# Data Classification, Security, and Privacy

## Jennifer Bayuk
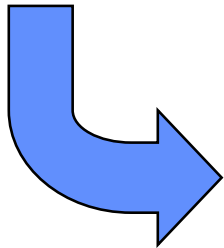
*Securities Industry and Financial Markets Association*

*Internal Audit Division*
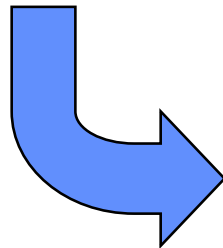
**October, 2007**

**BEAR STEARNS**

- **Logical Relationship**

- **Historical Practices**

- **Future Trends**

# Logical Relationship – Assumption

**Information model**

**Confidentiality, integrity, availability requirements**
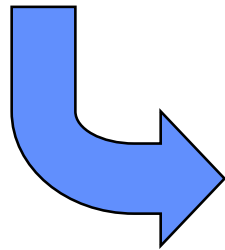
**Systems implementation**

# Logical Relationship - Assumption

*Note: Technically, an information classification program could start and end here. Existence of classification does not guarantee that associated requirements will be correctly developed or implemented.*

**Information model**
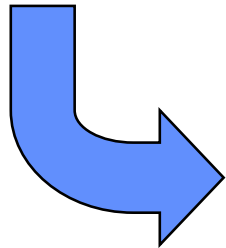
**Confidentiality, integrity, availability requirements**
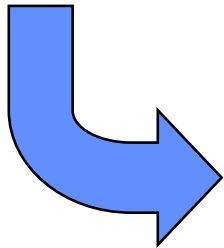
**Systems implementation**

**Quote from FFIEC InfoSec Handbook:**

Institutions may establish an information data classification program to <span style="color:red">identify</span> and <span style="color:red">rank</span> data, systems, and applications in order of importance. Classifying data <span style="color:red">allows</span> the institution to ensure <span style="color:red">consistent protection</span> of information and other critical data throughout the system. Classifying systems <span style="color:red">allows</span> the institution to <span style="color:red">focus</span> its controls and efforts in an efficient and structured manner.

# Logical Relationship - Expectation

*Completeness of implementation requires information to be labeled or collected in a consistent manner and stored accordingly.*

**Information model**

**Confidentiality, integrity, availability requirements**
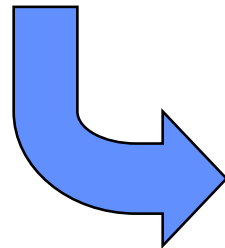
**Systems implementation**

