Data Classification and Privacy: A foundation for compliance

Brian Markham, CISA
University of Maryland at College Park
Office of Information Technology

Goals for today:

- Give you a solid understanding of both Data Classification and Data Privacy with respect to compliance;
- Link data classification and privacy to ongoing compliance issues;
- Discuss various best practices, methodologies, and approaches that you can take with you;
- Do my best to answer any questions you may have on audit related issues regarding these topics.

So...who am I?

- IT Compliance Specialist @ the Office of Information Technology at UMCP
- Responsible for audit and compliance initiatives within OIT
- Formerly employed by KPMG LLP and Grant Thornton LLP as an IS Auditor
- Have worked with many federal, state, and local governments as well as public companies, hospitals, and not-for-profits.

Why do we want to be in compliance?

- No one likes audit findings;
- Reduces organizational risk;
- Processes based on best practice and widely adopted standards are more effective than ad-hoc processes;
- Systems and data are more secure as a result of good internal control practices.

What is Data Privacy?

- Data Privacy - the relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data.
- The U.S. has trailed the E.U. and other countries in data privacy regulations and legislation;
- Passed Legislation: HIPAA, Gramm-Leach-Bliley, COPPA;
- Proposed Legislation: Data Accountability and Trust Act, Personal Data Privacy and Security Act of 2007 (S. 495).

Why Data Privacy?

- To protect people's personal information under the law;
- We want to comply with the law;
- We want to be able to classify our data to adequate protect data that should be private.

What is Data Classification?

- Data classification is the act of placing data into categories that will dictate the level of internal controls to protect that data against theft, compromise, and inappropriate use.
- Information security is best managed when data is classified and the risks associated with each category is uniform and understood.
- Data classification is an essential part of audit and compliance activities at any organization; public or private sector.

Why Classify Data?

- Simply put: EVERY IT general control audit requires some sort of data classification standard or approach.
- FISCAM: "Classify information resources according to their criticality and sensitivity"
- State of MD: "Documenting and ensuring that a process is implemented for the classification of information in accordance with the Information Sensitivity and Classification Standard"
- USM Guidelines: "Identify critical systems – high value, high risk, critical service, critical data"

Standards and Best Practices

- NIST has developed FIPS-199 as a guideline for federal agencies
- The IT Governance Institute has included data classification in COBIT 4.0
  - "Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme includes details about data ownership, definition of appropriate security levels and protection controls, and a brief description of data retention and destruction requirements, criticality and sensitivity. It is used as the basis for applying controls such as access controls, archiving or encryption." - ITGI

Standards and Best Practices (cont.)

- The IT Governance Institute has also listed data classification as an important component for Sarbanes Oxley section 404 compliance.
  - "Managing systems security includes both physical and logical controls that prevent unauthorized access. These controls typically support authorization, authentication, nonrepudiation, data classification and security monitoring. Deficiencies in this area could significantly impact financial reporting." - ITGI

Standards and Best Practices (cont.)

- As a response to FISMA, NIST developed FIPS-199 in 2003.
- FIPS-199 is the Federal Government's answer to data classification.
- It is a framework that can be easily understood, adopted, and implemented.
- It is based upon two components: security objectives and potential impacts.

FIPS-199

- Three security objectives: Confidentiality, Integrity, Availability (CIA);
- Three levels of potential impact: Low, Moderate, High;
- Was developed as a response to the E-Government Act of 2002 (Title III, also known as FISMA);
- Applies to all Federal Agencies.

FIPS-199 (cont.)

According to FISMA:

CONFIDENTIALITY

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information..." [44 U.S.C., Sec. 3542]
A loss of confidentiality is the unauthorized disclosure of information.

INTEGRITY

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity..." [44 U.S.C., Sec. 3542]
A loss of integrity is the unauthorized modification or destruction of information.

AVAILABILITY

"Ensuring timely and reliable access to and use of information..." [44 U.S.C., SEC. 3542]
A loss of availability is the disruption of access to or use of information or an information system.

FIPS-199 (cont.)

