



# Data Privacy and Risk Management

---

Jack Freund, CISSP/MP, CISA, CIPP  
FAIR Analyst  
[jfreund@riskmanagementinsight.com](mailto:jfreund@riskmanagementinsight.com)

# Whence PII...

Center Studios, LLC  
2000 Auburn Drive  
One Chagrin Highlands St.  
Beachwood, OHIO 44122

**LAWriter®** Ohio Laws and Rules

Route: [Ohio Revised Code](#) » [TITLE \[1-3\] XIII COMMERCIAL TRANSACTIONS -- OHIO UNIFORM COMMERCIAL CODE](#) » [CHAPTER 1349: CONSUMERS](#)

### 1349.19 Private disclosure of security breach of computerized personal information data

(A) As used in this section:

(1)(a) "Breach of the security of the system" means unauthorized access to and acquisition of computerized data that compromises the security of or a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person.

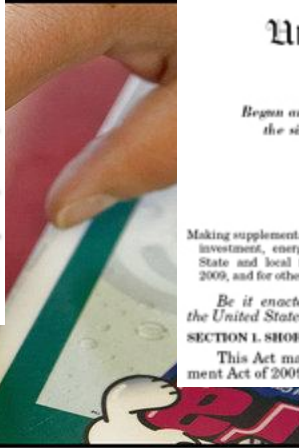
(b) For purposes of division (A)(1)(a) of this section:

(i) Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security of the system if the information is not used for an unlawful purpose or subject to further unauthorized disclosure.

(ii) Acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a person is not a breach of the security of the system.

(2) "Business entity" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether operating or not, organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country.

(3) "Consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" means a consumer reporting agency that regularly and routinely collects, receives, and disseminates information from third parties bearing on a consumer's creditworthiness, credit standing, or credit record.



One Hundred Eleventh Congress  
of the  
United States of America  
**AT THE FIRST SESSION**  
*Began and held at the City of Washington on Tuesday,  
the sixth day of January, two thousand and nine*

**An Act**

Making supplemental appropriations for job preservation and creation, infrastructure investment, energy efficiency and science, assistance to the unemployed, and State and local fiscal stabilization, for the fiscal year ending September 30, 2009, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

**SECTION 1. SHORT TITLE.**  
This Act may be cited as the "American Recovery and Reinvestment Act of 2009".



# Data Privacy Lifecycle - Collection

---

Name	Value
Name	<input type="text"/>
Sex	<input type="radio"/> Male <input checked="" type="radio"/> Female
Eye color	green ▾
Check all that apply	<input type="checkbox"/> Over 6 feet tall <input type="checkbox"/> Over 200 pounds
Describe your athletic ability:	
<input type="text"/>	
<input type="button" value="Enter my information"/>	

