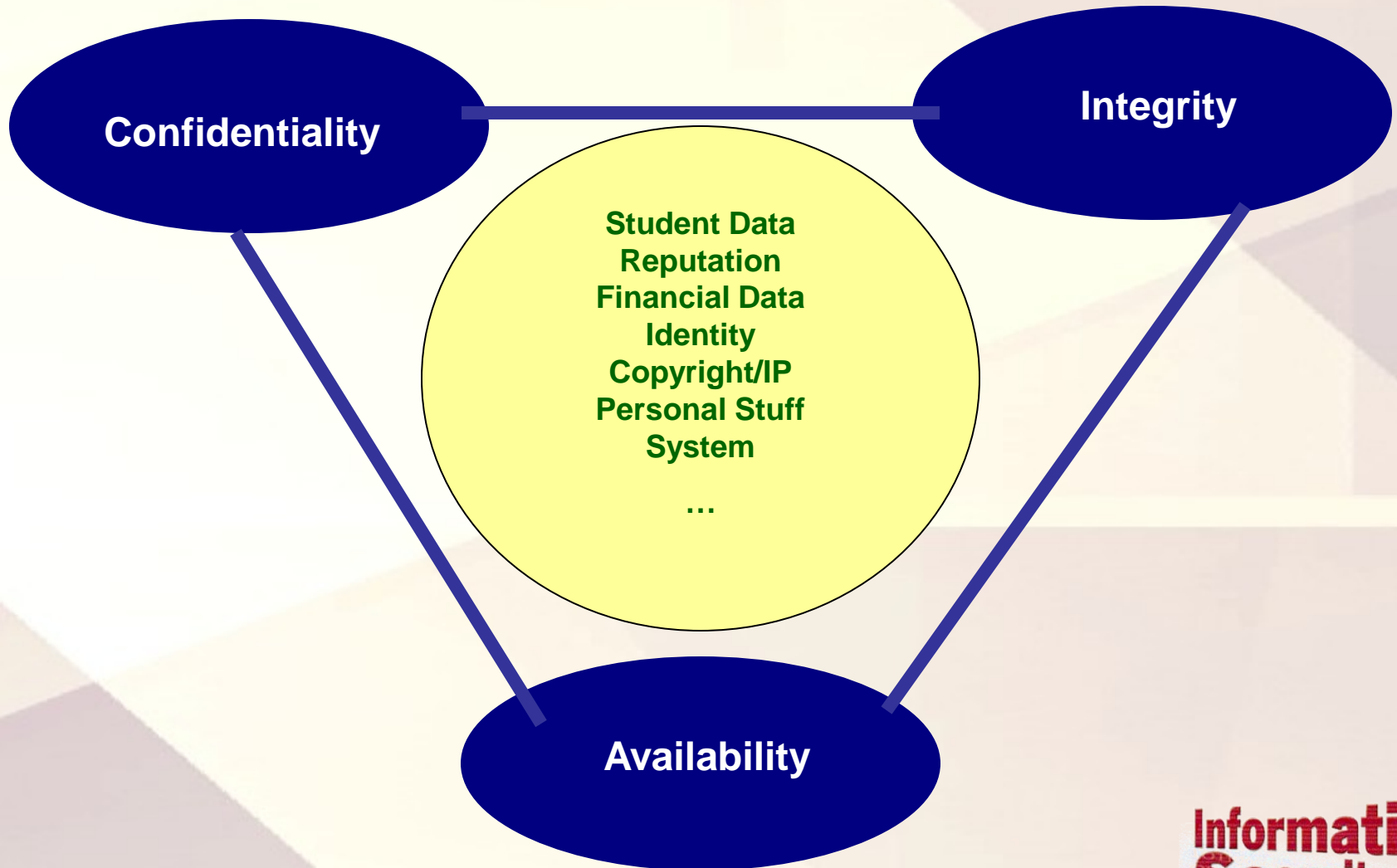# Basic Digital Records Security Measures

Dan O'Callaghan

Sinclair Community College

July 14, 2010

Information Security

Unique Digital Record Concerns

- Difficult to ensure that the content, context and structure of records is preserved and protected when the records do not have a physical existence.

- Digital records cannot be managed without a computer.

- Preservation
    - Ability to access and read digital records over time.
    - Digital records require appropriate combinations of software versions and operating systems to be accessed, and so are at risk because of the rate at which technological changes occur.

- Metadata

- Theft/Unauthorized access detection

Personal Information

ORC 1347/1349 defines "personal information" as:

- A person's first name (or initial) and surname, in combination with any of the following:

  - Social Security Number.

  - Driver's license number or state identification card number.

  - Financial account, debit, or credit number.

  - Other information that creates a '*material risk of the commission of the offense of identity fraud or other fraud to the individual*.'

Email & IM

Email and Instant Messaging **ARE NOT** secure methods of transmission.

- **NEVER** transmit a record containing "Personal Information" via Email or IM **UNLESS** an appropriate technical security measure is used.
  - Encryption (AxCrypt, TruCrypt, WinZip)
  - Digital Redaction (be very careful of metadata)
  - Secure email solution (not currently available at SCC)
- Consider similar for sensitive records with no personal information

Internet Accessibility

The Internet is essentially a single enormous network containing multiple smaller networks.

- Anything published or downloadable from the 'web' is potentially available world-wide

- **NEVER** publish/upload a record containing "Personal Information" to a Web resource **UNLESS** an appropriate technical security measure is used.
  - Encryption (AxCrypt, TruCrypt, WinZip)
  - Digital Redaction (be very careful of metadata)

- Consider similar for sensitive records with no personal information

Digital Storage

Consider CIA when storing digital records.

- **NEVER** store a record containing "Personal Information" on portable/mobile devices or media **UNLESS** an appropriate technical security measure is used.
  - Consider similar for sensitive records with no personal information

- Securely delete/destroy portable or 'back-up' media when sensitive record is no longer required.

- Strongly recommend network storage area (dept. share, H-Drive) instead of local (My Documents) storage.

More Information?
Any Questions?

Dan O'Callaghan
Sinclair Community College
444 W Third St, 13-000F
Dayton, OH 45402

Voice: 512-2452

Email (NOT SECURE!): daniel.ocallaghan@sinclair.edu