HEALTH
UNIVERSITY OF UTAH

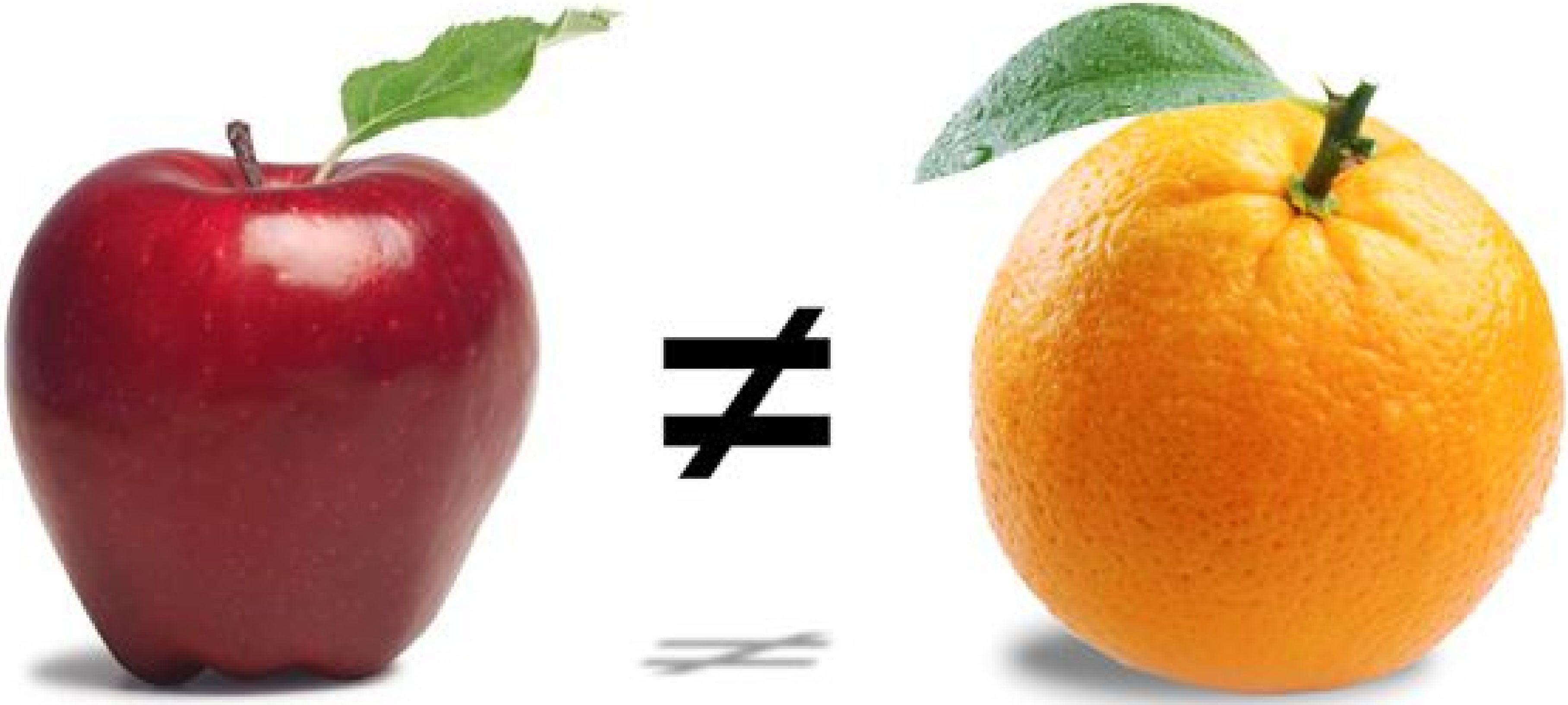
JERRY SMITH
SENIOR INFORMATION SECURITY AND PRIVACY ANALYST

CONFIDENTIAL

INTRODUCTION

- How are controls implemented to meet regulatory requirements for both privacy and security?
- There is a misconception that privacy and security are one in the same and the same controls can be used to meet regulatory requirements for both areas.
- Privacy and security are very different in their control perspectives and need to be treated differently.