- Privacy Statements
- Fair and Lawful Collection and Processing

# Data Privacy Lifecycle – At Rest

---



- Retention and Disposal
- Accuracy
- Notification Triggers



# Data Privacy Lifecycle – Sharing

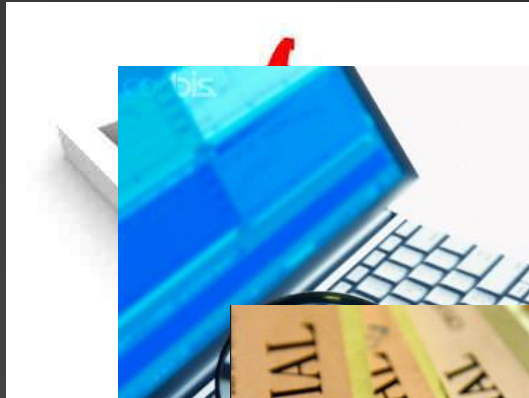
---



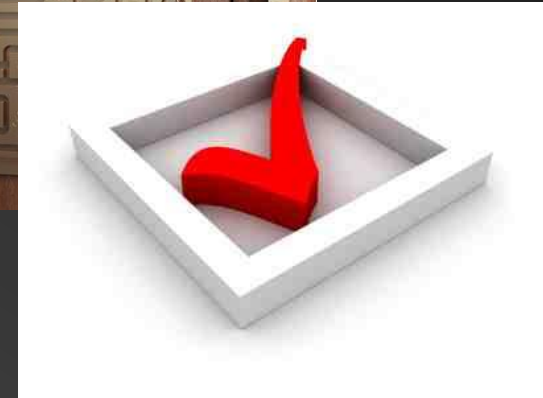
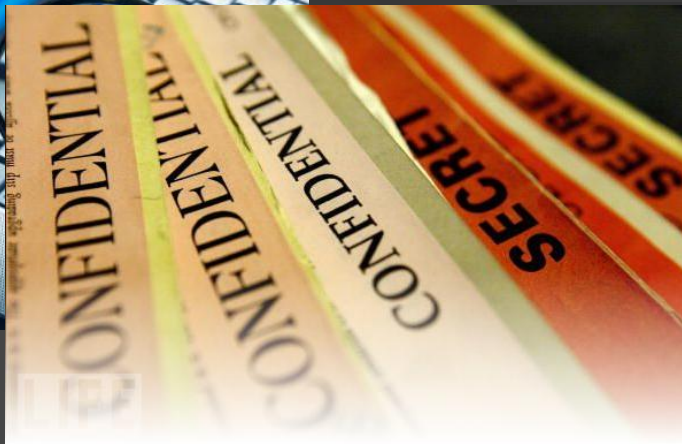
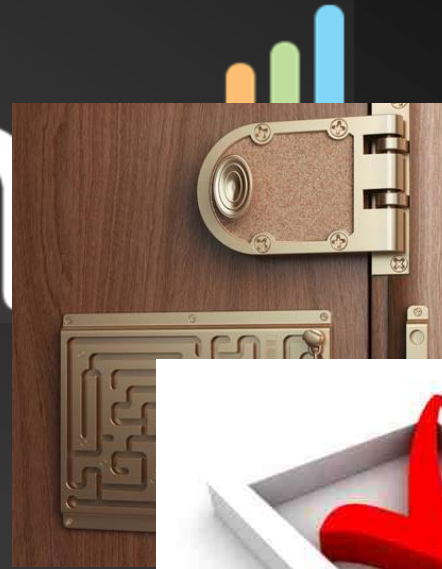
- Complaints and Appeals
- Third Parties/Data Sharing
- Consent to New Purposes

