DESIGN SECTION
Identifying New Threats to Privacy Data [Scene 1]

Slide 1.1

Course Open

CYB0153
Identifying New Threats to Privacy Data

Image:

VO: No VO.

Slide 1.2

Learning Goals

After this lesson, you will be able to:

1. Explain the history of threats to privacy data to predict future vulnerabilities.
2. Describe threat, non-approved share, and ransomware and how they relate to privacy data.
3. Recall CUI and its standards.
4. List three largely recognized categories to protect privacy data.
5. Describe three potential risk areas for data privacy in the future.

VO: Please familiarize yourself with the objectives of this topic.

Slide 1.3

Main Menu

Review of Privacy Frameworks	[Scene 2]
The Role of Threats and CUI	[Scene 3]

The Future of Risk Analysis and Privacy Protections	[Scene 4]
Assessment	[Scene 5]

VO: Choose a module from the list or click Next to continue.

Review of Privacy Frameworks
[Scene 2]

Slide 2.1

Lesson Open

Image:

VO: Welcome to Lesson 1. (Add Lindsay's standard lesson audio)

Slide 2.2

What is Privacy?

Image: Related stock video and/or image, with the animated lower MSI lower third.

Slide 2.3

Laying the Privacy Framework

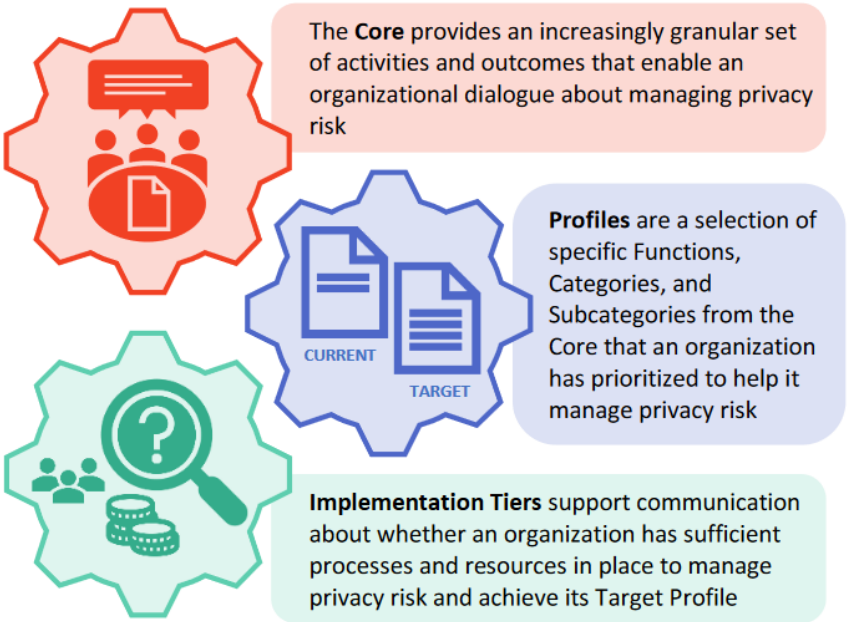


Figure 1: Core, Profiles, and Implementation Tiers

he

Image:

VO: For use in the field of cybersecurity, any discussion of privacy starts with the privacy framework outlined by the experts at NIST, the National Institute of Standards and Technology. Cybersecurity experts in both public and private roles have agreed upon these standards and adopting this universal framework creates opportunities for improved defense and awareness of challenges that are present in our industry every day.

VO: The framework itself is presented in three (3) basic areas: The Core (a listing of activities and outcomes), the Profiles (specific functions and categories that help manage risk), and the Implementation Tiers (a review of your current organizational infrastructure that outlines your readiness for managing risk). Over the next few slides, we will discuss each part in greater detail. Click each element of the graphic above to learn more.

