been what many see as unacceptable delays in announcing these breaches, in some cases holding the information secret for months, during which untold damage can be done to those whose lives are affected.

Causes of Data Loss (Threats)

The Open Web Application Security Project (OWASP)

- An online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.
- The Open Web Application Security Project (OWASP) provides free and open resources.
- It is led by a nonprofit called The OWASP Foundation.
- The OWASP Top 10-2021 is the published result of recent research based on comprehensive data compiled from over 40 partner organizations.

OWASP

2021 Top 10 Web Application Security Risks

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.

OWASP

2021 Top 10 Web Application Security Risks

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.

OWASP

2021 Top 10 Web Application Security Risks

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.

Top Security Gaps

Weak Security Controls	Failing to Measure and Track Risk	No or Unclear Policies
Improper Data Management	Budget Constraints (Funding, Talent, and Resources)	Lack of Disaster Planning

Who Are They?

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

- Organized crime groups
- State sponsors, usually foreign governments
- Terrorist groups

Who Else?

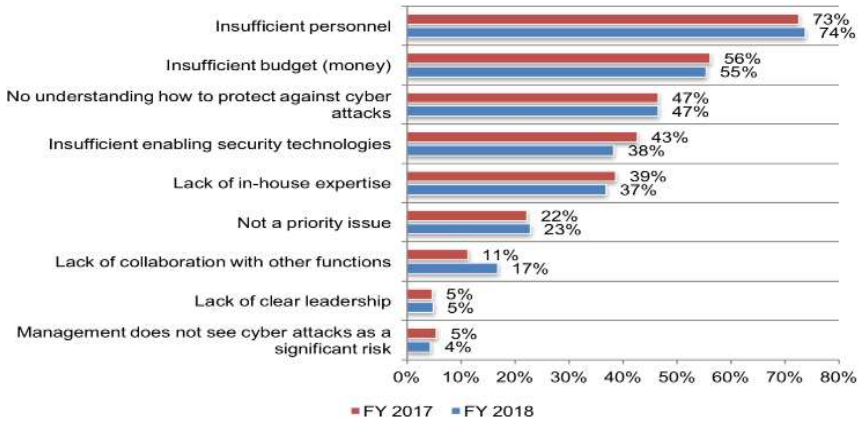
- **Hacktivists:** This includes those who hack not for personal gain, but to further a cause—for example, the Anonymous group that hacks from time to time for various political reasons.
- **Thrill hackers:** These people hack for notoriety. They deface websites and brag about their conquests to their fellow thrill hackers on websites where they share tools and methods.

Threat Agents

- **Operational:** Includes any process or procedure that can affect CIA (**C**onfidentiality, **I**ntegrity, **A**vailability).
- **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.

Why Do These Gaps Exist?

Figure 13. What challenges keep your IT security posture from being fully effective?
Three choices allowed



Defining Risk

Defining Risk

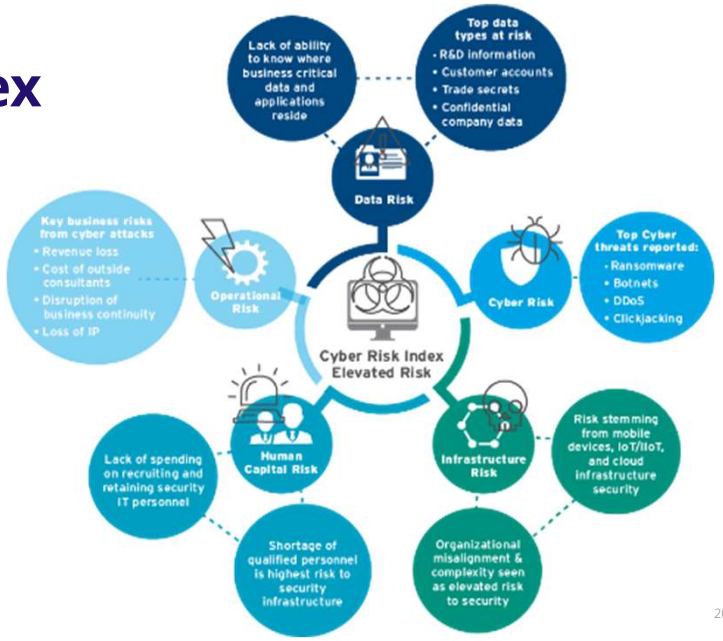
	Vulnerability	Threat	Risk
Definition	Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.	Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.	The potential for loss, damage or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

Data Breach Risks

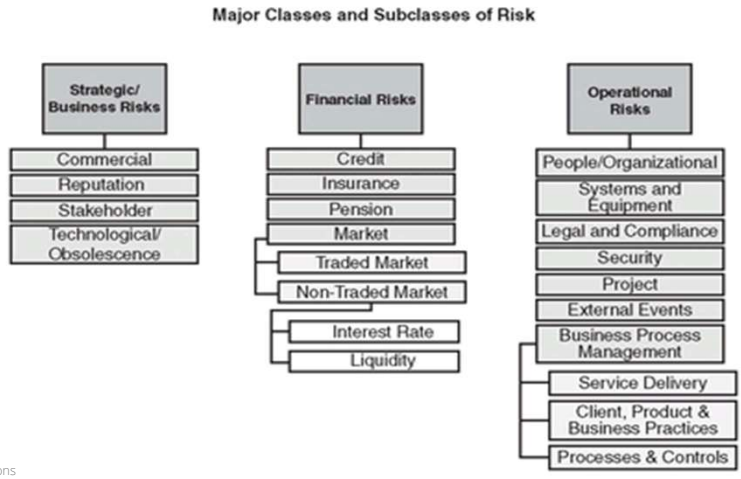
- Operational
- Market (Competitive)
- Compliance
- Reputational
- Financial

What Is Risk?