PRIVACY IS NOT THE SAME AS SECURITY

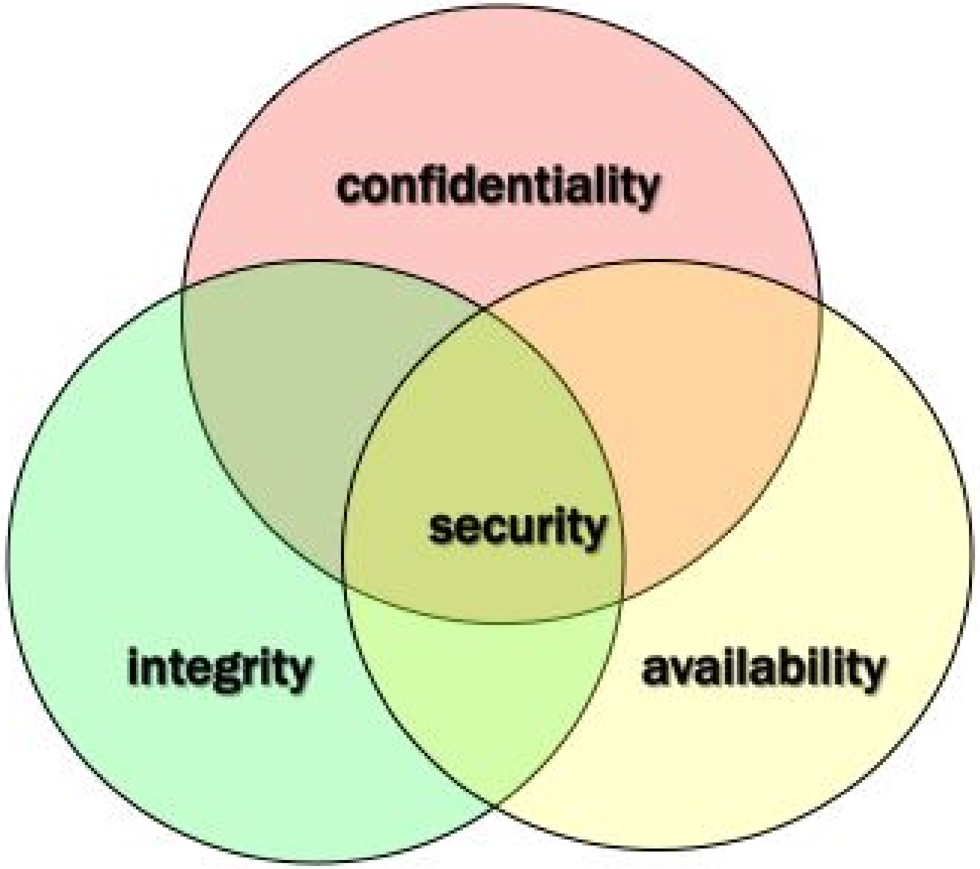


PRIVACY

- According to Health and Human Services (HHS), Privacy is defined as the appropriate use of data.
- Companies and vendors have data entrusted to them and that data should be used according to agreed purposes.
- There have been cases where companies have lost, sold, disclosed, rented, or had stolen data or information that was entrusted to them or other parties associated or affiliated with them.

INFORMATION SECURITY

- Ensures data isn’t used or accessed by unauthorized individuals or parties
- Ensures data is accurate and reliable when needed
- An Information Security plan includes facets to collect only required information, keeping data safe, and destroying information that is no longer needed



HEARTS AND MINDS

- Information Security establishes secure access
- Now at the door, entry is provided, and this is where the Privacy role comes into play
- Privacy monitors and audits; watches to ensure that nobody breaks “the fine china” in the room or alters, views, or makes any changes within the room (application) unless they have been given the authority

PRIVACY BUILD OUT

- Privacy **and** Information Security = Business Success
- “Rules of the Road”:
  - Limit access to align with business need (role based access)
  - Open a dialog with Information Security Team
  - Attend Information Security seminars
  - Learn about the *Fair Information Privacy Practices* found at www.healthit.gov
  - Start an opt-in as versus an opt-out

GOALS

- Transparency
- Individual Participation
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality and Integrity
- Security
- Accountability and Auditing

RISK ANALYSIS

Four factor breach analysis:

- ✓ **Factor 1:** Nature/extent of PHI/PII involved, types of identifiers, and re-identification risk?
- ✓ **Factor 2:** Unauthorized user or unauthorized recipient?
- ✓ **Factor 3:** Was PHI/PII actually accessed or used?
- ✓ **Factor 4:** Extent risk to PHI/PII has been mitigated.
  - Source: Health and Human Services (HHS), and Office of Civil Rights (OCR) of the United States