*Information model instantiation.*

**BEAR STEARNS**

## Expectation is that each activity makes it easier to achieve the next:

Data Classification ➡ Protection Profile ➡ Desired State

aka: *Security*

aka: *Privacy*

Information model

↳ Confidentiality, integrity, availability requirements

↳ Systems implementation

# Historical Practices
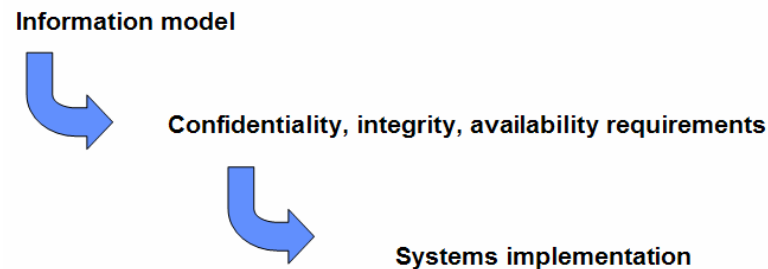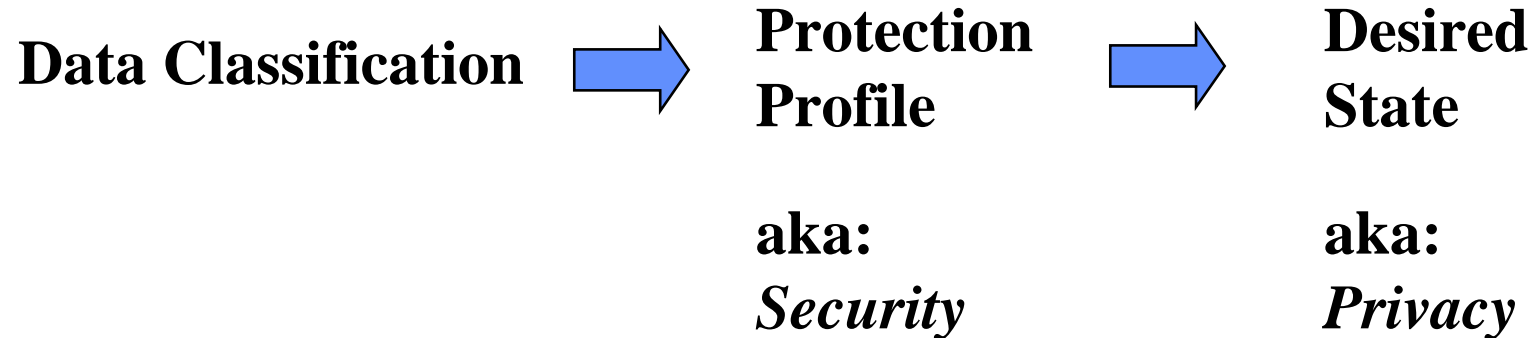
| Model | Example | Protection Profile | Desired state |
|---|---|---|---|
| *Military* | *Top Secret, Secret, Confidential, Public* | *System access according to level, no read up, no write down* | *Confidentiality* |
| *Common business adaptation* | *Mission critical, process-critical, non-public, public* | *Access and Change control over systems and applications according to level* | *Confidentiality, Integrity, Availability* |
| *Regulatory* | *PCI* | *Demonstrable due diligence for minimal access and quality controls at data level* | *Confidentiality, Integrity, Availability, Privacy* |

Require all information to be labeled as it is created

Store it only on systems that support these requirements:

- Prevent those at higher level from changing information at lower level (without an authorized change verification procedure)

- Prevent those at lower level from reading information at higher level

**Protection Profiles for each system to cover information lifecycle:**

- **handling**
- **storage**
- **transmission**
- **disposal**

**Systems that store or transmit data of different sensitivities should be classified as if all data were at the highest sensitivity.  Classification should be based on a weighted composite of all relevant attributes.**

*(source: FFIEC Information Security IT Examination Handbook)*

**Customized Protection Profiles for each system to cover information lifecycle, including:**

- Network, system, and application access controls

- Audit trail for access and change tracking

- Segregation of duties for critical changes

- Confidentiality procedures at user level

- Quality and change control over automated processing

- Backup and retention

- Recovery Time and Point objectives

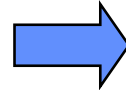**Actual protection measures are specifically proscribed for:**

- **Network architecture**

- **Network transmission**

- **Data storage**

- **Operating system security**

- **Application entitlements**

- **Media handling**

- **External Audit**

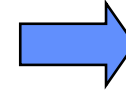*(source: PCI Security Standard Council)*

# Evolutionary Progression
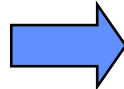
*Military*

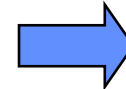Data Labels ➡ Rule-based Information Handling ➡ Confidentiality

*Business*

Data Classifications ➡ Protection Profile (via reasonableness standard) ➡ Confidentiality, Integrity, Availability

*Regulatory*

Data Specification ➡ Demonstrable Due Diligence ➡ CIA, plus Privacy "by definition"
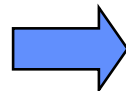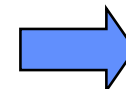
# Previous historical approaches

- *Were process rather than goal-oriented*

- *Relied on regulatory auditors to "raise the bar" on appropriate responses to risk*

- *Focused on aggregated data in systems and processes for handling, not on actual data content*