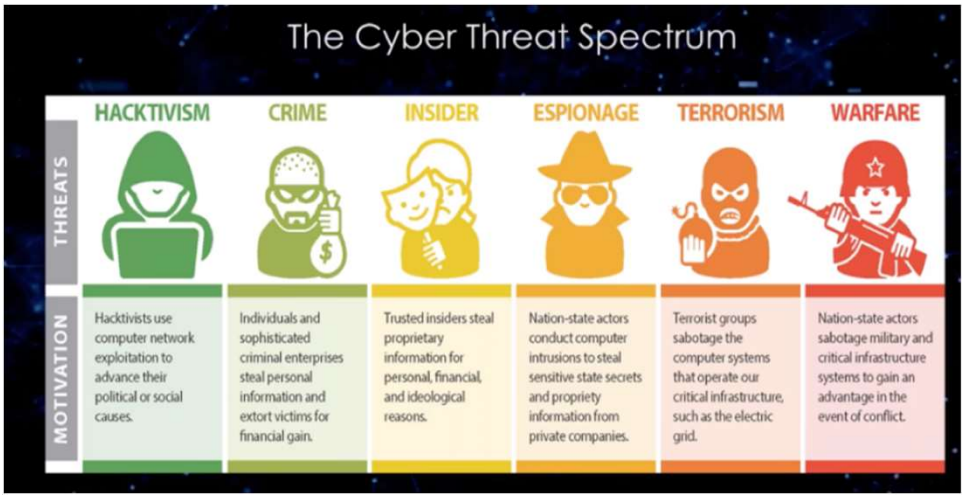
Risk Index



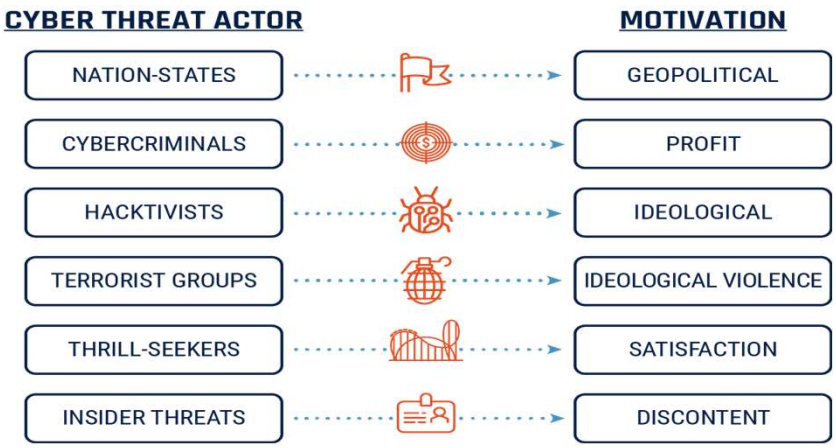
Risk Classification



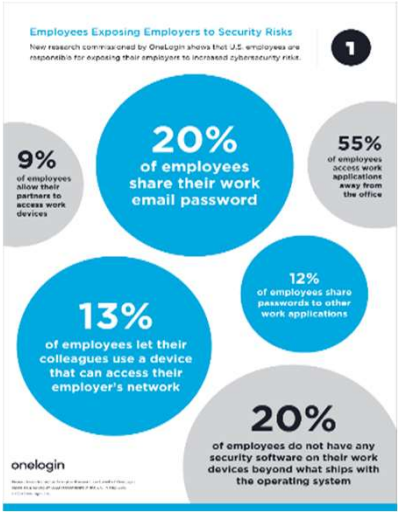
Deep Dive into Threats

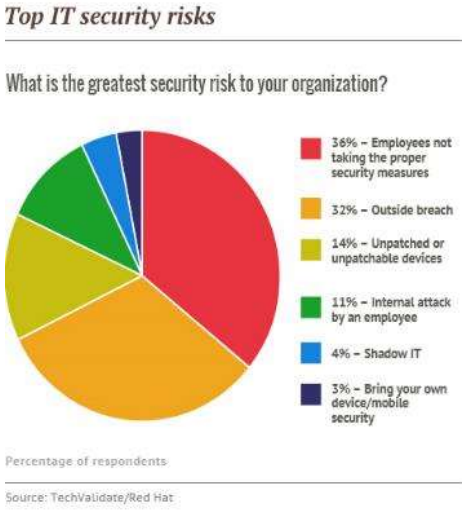


Threat Actors



Employee Security Risks





Third-Party Risks

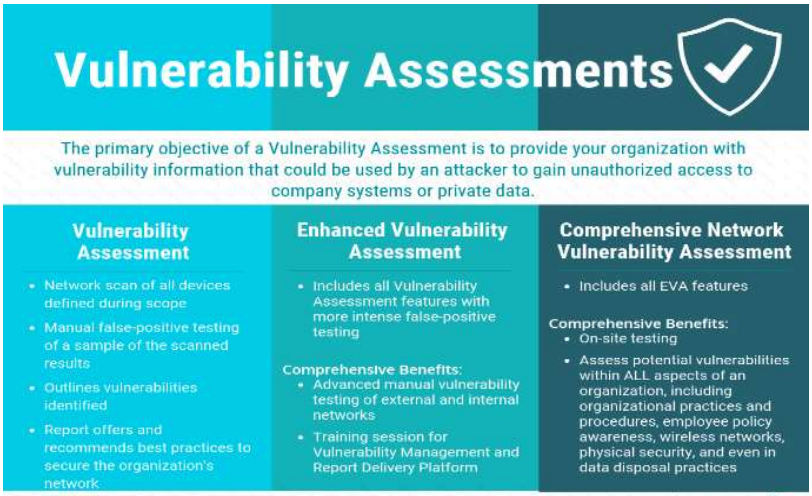
- Vendors
- Suppliers
- Business Associates (HIPAA)
- Processors (GDPR)

Vulnerability Life Cycle

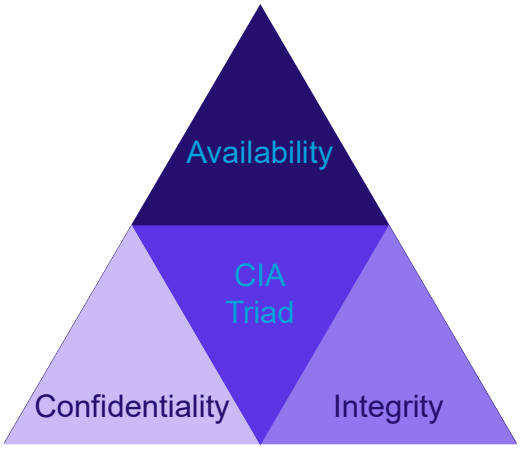
Defining Vulnerability

Vulnerability is a weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events.

