# Strengthening Data Privacy in PeopleSoft

Collaborate '08

Marilyn Prosch, Ph.D., CIPP
Arizona State University
School of Global Management & Leadership

Monica Nelmes Elliott
Approva Corporation
PeopleSoft Product Marketing

# Objectives

- Trends in data privacy and security breaches
- How Generally Accepted Privacy Principles (GAPP) are evolving to a meet a need for Continuous Privacy Monitoring (CPM)
- Automating GAPP to monitor user access information to prevent Segregation of Duties (SoD) violations and sensitive access issues
- Specific security risks and data governance issues in PeopleSoft
- Business case (costs/benefits) for implementing CPM

# Objectives

- ✓ Trends in data privacy and security breaches
- How Generally Accepted Privacy Principles (GAPP) are evolving to a meet a need for Continuous Privacy Monitoring (CPM)
- Automating GAPP to monitor user access information to prevent Segregation of Duties (SoD) violations and sensitive access issues
- Specific security risks and data governance issues in PeopleSoft
- Business case (costs/benefits) for implementing CPM

# 2007 was another year of growth in Privacy Breaches

- A former contractor for Bank of America unauthorizedly accessed the personal information (name, address, phone number, Social Security number) of an undisclosed number of customers, for the purpose of committing fraud.
  - The names and Social Security numbers of Hertz employees dating back to discovered on the home computer of a former employee.
- According to documents obtained under the Freedom of Information Act, 478 laptops were either lost or stolen from the IRS between 2002 and 2006. 112 of the computers held sensitive taxpayer information such as SSNs.
  - Laptop and data disk were stolen from the locked trunk of an unnamed auditor.
- A bag containing approximately 700 completed passport applications was reported missing on December 1. The bag, which was supposed to be shipped to Charlotte, NC, was found later in the International Airport.
  - Overseas hackers broke into two computers at Children's Hospital. One contains private patient data (including Social Security numbers) and the other holds billing and banking information.
- Mortgage files that included personal financial details about loan applicants were found in a dumpster. Empire Equity will pay $12,500 to the State of NC.


J. P. Morgan
General Electric
Gander Mountain
Gap Inc
*Atlantic Plastics, Inc.* *via accounting firm Hancock Askew*
*Wells Fargo* *via unnamed auditor*
Merrill Lynch
McKesson
Fidelity National Information Services
Premier Bank
*Altria & United Technologies* *via benefits consultant, Towers Perrin*
Albertson's
IBM
Lloyd's of London (FL)
Turbo Tax
TJ Stores
*Direct Loans* *via its IT contractor ACS*
Check into Cash
T-Mobile USA Inc
ADP
Winn-Dixie
Caterpillar, Inc.
Circuit City and Chase Card Services
Dai Nippon
TD Ameritrade
KeyCorp
Deb Shops, Inc.
Electronic Data Systems
Ceridian Corp.
Columbia Bank
Linden Lab
Bank of America
Pfizer
Greater Media, Inc.
Wesco
Hertz Global Holdings, Inc.
Piper Jaffrey
Tax Service Plus
Voxant.com
*Major League Baseball players* *via SFX Baseball, Inc.*
CVS Pharmacy
Life Is Good
Starbucks Corp.
Metro Credit Services
H&R Block
HarborOne Credit Union
West Shore Bank
Texas First Bank
Neiman Marcus
Telesource via Vekstar
ABN Amro Mortgage Group
VISA/FirstBank
Verisign
Boeing
eBay
Rabun Apparel Inc
Compulinx
KB Homes
RadioShack
American Family Insurance
Western Union
KSL Services, Inc
American Airlines
Hortica
Disney Movie Club
Stop & Shop Supermarkets
New Horizons Community Credit Union
Nikon Inc. and Nikon World Magazine
CTS Tax Service
Avaya
Empire Equity Group
MoneyGram International
Monster.com
Front Range Ski Shop
Fox News
Limewire
Johnny's Selected Seeds
Nissan Motor Co., Ltd.
Alcatel-Lucent
TennCare / Americhoice Inc.
Home Finance Mortgage, Inc.
American Education Services
AT&T
Four ARCO gas stations
*TransUnion Credit Bureau* *via Kingman, AZ, court office*
Couriers on Demand
Gymboree
*Aetna / Nationwide / Wellpoint Group Health Plans* *via Concentra Preferred Systems*
Jax Federal Credit Union
Cricket Communications
Kingston Technology Co.
Movie Gallery
*Howard & Partners law firm* *via its auditor Morris, Davis & Chan*
Chase Bank
Science Applications International Corp. (SAIC)