# Data Privacy Management Process

---



rmi

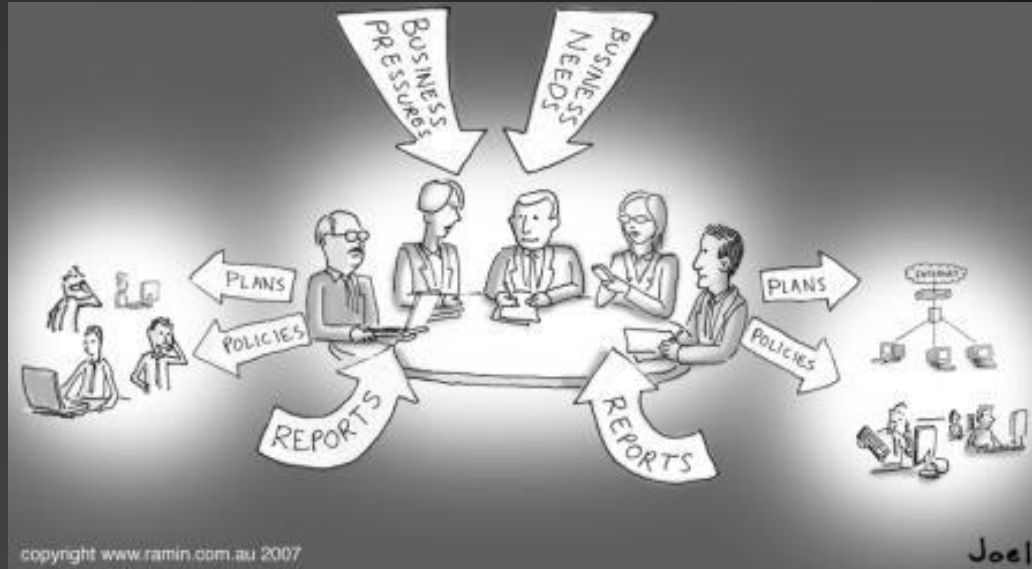


## Governance



# Govern...

---



- Define expectations
- Grant Power
- Verify Performance

# Finding that data...



# Classify

---

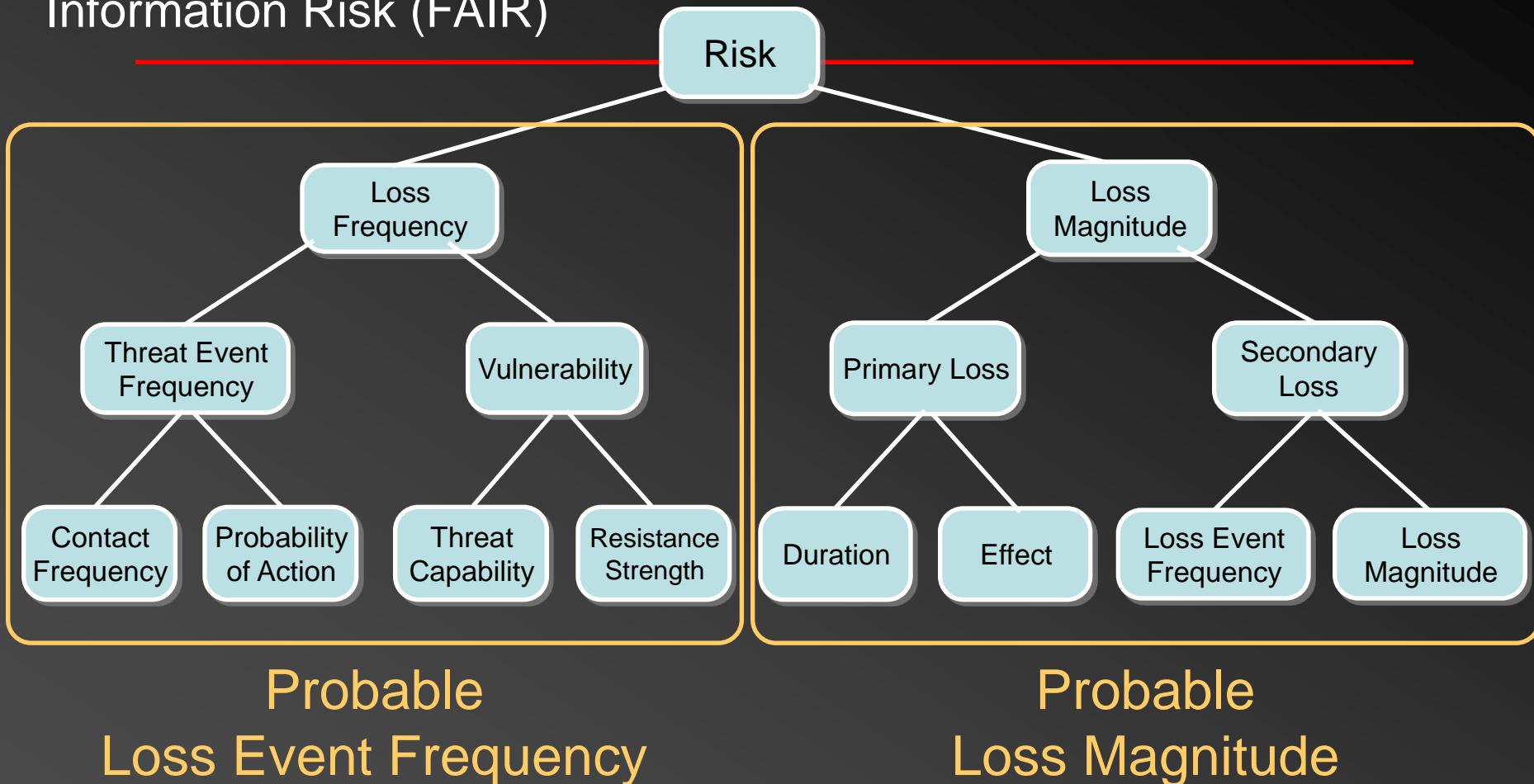


THE GEORGE  
WASHINGTON  
UNIVERSITY  
WASHINGTON DC

**Responsible University Official:**  
Chief Information Officer  
**Responsible Office:** Information  
Systems and Services  
**Origination Date:** April 12, 2004