Citation Credit:
https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

Slide 2.3.1

Framework Defined: The Core

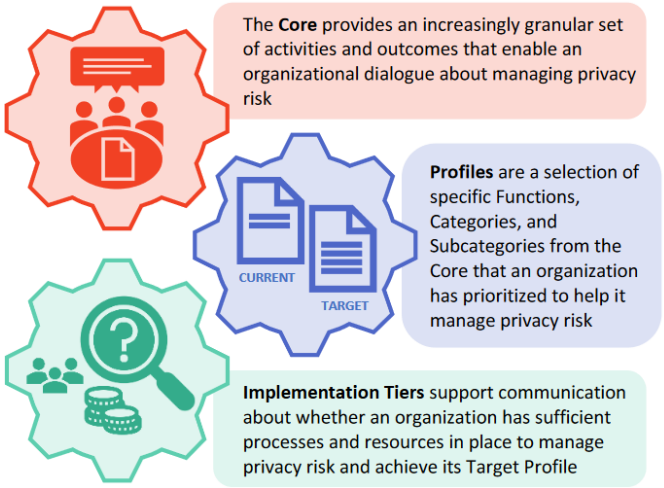


Figure 1: Core, Profiles, and Implementation Tiers

PR-P	Protect-P	PR.PO-P	Data Protection Policies, Processes, and Procedures
		PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology

Image:

VO: At the base level of your privacy framework you find the core, which is a set of rules and functions broken down into categories that give you the practical steps you need to minimize and manage overall organization risk at multiple levels of your company. As each function is defined, you will find certain cases where further details or instructions require each function to be broken down further into categories and even subcategories.

VO: For example, a basic risk management function like protecting your organization is so broad that the NIST framework breaks that down into five (5) different categories, including Data Security, Maintenance, and Protective Technology, just to name a few. For more information, review Appendix A of the NIST Privacy Framework. We've included a link to this document in the resources section of this presentation.

Citation Credit: (Link in Resource Tab)
https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

---

Slide 2.3.2

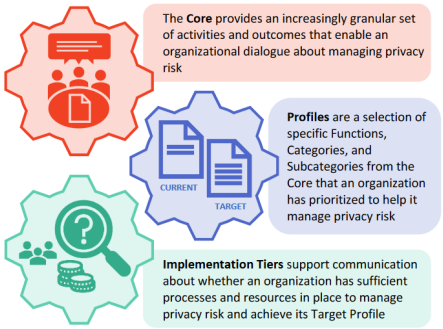
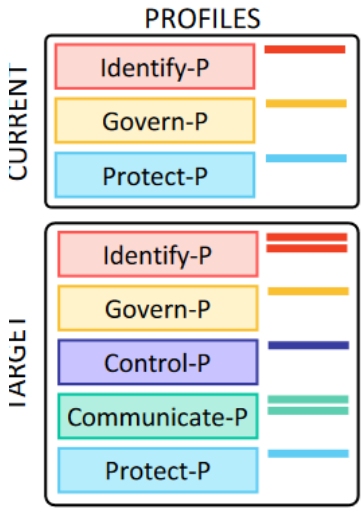


Figure 1: Core, Profiles, and Implementation Tiers



VO: As we move on in our discussion of the NIST Privacy Framework, we find the Profiles section is up next. In short, the profile area deals with two main conditions: the current (the now) and the target or future state (where you want to go). One important key to mention here is that before you can successfully guide your organization to an improved overall risk management position, you must spend adequate time creating and evaluating the current state of your everyday managed risk. While those needs may change from organization to organization, things like data management and long-term data storage are continual challenges that every organization must maintain in some shape or form.

VO: While there are levels of flexibility in how you proceed with creating your target profiles, one popular method in completing this step is to work backward, essentially starting with your target functions and outcomes (where you'd like to go) and then conduct a gap analysis to see how far you are from actually getting there. For example, the organization above has identified four functions in the Identify section of their Target Profile, but after completing a gap analysis discovered that they can't provide adequate current evidence to show examples of how only two conditions are currently being met.