J. P. Morgan
General Electric
Gander Mountain
Gap Inc
Atlantic Plastics, Inc. via accounting firm Hancock Askew
Wells Fargo via unnamed auditor
Merrill Lynch
McKesson
Fidelity National Information Services
Premier Bank
Altria & United Technologies via benefits consultant, Towers Perrin
Albertson's
PeopleSoft
Turbo Tax
IBM
TJ Stores
Direct Loans via its IT contractor ACS
Check into Cash
T-Mobile USA Inc
ADP
Winn-Dixie
Caterpillar, Inc.
Circuit City and Chase Card Services
Dai Nippon
TD Ameritrade
KeyCorp
Deb Shops, Inc.
Electronic Data Systems
Ceridian Corp.
Bank of America
Columbia Bank
Linden Lab
Pfizer
Greater Media, Inc.
Wesco
Hertz Global Holdings, Inc.
Piper Jaffrey
Tax Service Plus
Voxant.com
Major League Baseball players via SFX Baseball, Inc.
CVS Pharmacy
Life Is Good
Starbucks Corp.
Metro Credit Services
H&R Block
HarborOne Credit Union
West Shore Bank
Texas First Bank
Neiman Marcus
Telesource via Vekstar
ABN Amro Mortgage Group
VISA/FirstBank
Verisign
Boeing
eBay
Rabun Apparel Inc
Compulinx
KB Homes
RadioShack
American Family Insurance
Western Union
KSL Services, Inc
American Airlines
Disney Movie Club
Hortica
Stop & Shop Supermarkets
New Horizons Community Credit Union
Nikon Inc. and Nikon World Magazine
CTS Tax Service
Avaya
Empire Equity Group
MoneyGram International
Monster.com
Front Range Ski Shop
Fox News
Limewire
Johnny's Selected Seeds
Nissan Motor Co., Ltd.
Alcatel-Lucent
TennCare / Americhoice Inc.
Home Finance Mortgage, Inc.
American Education Services
TransUnion Credit Bureau via Kingman, AZ, court office
Couriers on Demand
AT&T
Four ARCO gas stations
Gymboree
Aetna / Nationwide / Wellpoint Group Health Plans via Concentra Preferred Systems
Jax Federal Credit Union
Cricket Communications
Kingston Technology Co.
Movie Gallery
Howard & Partners law firm via its auditor Morris, Davis & Chan
Chase Bank
Science Applications International Corp. (SAIC)