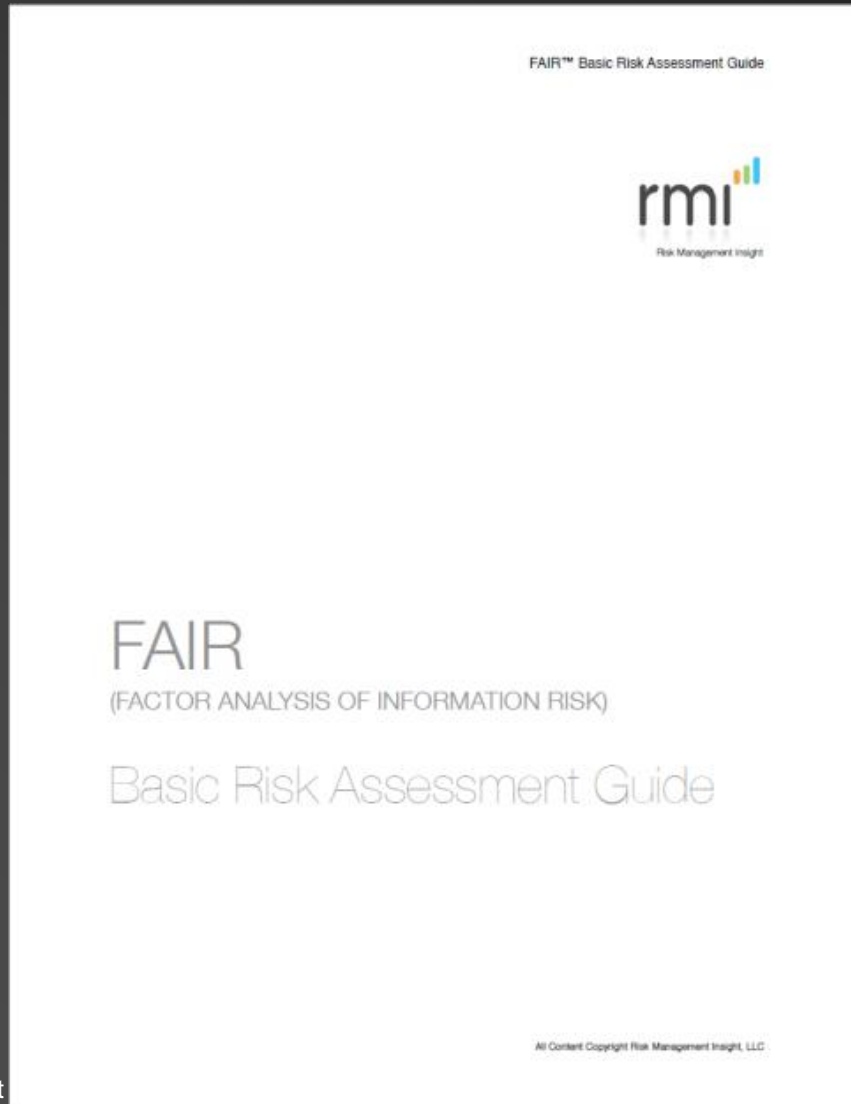
## DATA CLASSIFICATION SECURITY POLICY

# Factor Analysis of Information Risk (FAIR)



# Assessing Privacy Risk Using FAIR

---



## BRAG

1. ID Scenario
2. LEF
3. PLM
4. Calc



# The Scenario...Asset

---



The Credit Card Database  
PCI CHD Environment



# The Scenario...Threat (Tcom)

---

- Internal
  - Privileged
    - Technical
    - Non-Technical
  - Non-Privileged
    - Technical
    - Non-Technical
- External
  - Professional
    - Technical
    - Non Technical
  - Amateur
  - Malware

# Risk = LEF \* PLM

## FAIRLite v3.0

### Loss Event Frequency

Primary		Min	ML	Max	Curve Shape
	TEF	10	12	24	M
	Tcap	20%	50%	90%	M
	RS	40%	50%	65%	M
Secondary	LEF%	1%	5%	50%	M