Slide 2.3.3

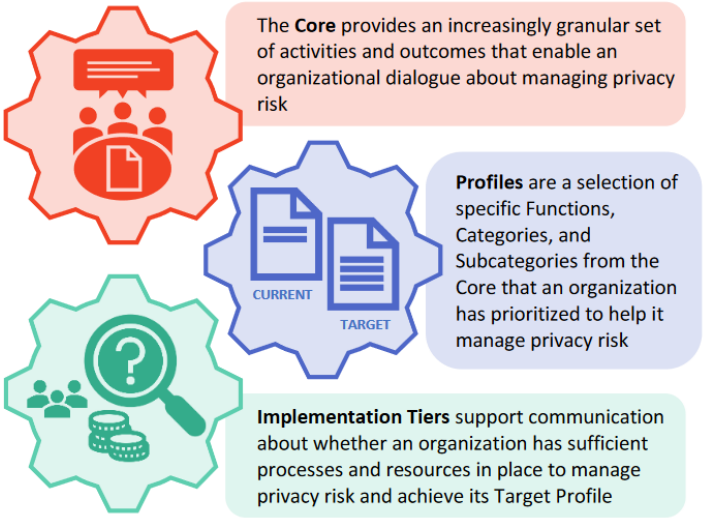


Figure 1: Core, Profiles, and Implementation Tiers

Tier 1: Partial
Tier 2: Risk-Informed
Tier 3: Repeatable
Tier 4: Adaptive

Image:

VO: The final point in our privacy framework is the implementation tiers, which provide a visual point of reference for how an organization views risk and whether that organization has the functions and processes built into its everyday operations to manage that risk. While NIST has outlined the five major functions of privacy and risk management (Identify, Govern, Control, Communicate, and Protect), the analysis and work to move along each implementation tier can and often do occur simultaneously. With new threat actors and increased levels of threat analysis continuing to challenge cyber experts, the urgency for data and systems protection remains a task that must be monitored and adjusted accordingly. The list above discusses the four implementation tiers.

For more information, refer to the NIST references available in the Resources section of this presentation.

Slide 2.4

Summary

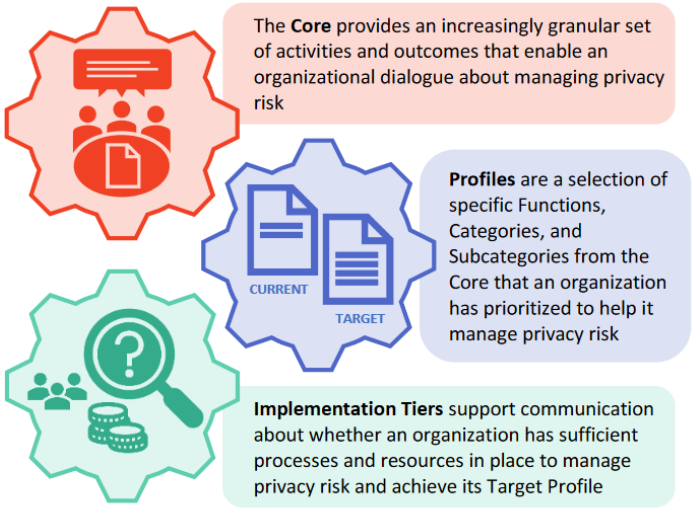


Figure 1: Core, Profiles, and Implementation Tiers

VO: Throughout this section, we have discussed the NIST Privacy Framework and how that framework is designed to be flexible enough to adapt to the continually changing needs of your organization. We reviewed the three basic areas: The Core, the Profiles, and the Implementation Tiers.

Throughout the rest of this presentation, we will build on this model to discuss how the control of personal information has influenced and will continue to influence risk management decisions in the future.

The Role of Threats and CUI [Scene 3]

Slide 3.1

Lesson Open

Image:

VO: Welcome to Lesson 2. (Add Lindsay's standard lesson audio)

Slide 3.2

Steps to Finding Threats

- Five Core Steps
- Work threats
- Home threats
- Security Controls

Image: Images based on vulnerability threats in work or home.

