



Developing A Comprehensive Approach To Handling Confidential/Sensitive Data

Darlene Quackenbush
IT Planning & Information Security Officer
James Madison University

Shirley Payne
IT Security & Policy Director
University of Virginia

Virginia Alliance for Secure Computing & Networking Conference
October 18, 2007



Agenda

- The Gathering Storm
 - Problem defined
 - Challenges ahead
- A Ray of Sunshine
 - EDUCAUSE Confidential Data Handling Blueprint
 - JMU and UVA Strategies
- Discussion





Rain Drops Keep Falling On My Head...

- *February 15, 2007. Hackers Use New Zero-Day Word Exploit In Targeted Attack. The attack targeted people with specific roles in a company. It was aimed at stealing both personal and corporate information.*



Rain Drops Keep Falling On My Head...

- *June 8, 2007. U.Va. Alerts Current and Former Faculty That Sensitive Information Has Been Exposed.* Investigators believe the hackers accessed information on 5,735 current and former faculty members. The information had been mistakenly included in the database of a special-purpose web application.



Rain Drops Keep Falling On My Head...

- *June 16, 2007.* **Professor Loses Student Data.** A flash drive holding information on about 8,000 current and former Texas A&M University students was lost by a mathematics professor while on vacation in Madagascar.



Rain Drops Keep Falling On My Head...

- *June 18, 2007. IT Managers Say Risk Of Data Loss Is Bad And Getting Worse.*
Nearly half of more than 1,000 IT and compliance professionals surveyed say their organizations are doing an inadequate job of lowering the rate of data loss. They lack the necessary security tools or internal controls to prevent, detect, and correct data security breaches.



Rain Drops Keep Falling On My Head...

- *September 11, 2007. More Personal Data Said To Be On Stolen Ohio Government Backup Tape. The missing tape, on which more than 1.3 million pieces of personal data were stored, was being used to carry information between two government sites. The incident is expected to cost the state almost \$3 million.*



Just How Stormy Is It?

- 1.9 billion electronic records reported exposed from 1980 to 2006
- Rate is increasing. Current rate is 672 records every 5 minutes!
- Higher Education accounts for one-third of all incidents, although <1% of total lost records.

Source: Erickson, K., & Howard, P. (2007). A case of mistaken identity? News accounts of hacker, consumer, and organizational responsibility for compromised digital records. *Journal of Computer-Mediated Communication*, 12(4), article 5.

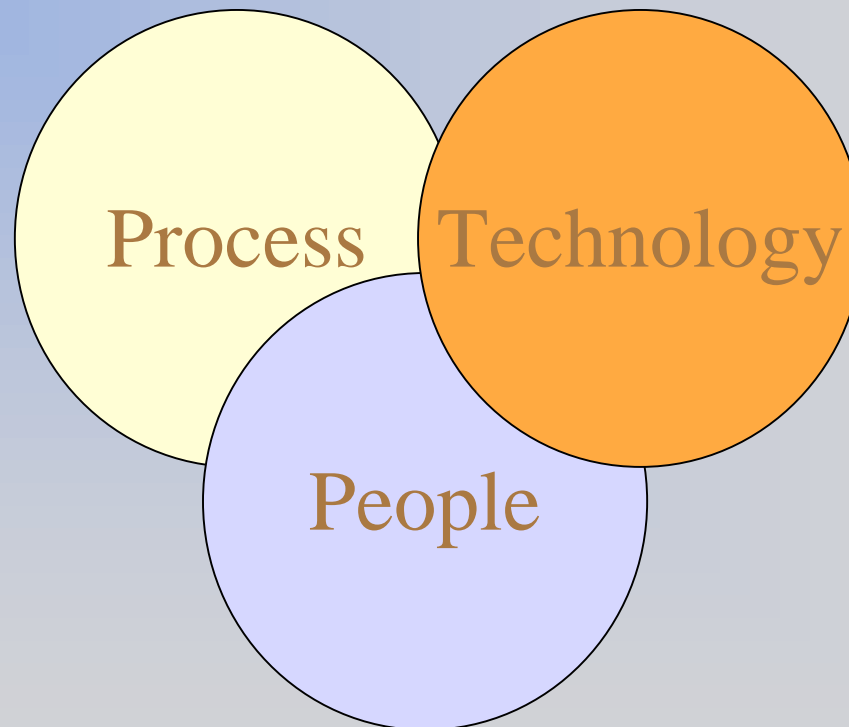
<http://jcmc.indiana.edu/vol12/issue4/erikson.html>



Consequences

- Strategic, e.g. loss of intellectual property
- Financial, e.g. regulation penalties, cost of notifications
- Legal, e.g. lawsuits
- Operational, e.g. critical system downtime
- Reputational, e.g. loss of trust

Security Relies On...

