

Instructional Scenario

Protecting the Digital Shadow



Course/Duty Area: Cybersecurity Fundamentals/Exploring Data Privacy and Security

Scenario:

SecureByte is a U.S.-based cybersecurity firm that provides cloud storage and data analytics services to small businesses. As they grow, they collect massive amounts of data from their clients, ranging from basic contact lists to sensitive financial records. Recently, a marketing partner offered SecureByte a significant amount of money to buy “anonymized” user data to help train a new AI-driven advertising tool. Simultaneously, SecureByte discovered that one of their portable storage drives containing employee records was misplaced during a recent office move.

The SecureByte leadership team has an issue: they want to maximize the value of the data they hold (knowledge) and ensure business growth, but they are concerned about the digital footprints they are creating for their clients and the legal/social consequences of a potential data compromise. They must now evaluate their data lifecycle—from the binary level to cloud storage—to protect their “digital shadow.”

Big Question:

How can SecureByte distinguish between data, information, and knowledge to leverage big data effectively while maintaining the legal and ethical integrity of personally identifiable information (PII)?

Focused Questions:

- How does raw, uninterpreted data (represented in binary or hex) transform into structured information and eventually actionable knowledge?
- What are the specific vulnerabilities and protection methods (like encryption, biometrics, and patching) for data when it is at rest, in transit, and being processed?
- How do active vs. passive collection techniques, such as cookies and device fingerprinting, contribute to a person’s digital footprint and impact their future career opportunities?
- What are the risks and benefits of using local storage (SSD), network storage (NAS), or cloud storage for sensitive PII?
- How do businesses identify and defend against data loss through SQL-injection, ransomware, and metadata leaks?

Student Project or Outcome:

Students will perform a data integrity and privacy audit and produce a comprehensive report and infographic for SecureByte’s leadership that analyzes their current data practices and recommends a “Secure by Design” protection strategy.

Project-Based Assessment:

- Create a diagram that identifies a specific data element (like a phone number) and shows its representation at the lowest level (Binary and Hexadecimal).
- Define PII and explain how data mining and AI can turn a simple digital footprint into a social or legal risk for an individual (e.g., impact on college/employment).
- Propose three specific security mechanisms to protect data in different states: one for data at rest (e.g.,

asymmetric encryption), one for data in transit (e.g., cryptography), and one for data being processed (e.g., host device hardening).

- Analyze a sample privacy policy to determine if it uses informed consent and identifies the use of data brokers or biometrics.

Teacher Resources:

- [Guide to Protecting the Confidentiality of Personally Identifiable Information \(PII\)](#), National Institute of Standards and Technology (NIST), U.S. Department of Commerce
- [SQL Injection](#), Cybersecurity and Infrastructure Security Agency (CISA)
- [#StopRansomware Guide](#), Cybersecurity and Infrastructure Security Agency (CISA)
- [Take a Step Towards Privacy: Understanding Digital Footprints](#), Internet Society
- Binary/Hexadecimal Worksheets: Practical exercises for low-level data representation

Scenario submitted by Chris Starke, Briar Woods High School, Loudoun County Public Schools