In plain English:

Confidentiality - Data Privacy Laws and Regulations

Integrity - How critical is it that data not be altered

Availability - Result of a Business Impact Analysis (BIA)

FIPS-199 (cont.)

According to FIPS-199, low, moderate, and high refer to the potential impact on organizations should their be a breach in security (CIA). Specifically:

The potential impact is LOW if: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
The potential impact is MODERATE if: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
The potential impact is HIGH if: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

FIPS-199 (cont.)

- So why implement FIPS-199?
  - It has been widely adopted by the Federal Government;
  - It ties back to best practice guidance developed by NIST;
  - FISCAM is the manual that is used by OLA to audit us; FISCAM is also the manual used to audit the Federal Government;
  - Being in line with FIPS-199 can only help us in the Federal grant application process.

FIPS-199: The Nine Box

\	Low	Moderate	High
Confidentiality			
Integrity			
Availability			

SC (Information Type) = {(Confidentiality, impact), (Integrity, impact), (Availability, impact)}

FIPS-199: The Nine Box

\	Low	Moderate	High
Confidentiality			
Integrity		X	
Availability		X	

SC Public Information = {(Confidentiality, NA), (Integrity, Moderate), (Availability, Moderate)}

But wait…there's more!

- Some institutions have GREAT home grown, best practice based data classification policies:
  - George Washington University
  - Stanford University
  - University of Texas - Austin

Stanford's Data Classification Guidelines

	Restricted Data (highest, most sensitive)	Sensitive Data (moderate level of sensitivity)	Public Data (low level of sensitivity)
Legal requirements	Protection of data is required by law (e.g., see list of specific HIPAA and FERPA data elements)	Stanford has a contractual obligation to protect the data	Protection of data is at the discretion of the owner or custodian
Reputation risk	High	Medium	Low
Other Institutional Risks	Information which provides access to resources, physical or virtual	Smaller subsets of protected data from a school or department	General university information
Access	Only those individuals designated with approved access and signed non-disclosure agreements	Stanford employees and non-employees who have a business need to know	Stanford affiliates and general public with a need to know
Examples	▪ Medical ▪ Students ▪ Prospective students ▪ Personnel ▪ Donor or prospect ▪ Financial ▪ Contracts ▪ Physical plant detail ▪ Credit card numbers ▪ Certain management information ▪ See below for more specific examples	▪ Information resources with access to restricted data ▪ Research detail or results that are not restricted data ▪ Library transactions (e.g., catalog, circulation, acquisitions) ▪ Financial transactions which do not include restricted data (e.g., telephone billing) ▪ Information covered by non-disclosure agreements	▪ Campus maps ▪ Business contact data (e.g., directory information) ▪ Email

Source: http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html

Other Resources

- Educause has a toolkit available online that provides step-by-step process guidance and templates;
- These materials provide a blueprint for handling data in a manner that is appropriate with laws, regulations, and compliance standards.
- https://wiki.internet2.edu/confluence/display/secguide/Confidential+Data+Handling+Blueprint#ConfidentialDataHandlingBlueprint-Step2

How to Implement

- Self Assessment: what are we doing now?
- Choose a methodology/standard for data classification;
- Classify data sets based on the approved methodology;
- Classify systems based on data types that they process;
- Re-Assess classifications for both data and systems annually.

Also check out...

- http://csrc.nist.gov/publications/PubsSPs.html
- http://csrc.nist.gov/publications/PubsFIPS.html
- http://www.isaca.com
- http://www.itgi.com

Audit Artifacts

- A data classification policy;
- Risk assessments by system;
- Completed data classifications (by system);
- DR strategy to ensure high criticality data/systems is protected against loss or damage;
- Annual reviews of data classification policy and ratings.

Key Takeaways:

- Data Privacy for certain types of data is mandated by law;
- More stringent data privacy legislation is coming;
- Data must be understood and classified in order to be adequately managed, controlled, and protected.
- Once critical data and systems have been identified controls must be implemented to achieve the privacy that is required.
- Annual assessments of classifications and controls are necessary.

Questions?

Contact Me at:

(301) 405.1057
bmarkham@umd.edu