VO: Security threats are starting to become a major problem for the workplace, and at home. Let's focus on work threats and how they affect a company along with its employee's security. The protection of personal information or data in the workplace is critical with the threat of security breaches that involve databases and shared network drives. Here are five core steps within the Risk Identification and Management process that used to find risk, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment, and Risk monitoring.

An organization should minimize the use, collection, and retention of personal information (PII). At-home threats have been on the rise since the Covid crisis of 2020, more people are finding themselves working from home, which is causing more disruptions to security threats.

Security controls provide a safeguard for the confidentiality of PII information and are often applied within a system to protect other types of information, data processed, stored, or transmitted from the system. Here are some examples from NIST SP 800-53 that could help protect from security threats.

1. *Access Enforcement (AC-3)*
2. *Separation of Duties (AC-5)*

3. *Least Privilege (AC-6)*
4. *Remote Access (AC-17)*
5. *User-Based Collaboration and Information Sharing (AC-12)*
6. *Access Control for Mobile Devices (AC-19)*

Slide 3.3

Bluetooth Vulnerability and Threats

- Open standard for short-range radio frequency (RF) communication.
- Bluetooth versions: 4.0, 4.1, and 4.2.
- Susceptible to general wireless networking threats:
    - DoS (Denial of Service) attacks
    - Eavesdropping
    - Man-in-the-middle (MITM) attacks
    - Message modification
    - Resource misappropriation

Image:

VO: Bluetooth is an open standard used for short-range radio frequency (RF) communication. It currently has 3 versions Bluetooth version 4.0 (adopted June 2010 and most prevalent), 4.1 (adopted December 2013), and 4.2 (adopted December 2014).

- *Bluetooth 4.1 improved the strength of Basic Rate/Enhanced Data Rate (BR/EDR) technology, cryptographic key, device authentication, and encryption by using the Federal Information Processing Standard (FIPS).*
- *Bluetooth 4.2 improved the strength of the low energy technology cryptographic key by making use of FIPS-approved algorithms, and by converting BR/EDR technology keys to low energy technology keys.*

Bluetooth wireless technology is susceptible to general wireless networking threats, which include the following:

1. *DoS (Denial of Service) attacks*
2. *Eavesdropping*
3. *Man-in-the-middle (MITM) attacks*
4. *Message modification*
5. *Resource misappropriation*

Bluetooth attacks are usually done by gaining access to improperly secured Bluetooth devices or implementations from unauthorized use of Bluetooth devices on systems or networks.

Slide 3.4

Inconsistent or Unconventional Passwords

- 3 Common factors that we use for authentication
- Multi-factor or dual-factor

Image: 

VO: The use of inconsistent or unconventional passwords is a big problem with users, since creating a complex and memorable password is very tricky for most people to do. Multi-factor or dual-factor authentication is helping control this security issue. Here are the 3 common factors we use for authentication:

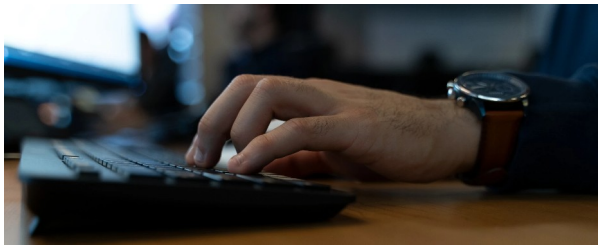
1. *Something we know (like a password)*
2. *Something we have (a smart card)*
3. *Something we are (a fingerprint or other biometric methods)*

To help solve the problem with password security problems, the start of multi-factor or dual-factor authentication, along with biometric authentication is being explored with new solutions. We will cover more about biometric authentication in the next lesson.