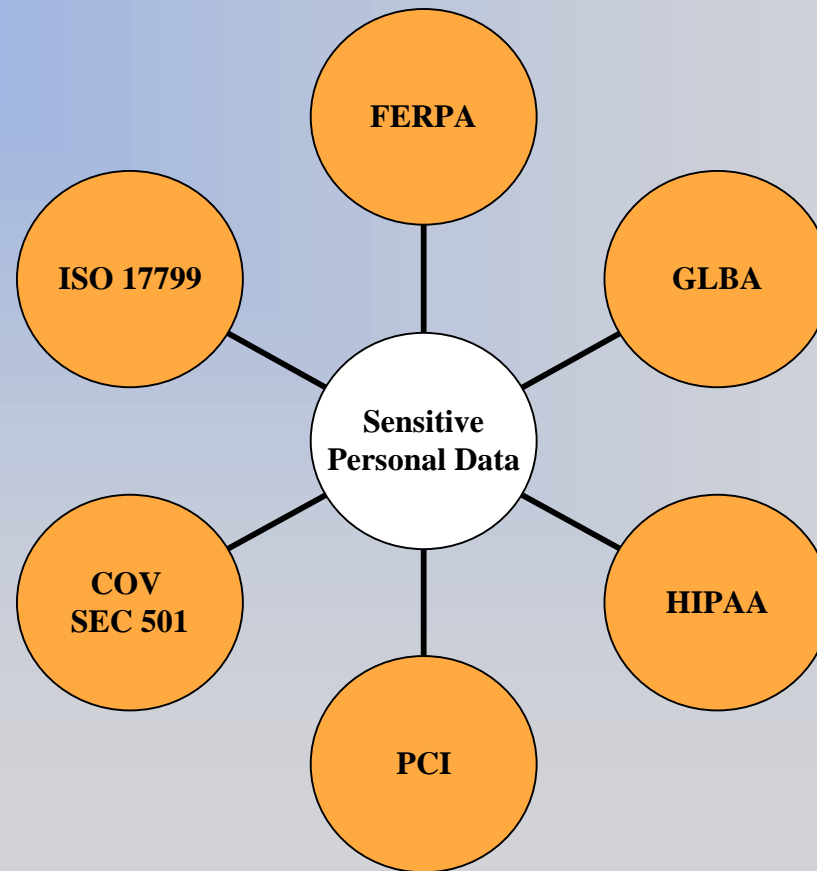




Why Is Security So Hard?

- Cultural issues
- Lack of awareness
- No technical silver bullet
- Determined opponents & commercial value of data
- Absence and enforcement of policies

*And if that weren't
enough...COMPLIANCE*





A Ray of Sunshine – A comprehensive approach

EDUCAUSE Confidential Data Handling Blueprint

Purpose

- To provide a list of key strategies to follow for stopping the leakage of confidential/sensitive data.
- To provide a toolkit that constructs resources pertaining to confidential/sensitive data handling.



A Comprehensive Approach

- Step 1: Create a security risk-aware culture that includes an information security risk management program
- Step 2: Define institutional data types
- Step 3: Clarify responsibilities and accountability for safeguarding confidential/sensitive data
- Step 4: Reduce access to confidential/sensitive data not absolutely essential to institutional processes
- Step 5: Establish and implement stricter controls for safeguarding confidential/sensitive data
- Step 6: Provide awareness and training
- Step 7: Verify compliance routinely with your policies and procedures

<https://wiki.internet2.edu/confluence/display/secguide/Confidential+Data+Handling+Blueprint>



Illustrating Its Use

- JMU sensitive data workgroup
- UVA sensitive data handling initiative



EDUCAUSE Blueprint Step 1

1. Create security risk-aware culture that includes an information security risk management program
 - 1.1 Institution-wide security risk management program
 - 1.2 Roles and responsibilities defined for overall information security at the central and distributed level
 - 1.3 Executive leadership support in the form of policies and governance actions



EDUCAUSE Blueprint Step 2

2. Define institutional data types

- 2.1 Compliance with applicable federal and state laws and regulations - as well as contractual obligations - related to privacy and security of data held by the institution (also consider applicable international laws)
- 2.2 Data classification schema developed with input from legal counsel and data stewards
- 2.3 Data classification schema assigned to institutional data to the extent possible or necessary