Vulnerability Assessments



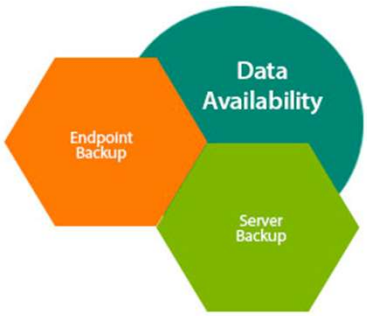
Core Cybersecurity Principles: The CIA Triad



Confidentiality

Integrity

Availability



CIA Examples

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Data Classifications

4 SKILLSET

Examples of Data Classifications

Risks Associated with Data

High Risk (Confidential)	Moderate Risk (Restricted)	Low Risk (Public)
• Protected health information • Personally identifiable information • Financial data • Employment records • Research data involving human subjects • User account or system passwords providing access to above elements	• Student records, except where covered under high risk • Unpublished regulated research data • De-identified health-related research data • WCM operational data • WCM intellectual property • Donors or potential donors • Information security data • Other internal WCM data, limited by intention or discretion of author or owner	• WCM public websites • Public Directory data • Publicly available research data sets • Otherwise unrestricted research data • Press releases • Job postings

What Do Attackers Want?

- Personally identifiable information (PII)
- Credit card data
- Trade secrets
- Personal financial information
- Personal health information (PHI); electronic protected health information (ePHI)
- Ransom cash/bitcoin

Question

Criminals access someone's computer and encrypt the user's personal files and data. The user is unable to access this data unless they pay the criminals to decrypt the files. This practice is called:

a. Botnet
b. Ransomware
c. Driving
d. Spam
e. None of the above
f. Not sure

Answer

b. Ransomware

Question

If a public Wi-Fi network (such as in an airport or café) requires a password to access, is it generally safe to use for sensitive activities?

a. Yes, it is safe

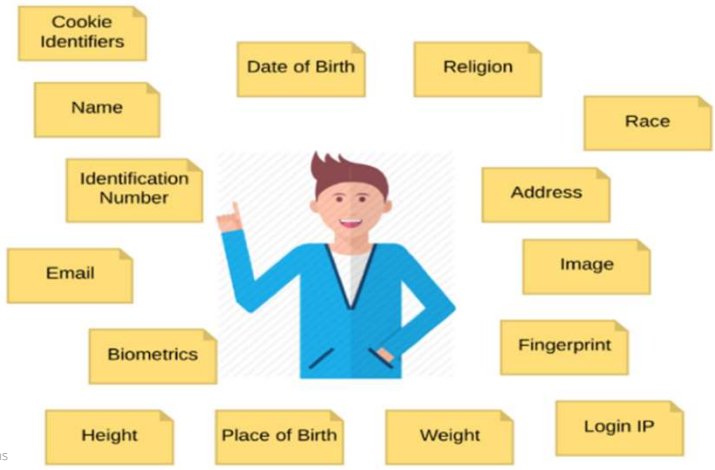
b. No, it is not safe

c. Not sure

Answer

b. No, it is not safe

Personally Identifiable Information (PII)

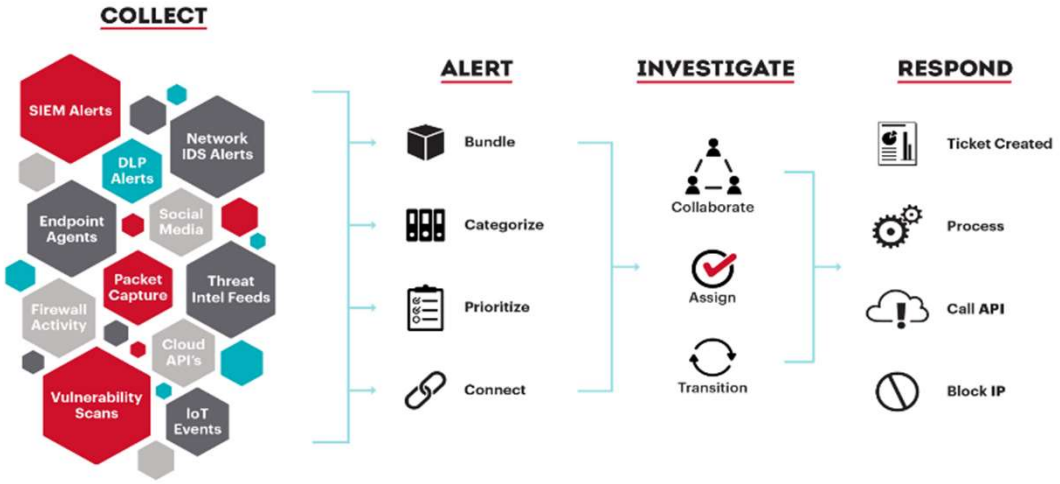


Personal Health Information (PHI)

Examples of PHI

- Names
- Addresses (including city, county and full zip codes)
- Dates Directly Related to Patient (including DOB, DOS and all ages over 89)
- Telephone Numbers
- Fax Numbers
- Email Addresses
- Social Security Numbers
- Medical Record Numbers
- Health Plan Numbers
- Account Numbers
- Certificate/License Numbers
- VINs, License Plate Numbers
- Device Identifiers and Serial Numbers
- URLs
- IP Addresses
- Biometric Identifiers (finger and voice prints)
- Full Face Photographic Images

Security Incident



Security Breach

How Do They Do It?

Social Engineering Threats

- Phishing
- Pharming
- Shoulder surfing
- Identity theft
- Dumpster diving
- Deepfakes

How Do They Do It?

Social Engineering Threats

- Pretexting
- Baiting
- Tailgating
- Piggybacking

How Do They Do It?

Malicious Software

- Trojan horse
- Virus
- Rootkit
- Worm
- Spyware
- Adware
- Ransomware

How Do They Do It?

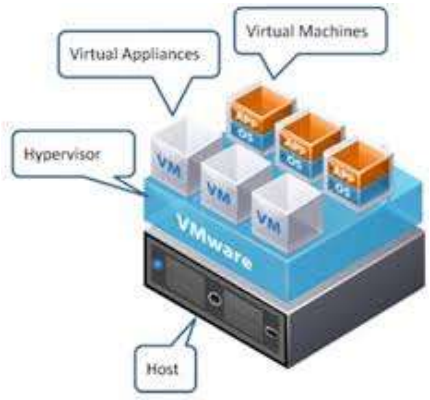
Mobile Devices

- 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
- Out of date devices
- Data leaks from apps on your mobile device

How Do They Do It?