Slide 3.5

CUI (Controlled Unclassified Information)

- Protection of unclassified federal information in nonfederal systems and organizations impacts the ability of the federal government to be successful in conducting its essential functions and mission.
- Designed to deal with several issues in managing and protecting unclassified information, which includes inconsistent markings, inadequate safeguarding, and needless restrictions by standardizing procedures and providing common definitions through the CUI Registry.
- CUI Registry is an online repository for information, guidance, policy, and requirements that pertain to CUI and including issuances by the CUI Executive Agent.
- Identifies the following:
    - Approved CUI categories
    - Provides general descriptions for each
    - Identifies the basis for controls
    - Sets out procedures for the use of CUI, including but not limited to:
        - Marking
        - Safeguarding
        - Transporting
        - Disseminating
        - Reusing
        - Disposing of the information

Image: 

VO: CUI or Controlled Unclassified Information is the protection of unclassified federal information in a nonfederal system and organizations, which impacts the ability of the federal government to be successful in conducting its essential functions and mission.

CUI is designed to deal with several issues within managing and protecting unclassified information, which includes inconsistent procedures and providing common definitions through the CUI Registry.

The CUI Registry is an online repository for information, guidance, policy, and requirements that pertain to CUI which include issuances by the CUI Executive Agent. The registry sets

procedures that include but are not limited to, Marking, Safeguarding, Transporting, Disseminating, Reusing, and disposing of the information.

Slide 3.6

Summary

Security threats are not going away, they are only going to get worse in the future. Understanding the role these threats play within an organization or at home is vital to successfully get control of security breaches from users.

VO: This concludes lesson 2. (Add Lindsay's standard summary audio)

The Future of Risk Analysis and Privacy Protections
[Scene 4]

Slide 4.1

Lesson Open

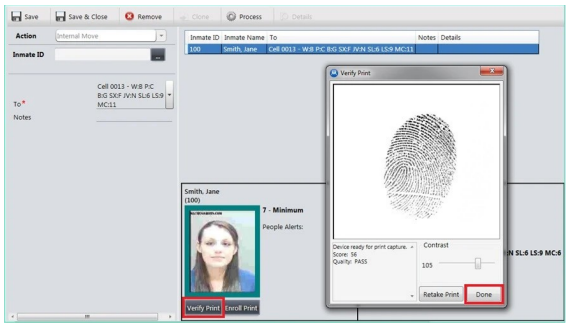
Image:

VO: Welcome to Lesson 3. (Add Lindsay's standard lesson audio)

Slide 4.2

Biometrics

- Biometrics is a way to measure a person's physical characteristics to verify their identity.
    - Physiological traits:
        - Fingerprints
        - Eyes
        - Behavioral characteristics (ex. security-authentication puzzle)
    - Biometric data must be unique, permanent, and collectible.
- Hopkinsville Police Department is no longer providing fingerprint services for background checks due to state regulations.
- ID document scanning technologies:
    - Smart Engines- Smart-ID engine, AI-driven detection
    - Can detect holographic security elements on ID cards and provides increased privacy protection with high accuracy fraud detection.

Image: 

VO: Biometrics is becoming more prevalent in today's world than ever before, especially with fingerprint, eye scanning devices, and behavioral characteristics such as a security-authentication puzzle. Biometric data is a way to measure a person's physical characteristics and a way to verify their identity. This biometric data must be unique, permanent, and collectible.

Using biometric for security for users' passwords, which could help solve the problem of users choosing weak and easily guessed passwords such as using "123456 or "password". It's worth noting that Hopkinsville Police Department in Kentucky is no longer going to provide fingerprint services for background checks due to state regulations.

A biometric company called Smart Engines has developed a new OCR identity scanning software that can detect holographic security elements on ID cards, which will provide privacy protection and higher accuracy of fraud detection, and liveness detection to identify documents. The AI-based algorithms Smart Engines is developing will be able to detect the liveness for 1,300 different ID cards, and passports.

Slide 4.3

Biometric Data could be Breached?