- *Did not entertain scenarios where multiple types of data in the same record in a single application or system should be treated differently at the infrastructure level*

# Regulatory Approach may be Problematic

**Data Classification** ➡️ **Protection Profile** ➡️ **Privacy (?)**

*InfoSec management best practices (e.g. ISO) are currently focused here, not here.*

*Priorities are decided based on perception of threat and vulnerabilities – focus is on closing holes at low cost, or having business "accept risk."*

*…..may generally be classified as*

- **Risk-Based**
  - Priorities are decided based on perception of threat and vulnerabilities – focus is on closing holes

- **Compliance based**
  - Priorities are decided based on requirements for due diligence using a reasonableness standard

*For the new era of regulatory approaches to Information Classification and associate control implementation, it needs to be goal-oriented.*

# Future Trends

- ***Reasonable measures are not good enough***

- ***Known vulnerabilities are not tolerable***

- ***Regulatory requirements are coming from customers and business partners in the form of legal contracts***

*PCI Data Security Standard (DSS) requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted.*

| | Data Element | Storage Permitted | Protection Required | PCI DSS Req. 3.4 |
|---|---|---|---|---|
| Cardholder Data | Primary Account Number (PAN) | YES | YES | YES |
| | Cardholder Name* | YES | YES* | NO |
| | Service Code* | YES | YES* | NO |
| | Expiration Date* | YES | YES* | NO |
| Sensitive Authentication Data** | Full Magnetic Stripe | NO | N/A | N/A |
| | CVC2/CVV2/CID | NO | N/A | N/A |
| | PIN / PIN Block | NO | N/A | N/A |

*\*   These data elements must be protected if stored in conjunction with the PAN.*
*\*\* Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).*

# PCI DSS V1.1

1: *Install and maintain a firewall configuration to protect cardholder data*

2: *Do not use vendor-supplied defaults for system passwords and other security parameters*

3: *Protect stored cardholder data (3.4 – detail with respect to PAN)*

4: *Encrypt transmission of cardholder data across open, public networks*

5: *Use and regularly update anti-virus software*

6: *Develop and maintain secure systems and applications*

7: *Restrict access to cardholder data by business need-to-know*

8: *Assign a unique ID to each person with computer access*

9: *Restrict physical access to cardholder data*

10: *Track and monitor all access to network resources and cardholder data*

11: *Regularly test security systems and processes*

12: *Maintain a policy that addresses information security*

# Example Securities Industry Data Types

Account access
(e.g. passwords, PINS)

Confidential (but not NPI)
counterparty

Confidential Firm Other

Customer holdings

Counterparty NPI

Banking Deal  Unannounced

Banking Info Other

Wide distribution nonpublic
(e.g. research)

Firm Holdings

Executed and reported
trades

Employee compensation

Employee NPI

Firm trade secrets

Pre-trade order flow

Public

*Are requirements as different as data types?*

# Example Securities Industry Data Types

Account access
   (e.g. passwords, PINS)

Counterparty NPI

Confidential (but not NPI)
   counterparty

Confidential Firm Other

Customer holdings

Pre-trade order flow

Executed and reported
   trades

Banking Deal  Unannounced

Banking Info Other

Wide distribution nonpublic
   (e.g. research)

Firm Holdings

Firm trade secrets

Confidential Firm Other

Employee compensation

Employee NPI

Public

*How many control groupings are there?*

# Example Securities Industry Data Types

**Account access (e.g. passwords, PINS)**

**Counterparty NPI**

**Confidential (but not NPI) counterparty**

**Confidential Firm Other**

**Customer holdings**

**Pre-trade order flow**

**Executed and reported trades**

**Banking Deal Unannounced**

**Banking Info Other**

**Wide distribution nonpublic (e.g. research)**

**Firm Holdings**

**Firm trade secrets**

**Confidential Firm Other**

**Employee compensation**

**Employee NPI**

**Public**

*Note: this is your web page!*

*Is it necessarily a hierarchy of controls?*

# *Discussion*