Attacks on Virtualization

- VM escape (user "escapes" from the guest environment to access the host OS)
- VMware is the hypervisor software in this example
- Data remanence



How Do They Do It?

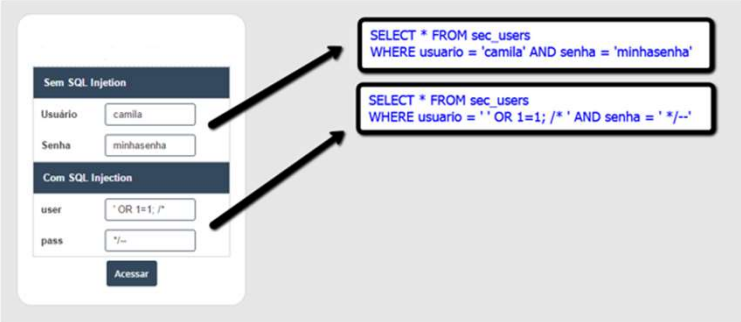
Web Servers

- 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

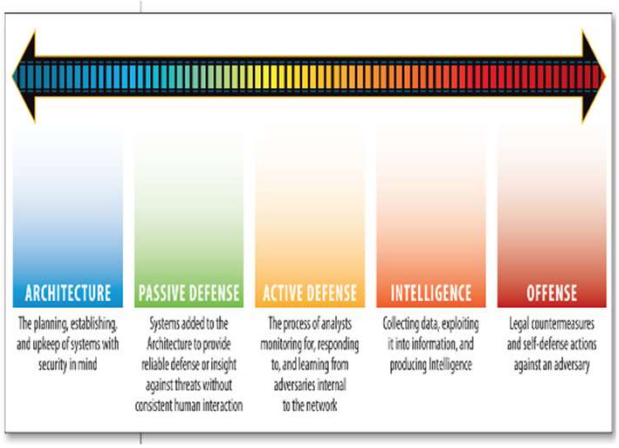
How Do They Do It?

Database Attacks

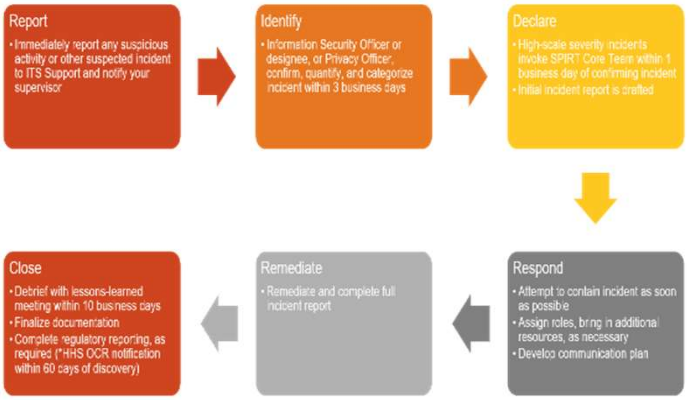
SQL injection



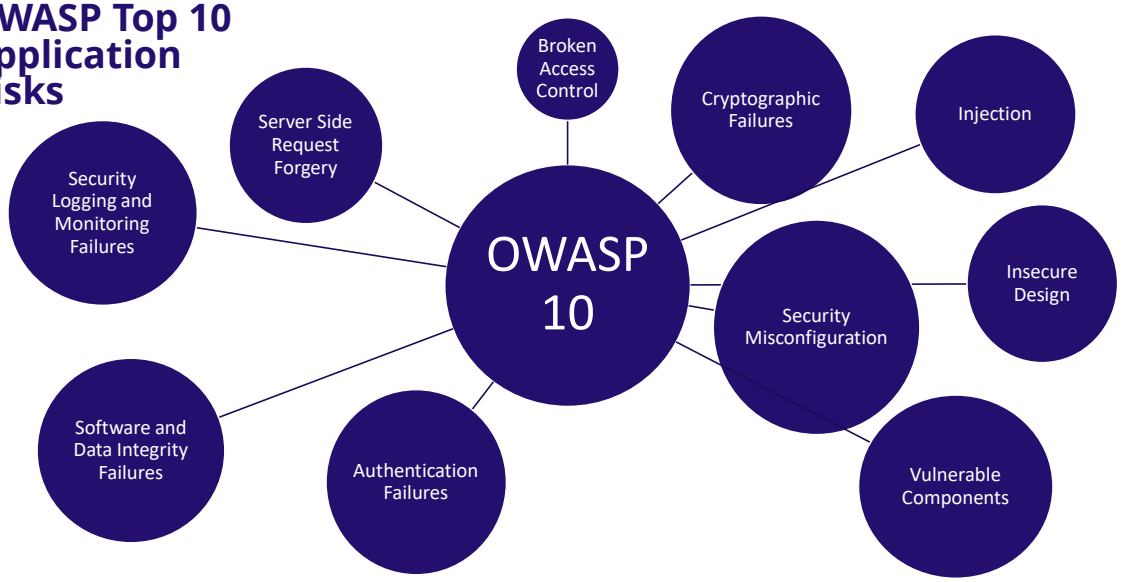
Offensive Security



Defensive Security



OWASP Top 10 Application Risks



Question

Which of the following is an example of a “phishing” attack?

a. Sending someone an email that contains a malicious link that is disguised to look like an email from someone the person knows
b. Creating a fake website that looks nearly identical to a real website in order to trick users into entering their login information
c. Sending someone a text message that contains a malicious link that is disguised to look like a notification that the person has won a contest
d. All of the above
e. Not sure

Answer

d. All of the above

Question

A group of computers that is networked together and used by hackers to steal information is called a:

a. Botnet

b. Rootkit

c. DDoS

d. Operating system

e. Not sure

Answer

a. Botnet

Activity 1

Mary is finishing up work on a project in a local cafe. Being somewhat security conscious, she has assured that her laptop screen cannot be seen by anyone in the cafe, both by sitting in a corner and by using a privacy screen (a darkened piece of plastic, which obscures the laptop screen to any prying eyes).