BREACH OUTCOME

Exploitation of an individual’s health or financial information could result in:

- Possible class action litigation
- Fines and/or penalties
- Embarrassment or other harm to the individual
- Damage to the reputation of the organization
- Loss of trust between the organization and the customers

OUR EMPLOYEES

- Value employee assets – front line of our efforts
- Use this resource effectively
- Train and educate continually and update for the constant threats
- Help employees understand the worth of data – about people and their lives
- Employees need to take a sense of ownership to protect the data and treat it with respect

PRODUCTS

- FairWarning
- Iatric
- Maize
- Securonix
- Protenus

ASSET

Implement Education and Training to instill the idea of ownership

- Employees understand protecting data is the right thing to do
- Employees understand why they should care about protecting customer privacy

The connection helps with two things:

1. Helps protect data
2. Helps identify when something might have occurred and we have a problem

HEARTS AND MINDS AGAIN

- We need the hearts and minds of our employees
- Technology controls have a high cost
- It only takes once for a breach
- Training and education for employees on the important aspects of Privacy and Information Security will help them make better decisions on the appropriate use of data and how to protect customers and organizational assets

KEY EMPLOYEE TRAINING CONSIDERATIONS

- Are you obtaining data in a safe manner so it cannot be overheard or seen by others?
- Did you secure documents and files that contain PII?
- Are you storing PII on only authorized portable electronic devices (i.e., work equipment, etc.)
- Did you follow proper privacy and security procedures to secure the stored PII (e.g., encryption)?
- Will you use the PII for the purpose it was provided?
- Are you only using the minimum necessary PII to get the job done?
- Are you accessing PII through secure and authorized equipment or connections?
- Did you verify the sharing is allowed?

KEY EMPLOYEE TRAINING CONSIDERATIONS (cont.)

- Have you verified everyone that the PII is being shared with has a need to know?
- Did you share only the minimum amount of PII and follow disclosure procedures?
- Did you share using the appropriate safeguards (e.g., encryption)?
- Is the PII part of a record that falls under the records retention schedule?
- Did you shred all papers containing PII?
- Did you return equipment (e.g., computer, copiers, and fax machines) to the IT Department for proper disposal

ASPECTS OF TRAINING AND EDUCATION

- Training and Education helps employees understand the implications of Privacy and how to roll it into their daily procedures and practices
- Training empowers them with the knowledge to meet Privacy and Information Security challenges
- Train employees with one voice and allow Privacy to become part of the dialog
- Campaign together for resources and instill in the culture the need for thinking in terms of both Privacy and Information Security

POLICY

- Enforceable
- Communicated through the organization
- EVERYONE needs to understand what it means and the consequences of not adhering to the policy
- If possible, integrate the Privacy and Information Security Policy
- Align in common language/purpose to assist in providing a unified protective structure for the organization

THINGS TO AVOID IN POLICY

- Wrong Location
- Wrong Data
- Wrong Link
- Wrong Technology
- Wrong Promise
- Wrong Promise (Part Two)
- Wrong Guarantee
- Wrong Version
- Wrong Training
- Wrong Practice

TAKEAWAY

- Add Privacy to your vocabulary – try to use it in conjunction with Information Security
- Privacy is a key component of how you control and protect sensitive data
- Privacy is a “Hearts and Minds” process
- Train your employees to utilize the key concepts of Fair Information Privacy Practices
- Recognize Privacy provides protection to your organizational assets and use your employee as a piece of that protective envelope to wrap protection and controls around your sensitive data

TAKEAWAY (cont.)

- Integrate with Information Security and unify your efforts which provide a consolidated approach to protecting your organization.
- Make sure that if there is a discussion of Cloud Service Providers (CSP) that Privacy is part of that discussion.
- Ensure IT and IT Security understand that Service Level Agreement (SLA) is the document that should drive the relationship between the CSP, the organization, and the Business Associate Agreement (BAA) and should dovetail into the SLA.
- Ensure if you establish a relationship with a CSP, that ownership of the data is established with CSP once data is moved to cloud space and the organization or CE retains ownership at all times.
- Encryption, Encryption, Encryption

QUESTIONS