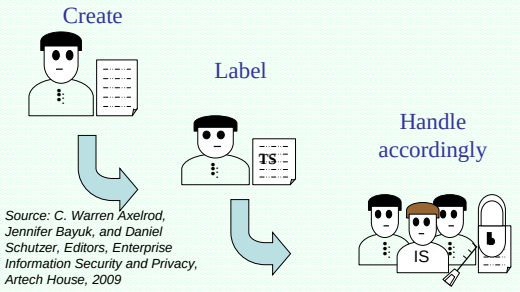
Information Classification

Jennifer L. Bayuk
jennifer@bayuk.com
www.bayuk.com

Overview

- Textbook information classification schemes and why to avoid them.
- Application inventory and corresponding data repositories.
- Roles and responsibilities with respect to data handling.
- Database schema basics required for classification efforts.
- Field-based information classification and protection techniques.
- Content filtering technology alternatives.

The Textbook Approach



Source: C. Warren Axelrod, Jennifer Bayuk, and Daniel Schutzer, Editors, Enterprise Information Security and Privacy, Artech House, 2009

"Handle Accordingly" Assumption

Information model

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.

Confidentiality, integrity, availability requirements

Systems implementation

Sanity Check:

Quote from FFIEC InfoSec Handbook:

Institutions may establish an information data classification program to identify and rank data, systems, and applications in order of importance. Classifying data allows the institution to ensure consistent protection of information and other critical data throughout the system. Classifying systems allows the institution to focus its controls and efforts in an efficient and structured manner.

Information Classification Assumption

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

Information Classification and Labeling → **Protection Profile** → **Desired State**

aka: *Security*

aka: *Privacy, Confidentiality*

Source: C. Warren Axelrod, Jennifer Bayuk, and Daniel Schutzer, Editors, Enterprise Information Security and Privacy, Artech House, 2009

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	Periodicity of access list and change control audits on systems containing data is increased according to level	Confidentiality, Integrity, Availability

Military Requirements for Protection Profile

- *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

(source: Amoroso, Fundamentals of Computer Security Technology, 1994)

Common Business Adaptation

- *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)

Business Strategy for Protection Profiles

- **Principal:** Information stored in or processed by (critical business applications | computer installation | network | end user environment) should be classified, based on its confidentiality, using an approved information classification scheme.
- **Objective:** To determine the level of protection that should be applied to the (critical business applications | computer installation | network | end user environment), thereby preventing unauthorised disclosure.
- General Strategy: ***Customized*** *Protection Profiles for each* (critical business applications | computer installation | network | end user environment) *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

Source: Standards of Good Practice, Information Security Forum, 2007 (www.securityforum.org).

Prescriptive Approach

- *Actual protection measures are specifically proscribed for:*
  - Network architecture
  - Network transmission
  - Data storage
  - Operating system security
  - Application entitlements
  - Media handling
  - External Audit

(source: Payment Card Industry Data Security Standard, Version 1.2 October 2008)

Historical vs Prescriptive

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	Periodicity of access list and change control audits on systems containing data is increased according to level	Confidentiality, Integrity, Availability
Prescriptive	Payment Card Industry Data Security Standards	Demonstrable due diligence for minimal access and quality controls at data level	Confidentiality, Integrity, Availability, and *Privacy for Data Subject*

Hierarchy Gone from Implementation Approach

Model	*Example*	*Implementation Approach*
Military	Top Secret, Secret, Confidential, Public	TopSecret always gets more security than secret, secret gets more than confidential, and public gets the least amount of security.
Common business adaptation	Mission critical, process-critical, non-public, public	Mission critical always gets more security than process-critical, process gets more than non-public, public gets the least amount of security.
Prescriptive	Payment Card Industry Data Security Standards	Some data fields get more security than others, even though they are not necessarily more critical to the organizational mission.

Information Classification Assumption Revisited

Information Classification and Labeling → **Protection Profile** → **Desired State**

aka: *Security*

aka: *Privacy, Confidentiality*

\+

Data Handling Requirements ← *Missing from original assumption*

Example: PCI Data Security Standards

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).

Evolutionary Progression

Military

Data Labels → **Rule-based Information Handling** → **Confidentiality**

Business

Data Classifications → **Protection Profile (via general strategies)** → **Confidentiality, Integrity, Availability**

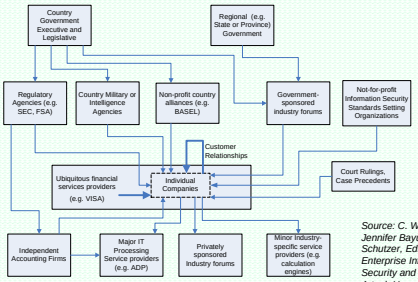
Prescriptive

Data Specification → **Demonstrable Due Diligence** → **CIA, plus Privacy "by definition"**

Textbook 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

Sources of Information Classification Schemas



Source: C. Warren Axelrod, Jennifer Bayuk, and Daniel Schutzer, Editors, Enterprise Information Security and Privacy, Artech House, 2009

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, software)*
- *Firm Holdings*
- *Executed trades*
- *Employee compensation*
- *Employee NPI*
- *Firm trade secrets*
- *Pre-trade order flow*
- *Public*

NOTE: This is your website!