Mary connects to the café's open Wi-Fi network by first logging into a web page, which appears to be from the café's website, uses Google to search for a few items, and then enters her name and password to access her work email. However, Mary is unaware that the Wi-Fi network in the café has been compromised. 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 warnings and all her work files disappear 5 minutes later. Later, the security desk representative at Mary's employer becomes aware of the breach and shuts her access off.

Activity 1

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?

Activity 1 Answer

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

Activity 2

- 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.

Activity 2

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?

Activity 2 Answer

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.

Cybersecurity Regulatory and Legal Rules: Federal and State

Federal Laws

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.

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. The Act creates a voluntary cybersecurity information sharing process designed to encourage public and private sector entities to share cyber threat information.

Federal Laws

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): 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).

Gramm-Leach-Bliley Act (GLBA) of 1999: 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 security and identity theft rules.

Computer Fraud and Abuse Act (CFAA): This law defines "protected computers" and affects any entities that might engage in the hacking of "protected computers" which is defined in this Act as a as a computer used exclusively by a financial institution or the U.S. government.

Federal Laws

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: 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 Private-sector organizations that collect, use, and disclose personal information in the course of commercial business in Canada are covered by the PIPEDA.

Basel II: 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, an updated version of this regulation, was implemented in January of 2022.

Payment Card Industry Data Security Standard (PCI DSS)

Federal Laws

- Federal Information Security Management Act (FISMA) of 2002
- Economic Espionage Act of 1996
- USA PATRIOT Act
- Health Care and Education Reconciliation Act of 2010

Federal Privacy Laws

Federal Law	Type of Data Protected
The Health Insurance Portability and Accountability Act (HIPAA)	Medical data held by certain entities, like hospitals.
Gramm-Leach-Bliley Act (GLBA)	Personal financial data held by financial services firms.
The Fair Credit Reporting Act (FCRA)	Consumer credit data held by credit reporting agencies.
The Communications Act	Consumer network information held by telephone companies.
The Family Educational Rights and Privacy Act (FERPA)	Education records held by education institutions.
The Video Privacy Protection Act (VPPA)	Personal rental information for video rentals, video games, etc.
The Driver Privacy Act	Data gathered by electronic data recorders in vehicles.
The Children's Online Privacy Protection Act (COPPA)	Personal data of children under 13 that is collected online.

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 people who are citizens of or reside in the countries which make up the European Economic Area ("EEA").
- The regulation went into effect on May 25, 2018.
- The GDPR has levied harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

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).

State Privacy Laws

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)

***Effective January 1, 2023**

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.

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.

Virginia's Consumer Data Protection Act (CDPA)

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

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, so it's a good idea to keep an eye on this law as it evolves.

Colorado Privacy Act (CPA)

In June 2020, Colorado became the third U.S. state to pass a privacy law. It contains some similarities to California's two privacy laws as well as Virginia's recently passed CDPA. It even borrows some terms and ideas from the EU's General Data Protection Regulation.

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 (July 1, 2023).

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).

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.

As of March 2020, the law is fully enforceable.

This law broadens the scope of consumer privacy and provides better protection for New York residents from data breaches of their personal information.

Scenario 1

Identifying the difference: When is notification required?

As a group, examine the scenarios in the handout and identify in which scenario breach notification is required. Assume that the laws provided are current. Research each state's Security Breach Notification Law, found at this link: www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Scenario Answers

- N.Y. Gen. Bus. Law § 899-aa "In the event that more than ***five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing…"*** The NY SHIELD Act (revises Section 899-aa and creates Section 899-bb) may also be applicable, which would require additional notification to the New York State Police, the State Attorney General, and the New York Department of State Office within ten days under certain circumstances; and, if the laptop data is related to certain categories of data (including financial or insurance firms/clients/customers), the NYDFS (New York Department of Financial Services) cybersecurity notification requirements would also apply, including providing notification to the NYDFS Superintendent within a certain timeframe.

- N.C. Gen. Stat. §§ 75-61, 75-65 "In the event a business provides notice to more than ***1,000 persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the attorney general's office."***

- Fla. Stat. § 501.171 ***"If a covered entity discovers circumstances requiring notice of more than 1,000 individuals at a single time, the covered entity shall also notify, without unreasonable delay, all consumer reporting agencies."***

Utah Consumer Privacy Act *(New)*

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 who 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 below.

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

Connecticut Data Privacy Act (CTDPA) *(New)*

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.

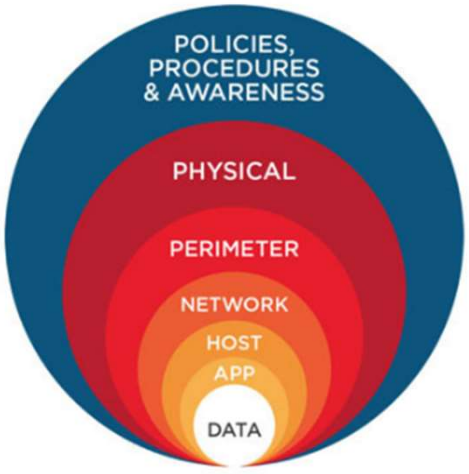
Like all privacy laws, the first thing organizations should consider is whether or not they fall under the bill's scope. The first threshold for Connecticut's new privacy law is that an organization must do business in Connecticut (CT) or market goods or services to CT residents.

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

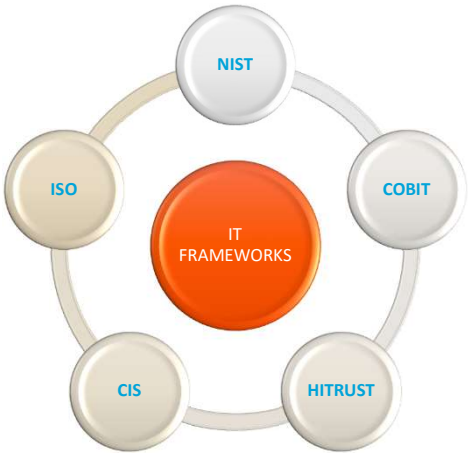
Limit Cybersecurity Risks by Applying Core Principles