- Biometric data can be breached:
    a. Fingerprint or Face scan can be stored within a database and be replaced by a hacker.
    b. Spoof your fingerprint or face which could be created from the stored template data.
    c. Steal the template data which could be used to gain access to the unauthorized systems.
    d. Template data that's been stolen can be used by a hacker to track an individual without their knowledge, from one system to another.

Image:

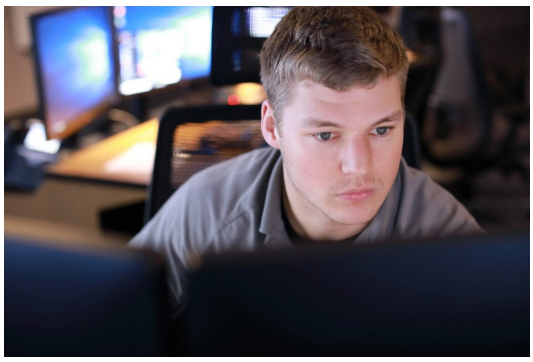
VO: Biometric data is a part of something known as biometric template data, which is usually linked to your fingerprints or face. Here are 4 examples of ways biometric data could be breached.

1. *Fingerprint or Face scan can be stored within a database and be replace by a hacker and used to gain unauthorized access to a system.*
2. *A spoof of a person's fingerprint or face data could be created from the stored template data.*
3. *A hacker can steal the template data which could be reused to gain unauthorized access to a system.*
4. *Template data that's been stolen can be used by a hacker to track an individual without their consent or knowledge, which can be used to track the user from one system to another.*

Slide 4.4

Biometric Data Needs Protection

- Cancellable Biometrics
    a. Complex mathematical functions are used to transform the original template data when your fingerprint or face is being scanned.
    b. Non-reversible, no risk of the transformed template data being turned back into the original fingerprint or face scan.
    c. In case of a breach, the stored records can be deleted.
    d. When you scan your fingerprint or face again, the scan will change with a unique template even when using the same finger or face.
- Biometric Cryptosystems
    a. Orginal template data is combined with a cryptographic key, which generates a “black box”.
    b. The cryptographic key is the “secret” and query data is the key to unlock the black box.
    c. The cryptographic key is then released upon after successful authentication.

Image: 

VO: The use of biometric systems is being used even more than ever before, you can find them being used in civil, commercial, and national defense applications such as electronic devices in smartphones, credit cards with embedded fingerprint scanners, and wearable fitness devices that use biometrics to unlock smart cars and homes. Protecting raw template data fall into two categories which are Cancellable Biometrics and Biometric Cryptosystems.

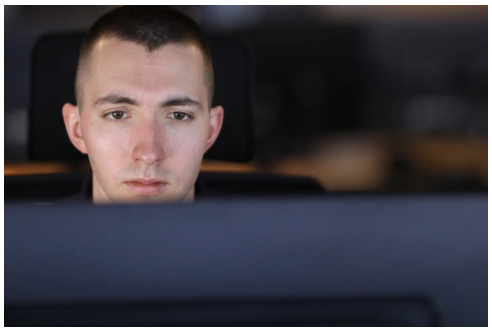
Cancellable biometrics is a mathematical function that can be used to transform the original template data when your fingerprint or face is being scanned. Once the transform has taken place it's non-reversible and no risk of the transformed template data being turned back into the original fingerprint or face scan. If a breach has taken place, the stored records can be deleted. Lastly, when you scan your fingerprint or face again, the scan will change with a unique template even when using the same finger or face.

Biometric Cryptosystems is when the original template data is combined with a cryptographic key, which will generate a black box. This cryptographic key is the secret and query data is the key to unlocking the black box. Once successful, the cryptographic key is then released upon successful authentication.