There may be some similar protection profiles.

But is this a hierarchy of levels?

BREAK

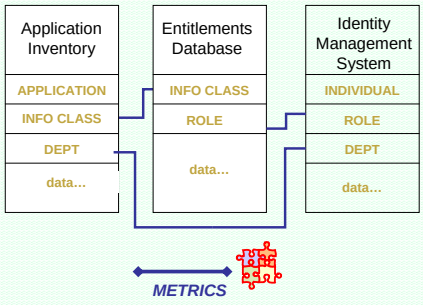
Groups should gather by industry and come up with a list of at least five information classification categories in their own industry and be prepared to describe the protection profile.

Application Inventory

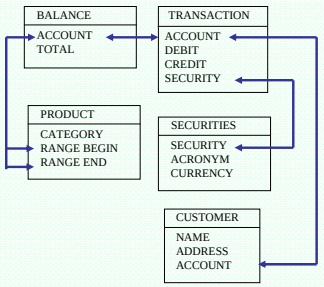
Area	Applications / Products	Commissions	Trade Surveillance	General Ledger	Finance Reporting	Fixed Asset	Bloomberg	Proprietary Research	Clearing Services	Lawson	Building Mgmt	Email	Active Directory
Front Office	Equities		CC,POF,ERT			POF,ERT	WDP	WDP				CFO	
	Research						WDP	FTS				CFO	
	Research Sales						WDP	FTS				CFO	
	Portfolio Trading		CC,POF,ERT				WDP	WDP				CFO	
	Derivatives/Options	EC	CC,POF,ERT				WDP	WDP				CFO	
	Proprietary Trading		POF,ERT		FH	POF,ERT	WDP	WDP				CFO	
Back Office	Back Office Ops	CFO				ERT			FH,ERT			CFO	
	Global Risk			FH	FH		WDP	WDP	FH,ERT		CFO	CFO	
	Finance	CFO		FH	CFO			WDP		CFO,EC		CFO	
	Compliance		CC	FH	CFO			WDP	FH,ERT	EC		CFO	
	Legal											CFO	
	Information Tech	WDP	WDP	WDP	WDP	WDP	WDP	WDP	WDP	WDP	WDP	CFO	AA
	Strategic Planning	CFO,EC		FH	CFO		WDP	WDP				CFO	
	Facilities										CFO	CFO	
	Human Resources									EC,EN		CFO	

Account access	AA	Firm Holdings	FH
Confidential counterparty	CC	Executed and reported trades	ERT
Confidential Firm Other	CFO	Employee compensation	EC
Customer holdings	CH	Employee NPI	EN
Counterparty NPI	CN	Firm trade secrets	FTS
Banking Deal Unannounced	BDU	Pre-trade order flow	POF
Banking Info Other	BIO	Public	PUB
Wide distribution nonpublic	WDP		

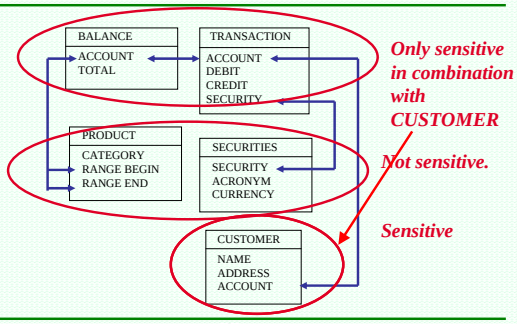
Application Inventory



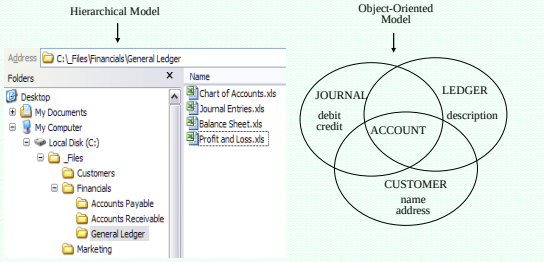
Database Schema Basics



Example Requirements

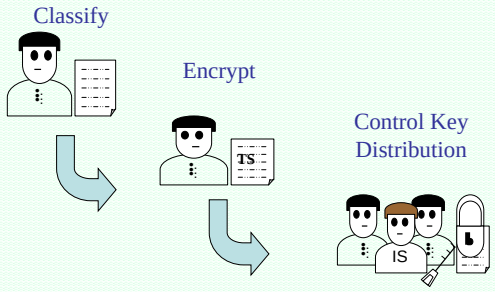


Other Data Storage Models

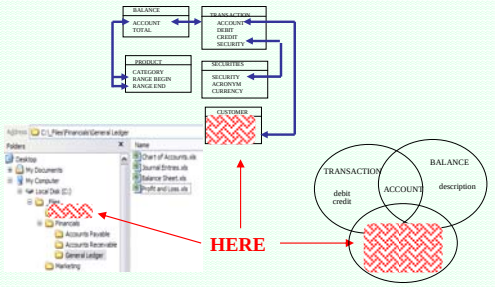


Source: C. Warren Axelrod, Jennifer Bayuk, and Daniel Schutzer, Editors, Enterprise Information Security and Privacy, Artech House, 2009