Core Cybersecurity Principles

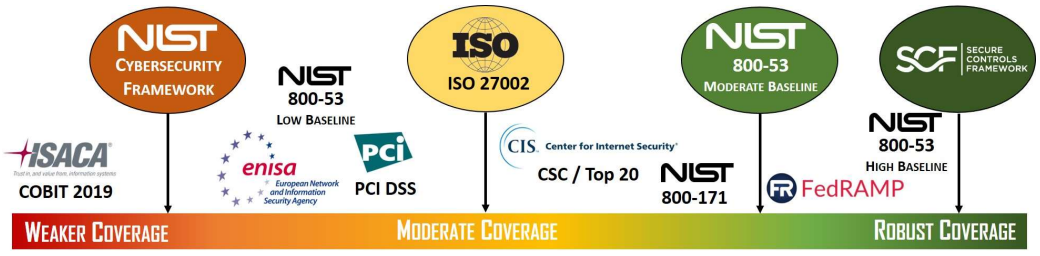
1) Confidentiality
2) Integrity
3) Availability
4) Defense-in-depth
5) Job rotation
6) Separation of duties
7) Principle of least privilege
8) Need-to-know principle



Top Security Frameworks

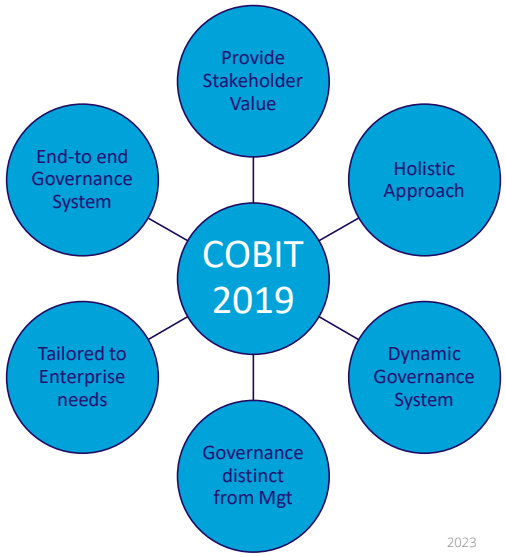


Security Coverage



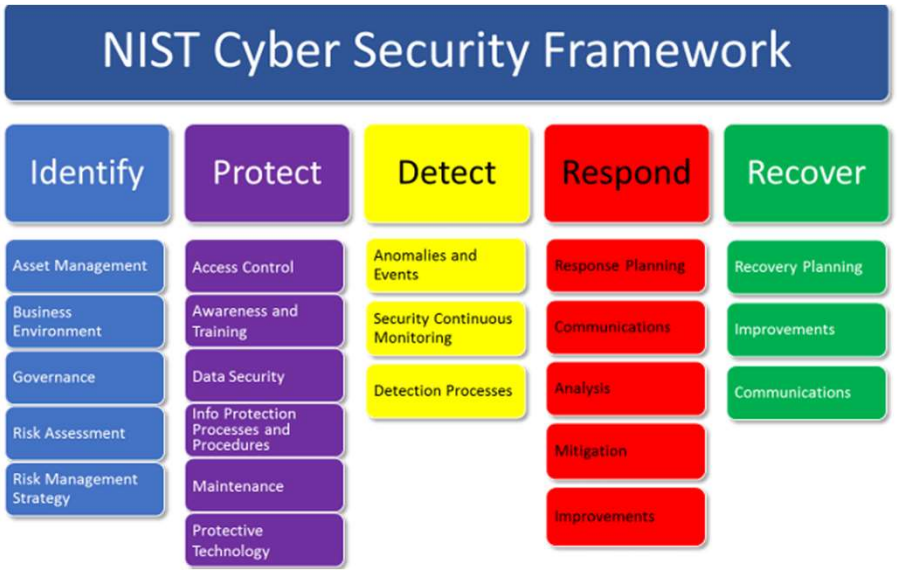
COBIT 2019

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



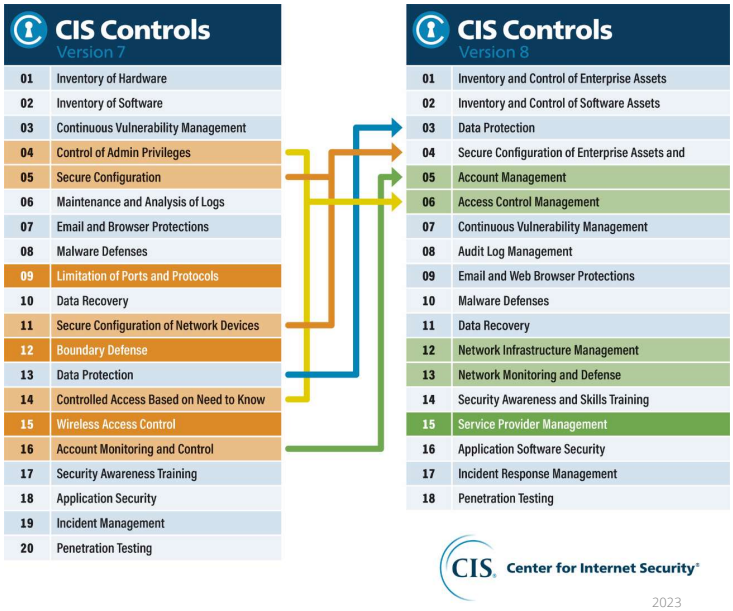
ISO 27001


ISO 27001 CONTROLS
1. Information Security Policies
2. Organization of Information Security
3. Human Resource Security
4. Asset Management
5. Access Control
6. Cryptography
7. Physical and Environmental Security
8. Operations Security
9. Communications Security
10. System Acquisition and Maintenance
11. Supplier Relationships
12. Security Incident Management
13. Business Continuity Management
14. Compliance
VARONIS


NIST Cyber Security Framework
Identify
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Protect
Access Control
Awareness and Training
Data Security
Info Protection Processes and Procedures
Maintenance
Protective Technology
Detect
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Respond
Response Planning
Communications
Analysis
Mitigation
Improvements
Recover
Recovery Planning
Improvements
Communications

CIS Controls

The CIS Controls (formerly known as Critical Security Controls) are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. On May 18, 2021, CIS launched version 8 of the controls, released at the global RSA Conference 2021.