### LOSS MAGNITUDE

Primary		Min	ML	Max	Curve Shape
	Productivity	\$ 25,000	\$ 35,000	\$ 50,000	M
	Response	\$ 1,000	\$ 10,000	\$ 35,000	M
	Replacement	\$ -	\$ -	\$ -	M
	CompAdv	\$ -	\$ -	\$ -	M
	F/J	\$ -	\$ -	\$ -	M
	Reputation	\$ -	\$ -	\$ -	M
Secondary	Productivity	\$ -	\$ -	\$ -	M
	Response	\$ -	\$ -	\$ -	M
	Replacement	\$ -	\$ -	\$ -	M
	CompAdv	\$ -	\$ -	\$ -	M
	F/J	\$ -	\$ 35,000	\$ 350,000	M
	Reputation	\$ -	\$ -	\$ -	M

Iterations



# What is our risk?

Primary		Minimum	Average	Mode	Maximum
LEF (yr)		4.82	6.04	5.58	8.18
LM	\$	33,576	45,993	46,873	58,904

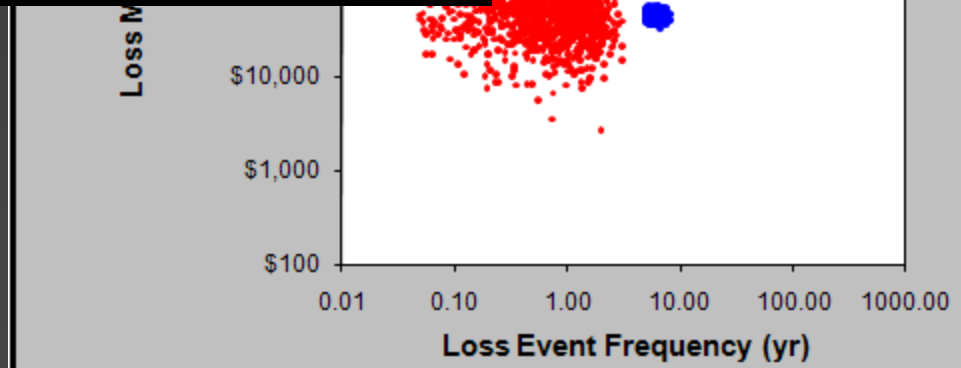
Secondary		Minimum	Average	Mode	Maximum
LEF (yr)		0.05	0.88	0.49	3.56
LM	\$	1,338	47,653	33,358	184,312