Slide 4.5

Facial Recognition

- Massachusetts Police reform bill (S.2963)
    - The first state to pass statewide limitations on law enforcement's use of facial recognition technology.
    - Registries of Motor Vehicles would still be allowed to continue to use the software to verify a person's identity when issuing a license or other documents.
- Police can obtain permits to use the RMV technology for violent crime investigations.

Image: 

VO: A Police reform bill called S.2963 was introduced in Massachusetts in late 2020 to set a limitation on law enforcement's use of facial recognition technology. The reason for the reform bill is that advocates are arguing is plagued by false matches, racial bias, and potential privacy violations.

If passed, Massachusetts will be the first state to pass a statewide limitation on law enforcement's use of facial recognition technology. The reform does have a few exceptions to the ban, the Registry of Motor Vehicles would still be allowed to continue with using software to verify a person's identity when issuing a license or other documents, and police can still obtain permits to use the RMV technology for violent crime investigations.

Slide 4.6

The Role of AI

- Nothing has changed, just built on layers to break through fixes.
- Attack methods tend to cycle as time goes on.
- Existing encryption algorithms or techniques for non-AI-based biometric systems are incompatible with AI-based biometric systems.

Image: AI-based image, related video

VO: How does the role of AI (artificial intelligence) play with new biometric systems which can start to be found in consumer electronics such as a smart camera with built-in AI that can track faces or recognize them.

AI is not 100 percent safe, potential threats can still happen with the integration of biometric systems into AI, such as deep artificial neural networks that enhance the performance of these biometric systems.

For example, a team of researchers at New York University developed a tool named DeepMasterPrints. The tool is used for a deep learning technique that will generate fake fingerprints which can be used to unlock a large number of mobile devices, which is very similar to a master key for a door.

Slide 4.7

Best Practices

- Collection
- Maintaining
- Logistics (any passing of information)

Image: 

VO: Here are some best practices you should follow to keep your privacy safe and secure. The first best practice is how you collect and store your private data, which can help with security breaches in the future. Next, is maintaining such audits, passwords, and account management. Lastly, is logistics which is how you pass information to people, data privacy within an organization.

Slide 4.8

Summary

The future of Risk Analysis and Privacy Data is starting to see a big shift with advanced AI technology such as fingerprint scanners, facial recognition which fall into the Biometric data category. Organizations need to take the threat of biometric data being the target for future security breaches and prepare to solve the issue with AI being used to create these problems for organizations in the future.

VO: This concludes lesson 3. (Add Lindsay's standard summary audio)

Assessment [Scene 5]

Slide 5.1

Final Assessment

The final assessment includes questions to test your knowledge of the material presented in the course. You must pass the assessment with a score of 80% or higher to receive credit for this course.

You must answer each question to continue. At the end of the assessment, your score will be provided. If you do not pass, you are given the option to retake the assessment.

For each question, select your answer and press the Checkmark (✓) button on the bottom right.

When you are ready to begin, press the Next arrow.

VO: Welcome to the final assessment. Please familiarize yourself with the instructions and pass requirements.

Slide 5.2

Question 1 out of 5

What are the three basic areas of the Privacy Framework?

The Core, Profiles, and Privacy
The Core, Profiles, and Private
*The Core, Profiles, and Implementation Tiers
Implementation, Profiles, and Privacy

Slide 5.3

Question 2 out of 5

True or False: Bluetooth wireless technology is not susceptible to general wireless networking threats?

True
*False

Slide 5.4

Question 3 out of 5

True or False: CUI is designed to manage several issues such as protecting unclassified information or inadequate safeguards?

*True
False

Slide 5.5

Question 4 out of 5

CUI Registry is an online repository for information, guidance, and policy, but what issuance is it held by?

CUI Agent
Safeguarding Agent
CUI Marking Agent
*CUI Executive Agent

Slide 5.6

Question 5 out of 5

What are the three best practices you should follow to Identify new threats and protecting private data?

Collection, Maintaining, Future-proofing
Security, Privacy, Collection
*Collection, Maintaining, and Logistics
Logistics, Privacy, Collection