HITRUST CSF

Recommendations from AICPA

- Risk assessment
- Account for sensitive data
- Require strong passwords
- Enable multifactor authentication
- Update software
- Audit security measures
- Monitor problems

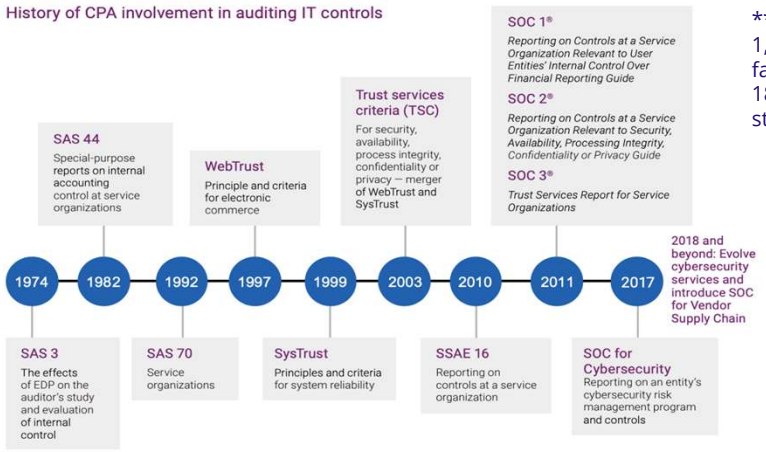
System and Organization Controls (SOC) for Cybersecurity

	SOC for Cybersecurity examination[6]	SOC 2 examination[7]
What is the purpose of the report?	To provide **general users** with useful information about an entity's cybersecurity risk management program for making informed decisions	To provide **specified users** (who have sufficient knowledge and understanding of the service organization and its system as discussed here) with information about controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy to support users' evaluations of their own systems of internal control
Who are the intended users?	Management, directors, and a broad range of general users including analysts, investors, and others whose decisions might be affected by the effectiveness of the entity's cybersecurity risk management program	Management of the service organization and specified parties **who have sufficient knowledge and understanding of the service organization and its system**
Who can perform the examination and under what professional standards and implementation guidance is the examination performed?	Independent CPAs under AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*) AICPA Attestation Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*	Independent CPAs under AT-C section 105, *Concepts Common to All Attestation Engagements, and AT-C section 205, Examination Engagements* (AICPA, *Professional Standards*) *AICPA Guide SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, processing integrity, confidentiality, or privacy*[8]

Sample SOC Cybersecurity Report

- Section 1–Assertion of the Management of XYZ Manufacturing
- Section 2–Independent Accountant's Report
- Section 3–XYZ Manufacturing's Description of its Cybersecurity Risk Management Program

CPAs: In the Cybersecurity Movement



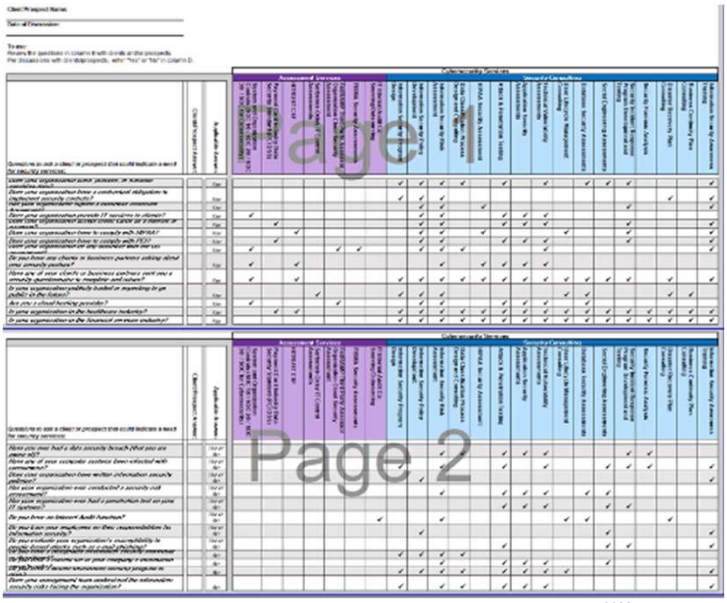
** Note that SOC 1, 2, and 3 reports fall under the SSAE 18 attestation standard.

Why CPAs?

1. **CPAs** are specialists in risk; CPA firms understand business and financial risk.
2. **CPAs** understand business; accounting is the language of business.
3. **CPAs** realize the importance of securing the information of their clients.
4. **CPAs** design, implement, and assess controls.
5. **CPAs** are often in company leadership positions.
6. **CPAs** are trusted to report on effective controls.

Client Assessment: Cybersecurity Service Opportunities

Tool is used to generate engagement with the Client to assess ways in which your firm can help them to enhance their security efforts.



Final Review

Principles, Regulations, and Rules

Any questions?

Unit 2

Cybersecurity Risk Management and Assurance

KAPLAN

AICPA's Cybersecurity Risk Management Framework

AICPA's Cybersecurity Risk Management Framework

Enables organizations to take a proactive approach to cybersecurity risk management

Intended for management to use to design and describe its cybersecurity risk management program

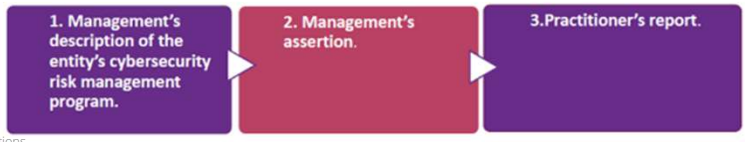
Key component of the new SOC for Cybersecurity engagement

AICPA's Cybersecurity Risk Management Framework

Examination results in the issuance of a general-use cybersecurity report designed to meet the needs of a variety of potential users

Report 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



XYZ Cybersecurity Program

- **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

XYZ Cybersecurity Program

- **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:
  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.

XYZ Cybersecurity Program

- **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

XYZ Cybersecurity 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

XYZ Cybersecurity Program

- **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

XYZ Cybersecurity Program

- **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

XYZ Cybersecurity 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

XYZ Cybersecurity Program

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

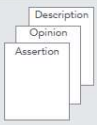
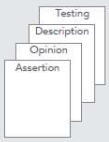
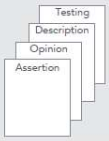
b. Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents

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 the specified period, and destruction of the information at the end of the retention period

Reporting Levels

Reporting Levels	Intended Audience	Benefits (Entity and Recipient)
• Entity 	• Board/audit committee • Management • Investor • Regulators • Analysis	• Provides transparency to key elements of the entity's cyberrisk management program • Improves communications • Enhances confidence in the integrity of info presented
• Service provider 	• Business unit management • Vendor risk management • Accounting/internal audit • CISO • BCP	• In addition to entity-level benefits, provides sufficient, detailed information to address the user vendor risk management needs
• Supply chain 	• Business unit management • Vendor risk management • Accounting/internal audit • CISO • BCP	• In addition to entity-level benefits, provides sufficient, detailed information to address the user's supply chain risk management needs

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) and present your group's assessment of the sufficiency with which the organization complies.