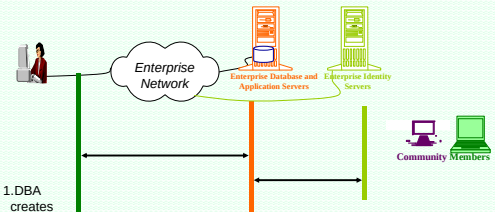
The Encryption Approach



Encryption = > Isolation



Database Field Encryption



1.DBA creates database schema, specifying fields requiring encryption

2.DBA grants rights to certain application community (perhaps at server level)

3.DBMS encrypts specified fields with keys and restricts key access to application users

4.All users log into app to either store or retrieve data

Database Encryption Pros and Cons

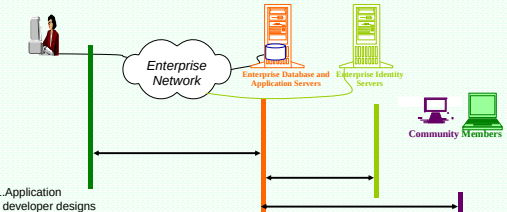
Pros:

- Where users cannot access the database directly, but instead the application has the only database login with database decryption capability, user access to data can be restricted to application functionality. For example, applications can restrict the amount of data a user can decrypt with a single operation to prevent users from copying whole files or unencrypted data in bulk.
- Allows a department authority to specify which groups of individuals certain types of information should be shared. Users cannot arbitrarily add individuals to access lists.
- Correct implementation does not rely on correct user behavior or application code.

Cons:

- Database Administrators (DBAs) and Application Support staff still have keys to the kingdom (though their access may be audited).
- Anyone with direct DBMS login access that is in a group with access to the keys may still bulk-download data and, given the overhead of user-level audit on DBMS queries, it is not likely that the access would be audited.
- If database fields that are encrypted have utility beyond a single application, reports that include the data may be difficult to generate, because select queries that rely on matching data across tables may be difficult if not impossible to implement.

Application Field Encryption



1.Application developer designs encryption APIs that encrypt prior to store and decrypt upon DB retrieval, DB schema is equipped with shadow query field

2.Application admin grants rights to users based on need to know

3.APIs encrypt specified fields with keys encrypted by user-level keys and requires user to present private key to decrypt

4.All users log into app to and present keys to store or retrieve data

Application Level Pros and Cons

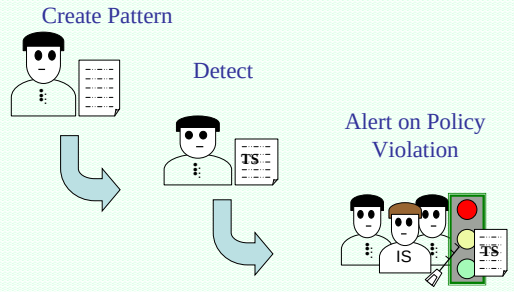
Pros:

- Allows user access to data to be restricted to application functionality without exception. For example, applications can restrict the amount of data a user can decrypt with a single operation to prevent users from copying whole files or unencrypted data in bulk.
- Allows a department authority to specify which groups of individuals certain types of information should be shared. Users cannot arbitrarily add individuals to access lists.
- DBA can be prevented from accessing decryption keys by storing them on alternative technology, so administrative access to data would require multiple administrators to collude to violate policy.

Cons:

- The correct implementation relies on correct application source code. A rogue developer could allow excessive access to data by putting back-doors in the code. However, they could not grant access to data to anyone that did not have access to the application.
- If database fields are encrypted that have utility beyond a single application, all applications and reports that use them must rely on the shadow field to specify records. If the shadow field becomes corrupted (perhaps via a bug in the application source code), the only way to recreate the data would be to decrypt and recreate all the encrypted records and shadow fields.

The Pattern-Filter Approach



The Pattern-Filter Alternative

- Devices placed strategically around network monitoring traffic for pre-defined patterns, e.g. NNN-NN-NNNN.
- Requires all traffic to be cleartext.
- Usually technology-specific – requires different software for shared file systems, database, email, web.
- Can be configured to alert or just log (either way, false positives require investigation)
- Often marketed as “Data Loss Prevention.”

Pattern-Filter Pros and Cons

Pros:

- Does not require operator to understand application data flow.
- Can act as detective supplement to preventive control of data containment via encryption.

Cons:

- Requires data to be defined by technology patterns rather than business semantics.
- It is difficult to define patterns that do not also flag false positives.
- Insiders who understand strategic placement of system and limitations of reliance on cleartext can easily defeat.

Proscriptive 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.”

Future Trends

- General security strategies are no longer good enough.
- Known vulnerabilities are not tolerable.
- Proscriptive requirements are coming from customers and business partners in the form of legal contracts.

Questions? Discussion…

Jennifer L. Bayuk
jennifer@bayuk.com
www.bayuk.com