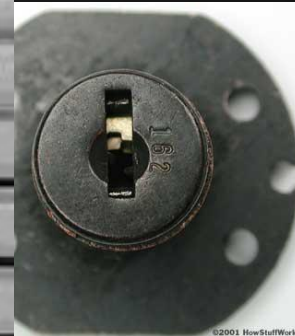
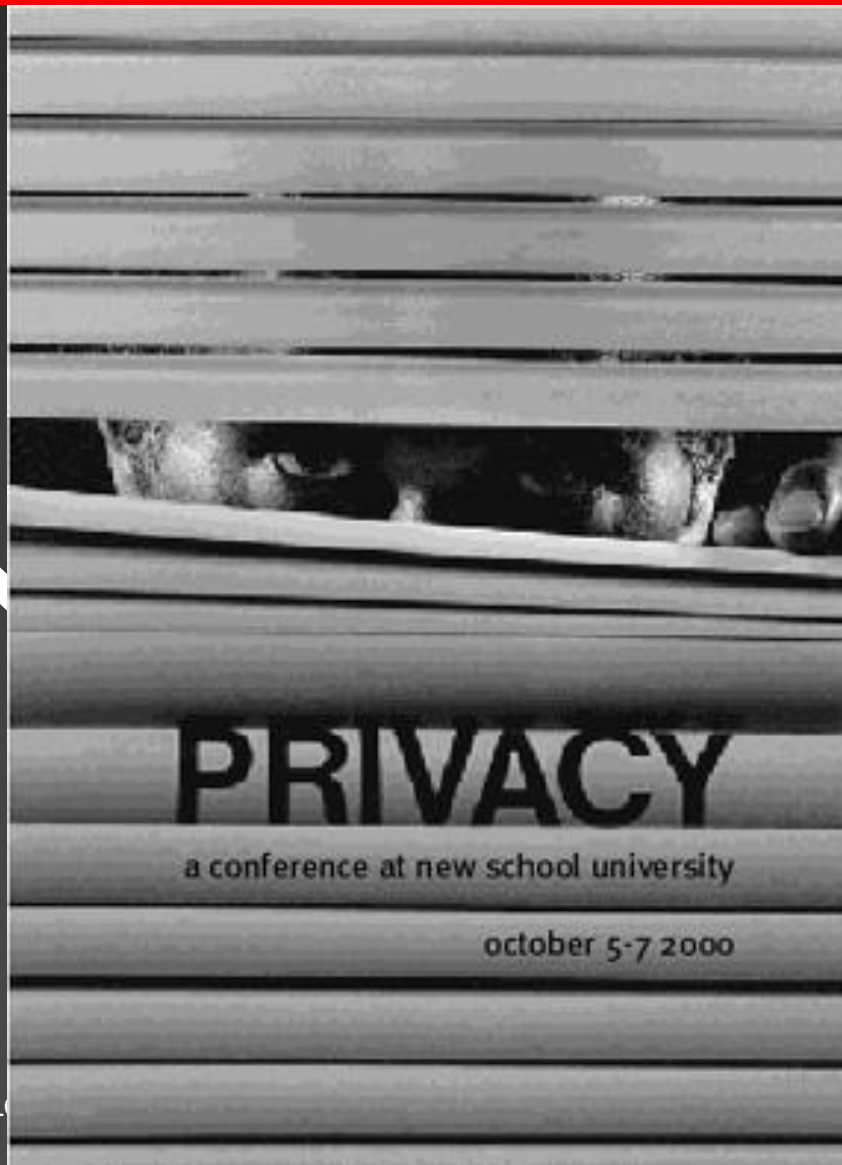
Total Exposure		Minimum	Average	Mode	Maximum
LEF (yr)					
LM	\$				

Risk Levels	Avg Exp >
Very High	\$ 10,000,000
High	\$ 1,000,000
Medium	\$ 100,000
Low	\$ 10,000
Very Low	\$ 1,000

Risk Primary ■  
Secondary ■



# If I buy this...



©2001 HowStuffWorks



---

# Questions?