Performing Quantitative Risk Management

Quantitative Risk Analysis

- Equations are used to determine total and residual risks. The most common equations are for single loss expectancy (SLE) and annual loss expectancy (ALE).
- SLE is the monetary impact of each threat occurrence. To determine the SLE, you must know the asset value (AV) and the exposure factor (EF).
- EF is the percent value or functionality of an asset that will be lost when a threat event occurs.
- SLE = AV × EF

Quantitative Risk Analysis

For example, an organization has a web server farm with an AV of $20,000. If the risk assessment has determined that a power failure is a threat agent for the web server farm and the exposure factor for a power failure is 25%, the SLE for this event equals $5,000.

Quantitative Risk Analysis

- ALE (Annual Loss Expectancy) is the expected risk factor of an annual threat event.
- To determine the ALE, you must know the SLE and the annualized 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).
- ALE = SLE × ARO

Quantitative Risk Analysis

- Using the previously mentioned example, if the risk assessment has determined that the ARO for the power failure of the web server farm is 50%, the ALE for this event equals $2,500.
- Using the ALE, the organization can decide whether to implement controls.

Safeguard Selection

- The most common criteria for choosing a safeguard is the cost effectiveness of the safeguard or control.
- Planning, designing, implementing, and maintenance costs need to be included in determining the total cost of a safeguard.
- (ALE before safeguard) – (ALE after safeguard) – (annual cost of safeguard) = safeguard value

Safeguard Selection

- Implementing a safeguard can improve the ALE but will not completely do away with it.
- Knowing the corrected ALE after the safeguard is implemented is necessary for determining the safeguard value.
- A legal liability exists if the cost of the safeguard is less than the estimated loss that would occur if the threat is exploited.

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 $2,500 ALE.
- The organization may want to deploy a power backup if it can be purchased for less than $2,500 a year. 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.

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.

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.

Net Present Value (NPV)

- NPV considers the fact that money spent today is worth more than savings realized tomorrow.
- 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%. Divide the yearly savings ($2,500) 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:

NPV = $2,500 / (1.15) = $2,174 (rounded up)

Net Present Value (NPV)

- 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:

NPV = $2,500 / $(1.15)^2$ = $1,890 (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

- Total cost of ownership measures the overall costs associated with undergoing the organizational risk management process.
- Costs might include insurance premiums, financing, administrative costs, and any losses incurred.

Approaches to Handling Risk

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.

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.

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.

Accept. This strategy amounts to making the decision to do nothing and live with the risk.

Reasonable Assurance and Third-Party Risks

AICPA Professional Code of Conduct

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**.

AICPA Professional Code of Conduct

1.700.040 – Disclosing Information to a Third-Party Service Provider

.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**:

AICPA Professional Code of Conduct

a. 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 on the third-party service provider's controls and procedures to safeguard confidential client information.

b. Obtain **specific consent** from the client before disclosing confidential client information to the third-party service provider.

AICPA Professional Code of Conduct

1.700.040 – Disclosing Information to a 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. [Reference: paragraphs .001–.002 of ET section 391]

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 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

Tools

- **(SOC) for Cybersecurity:** Cybersecurity risk management reporting framework that assists organizations as they communicate relevant and useful information about the effectiveness of their cybersecurity risk management programs.
- **PCPS Cybersecurity Toolkit (The AICPA's Private Companies Practice Section):** Collection of learning resources, staff training tools, and tools to use with clients to assess their needs for cybersecurity services.

PCPS Cybersecurity Toolkit

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.

PCPS Cybersecurity Toolkit

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.

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.

PCPS Cybersecurity Toolkit

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 above, 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.

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.

PCPS Cybersecurity: Links to Other Resources

HACKED! Building defenses against and responses to intrusion

CPA cybersecurity checklist

Building a business model for cybersecurity

The Professional Ethics Executive Committee (PEEC) ....questions about independence when providing cybersecurity services. Frequently Asked Questions.

AICPA Cybersecurity Risk Management Framework

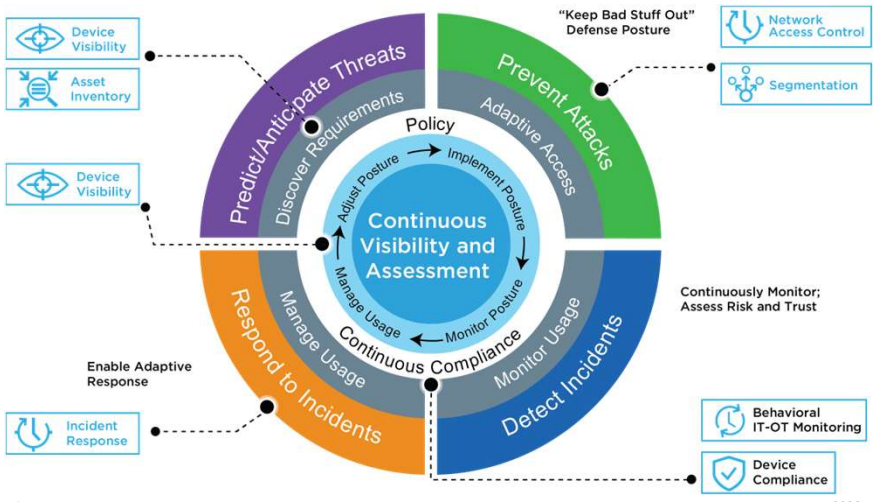
Cybersecurity Resource Center

Information Management and Technology Assurance Resources

Activity 4: Polling Question

Has your firm ever been reviewed under a cybersecurity risk assessment?

Final Points



Final Review

Cybersecurity Risk Management and Assurance

Any questions?

Reminders

- **Post event evaluation:** Please complete the course evaluation that will be viewable once the session ends. We welcome your feedback!


KAPLAN