EDUCAUSE Blueprint Step 3

3. Clarify responsibilities and accountability for safeguarding data
 - 3.1 Data stewardship roles and responsibilities
 - 3.2 Legally binding third party agreements that assign responsibility for secure data handling



EDUCAUSE Blueprint Step 4

4. Reduce access to data not absolutely essential to institutional processes
 - 4.1 Data collection processes (including forms) should request only the minimum necessary confidential/sensitive information
 - 4.2 Application outputs (e.g., queries, hard copy reports, etc.) should provide only the minimum necessary confidential/sensitive information
 - 4.3 Inventory and review access to existing confidential/sensitive data on servers, desktops, and mobile devices



EDUCAUSE Blueprint Step 4 - continued

4. Reduce access to data not absolutely essential to institutional processes
 - 4.4 Eliminate unnecessary confidential/sensitive data on servers, desktops, and mobile devices
 - 4.5 Eliminate dependence on SSNs as primary identifiers and as a form of authentication*

*Note: SSNs may need to be used for certain things (e.g., student employees, student financial aid, etc.) and we recommend that schools limit the use of SSNs to necessary processes only.



EDUCAUSE Blueprint Step 5

5. Establish and implement stricter controls for safeguarding data
 - 5.1 Inventory and review/remediate security of devices
 - 5.2 Configuration standards for applications, servers, desktops, and mobile devices
 - 5.3 Network level protections
 - 5.4 Encryption strategies for data in transit and at rest



EDUCAUSE Blueprint Step 5 - continued

5. Establish and implement stricter controls for safeguarding data

5.5 Policies regarding confidential/sensitive data on mobile devices and home computers and for data archival/storage

5.6 Identity management and resource provisioning processes

5.7 Secure disposal of equipment and data

5.8 Consider background checks on individuals handling confidential/sensitive data



EDUCAUSE Blueprint Step 6

6. Provide awareness and training

- 6.1 Make confidential/sensitive data handlers aware of privacy and security requirements
- 6.2 Require acknowledgement by data users of their responsibility for safeguarding such data
- 6.3 Enhance general privacy and security awareness programs to specifically address safeguarding confidential/sensitive data
- 6.4 Collaboration mechanisms such as e-mail have strengths and limitations in terms of access control, which must be clearly communicated and understood so that the data will be safeguarded



EDUCAUSE Blueprint Step 6 -- Resource

EDUCAUSE Security Awareness & Training Resources

<https://wiki.internet2.edu/confluence/display/secguide/Awareness+and+Training>



EDUCAUSE Blueprint Step 7

7. Verify compliance routinely with your policies and procedures

7.1 Routinely test network-connected devices and services for weaknesses in operating systems, applications, and encryption

7.2 Routinely scan servers, desktops, mobile devices, and networks containing confidential/sensitive data to verify compliance

7.3 Routinely audit access privileges

7.4 Procurement procedures and contract language to ensure proper data handling is maintained



EDUCAUSE Blueprint Step 7 - continued

7. Verify compliance routinely with your policies and procedures
 - 7.5 System development methodologies that prevent new data handling problems from being introduced into the environment
 - 7.6 Utilize audit function within the institution to verify compliance
 - 7.7 Incident response policies and procedures
 - 7.8 Conduct regular meetings with stakeholders such as data stewards, legal counsel, compliance officers, public safety, public relations, and IT groups to review institutional risk and compliance and to revise existing policies and procedures as needed



Additional Resources

Virginia Alliance for Secure Computing & Networking

<http://vascan.org>

Information Security Governance Assessment Tool for Higher Education

<http://www.educause.edu/ir/library/pdf/SEC0421.pdf>

JMU's Sensitive Data Protection Resources

<http://www.jmu.edu/computing/sensitivedata>

U.Va.'s SSN Initiative

<http://www.virginia.edu/ssninitiative>




Recommendations

- Think broadly and get started
- Prioritize based on risk
- Find your allies
- Coordinate all needed work to ensure consistent solutions
- Communicate status widely



Discussion

- 
- What are your concerns about confidential/sensitive data handling?
 - What solutions are being applied at your institutions?
 - **QUESTIONS**



Feel free to contact us...

Darlene Quackenbush – quackedh@jmu.edu

Shirley Payne – payne@virginia.edu