U.S. Dept. of Commerce
and Census Bureau

FEMA

*Transportation Security Administration* *via Accenture*

U.S. Army Cadet Command

U.S. Dept. of Agriculture

Internal Revenue Service

Congressional Budget Office

U.S. State Department

*Camp Pendleton Marine Corps base* *via Lincoln B.P. Management*

Army National Guard
130th Airlift Wing

Picatinny Arsenal
DOD Weapons Research Center

U.S. Dept. of Veteran's Affairs

Indian Consulate
via Haight Ashbury
Neighborhood Council Recycling

American Ex-Prisoners of War

*Colorado Dept. of Human Services* *via Affiliated Computer Services (ACS)*

Wisconsin Dept. of Revenue
via Ripon Printers

Wisconsin Assembly

Administration for Children's Services - NY

NY Dept. of State

NY Dept. of Labor

Kentucky Personnel Cabinet

Florida National Guard

Florida Labor Department

NC Dept. of Transportation

North Carolina Dept. of Motor Vehicles

North Carolina Dept. of Revenue

Illinois Dept. of Corrections

Illinois Dept. of Financial
and Professional Regulation

Illinois Dept. of Transportation

Michigan Dept. of Community Health

Massachusetts Dept. of Industrial Accidents

Indiana State Department of Health

Indiana Dept. of Administration

Indiana Dept. of Transportation

Indiana State Web site

*State of Connecticut* *via Accenture Ltd.*

Connecticut Department of Revenue Servi

Conn. Office of the State Comptroller

California National Guard

California Public Employees'
Retirement System

Calif. Dept. of Health Services

Ohio state workers

Ohio State Auditor

Ohio Ethics Committee

Ohio Board of Nursing

Texas Commission on Law
Enforcement Standards & Education

Idaho Army National Guard

Georgia Secretary of State

Georgia County Clerk

Georgia Div. of Public Health

Maine State Lottery Commission

PA Public Welfare Department

PA Dept. of Transportation

West Virginia Board of
Barbers and Cosmetologists

Maryland Dept. of Natural Resources

Maryland Department of the Environment

Cuyahoga County
Dept. of Development

Los Angeles County
Child Support Services

Chicago Board of Elections

Chicago Voter Database

Tuscarawas County
and Warren County

Fresno County

City of Chicago via contractor

Detroit Water and Sewerage Department

Orange County (FL) Controller

Champaign Police Officers

City of Savannah

Huntsville County

Bowling Green Police Dept.

Santa Clara County
Employment Agency

Hidalgo County Commissioner's Office

Lynchburg City

Fort Monroe

Port of Seattle

ChildNet

Metropolitan St. Louis
Sewer District

City of Encinitas

Washiawa Women,
Infants and Children program (HI)

Pima Co. Health Dept.

City of Visalia, CA

Cleveland Air Route
Traffic Control Center

Fresno County/Refined Technologies Inc.

New York City Financial
Information Services Agency

City of Wickliffe, OH

*Berks Co. Sheriff's Office*
*via contractor Canon*
*Technology Solutions*

Johnston County, NC

City of Grand Prairie

City of Lubbock

Cumberland County, PA

Poulsbo Department of Licensing

---

Indianapolis Public Schools

Harrison County Schools

Chicago Public Schools
via All Printing & Graphics, Inc.

Waco Independent School District

Jackson Local Schools

Willamette Educational Service District

Chicago Public Schools

San Diego Unified School District

Greenville County School District

Clarksville-Montgomery County
Middle and High Schools

Shamokin Area School District

Germanton Elementary School

Cedarburg High School

St. Mary Parish

Riverside High School NC

San Juan Capistrano
Unified School District (CA)

Iowa Dept. of Education

Big Foot High School, WI

Yuma Elementary School District

Troy Athens High School

Loomis Chaffee School

St. Vrain Valley School District (CO)

Clay High School, OH


University of Colorado-Boulder, Leeds School of Business
Virginia Commonwealth University
University of Michigan
UCLA
University of Idaho
Rutgers-Newark University
Northwestern University
Loyola University
Yale University
University of Iowa – Psychology Dept.
Villanova University students & staff
Via Insurance broker
Purdue University
Mississippi State University
University of Missouri
Berry College
via consultant Financial Aid Services Inc.
Georgia Tech Univ.
Louisiana State Univ
Ohio State Univ.
University of Minnesota
University of South Carolina
Johns Hopkins University
Montana State University
Notre Dame University
University of Texas at Arlington
Texas A&M University
University of California, Davis
University of Virginia
University of Texas - Dallas
New Mexico State Univ.
University of Nebraska
Connors State College
University of Toledo
Texas Woman's University
Georgia Institute of Technology
University of New Mexico
Eastern Illinois University
Radford University
Westminster College
De Anza College
Univ. of Montana - Western
City College of San Francisco
UC San Francisco
Black Hills State Univ.
Cal State Los Angeles
Nassau Community College
Metropolitan State College of Denver
Central Connecticut State University
Montgomery College
Bowling Green State University
Adams State College
Los Rios Community College
Goshen College
Stony Brook University
Community College of Southern Nevada
Highlands University
Penn State Univ. - USMC
East Carolina University
Vanguard University
Gadsden State Community College
Grand Valley State University

Univ. of Pittsburgh, Med. Center

Manhattan Veteran's Affairs Medical Center &
New York Harbor Health Care System

Beaumont Hospital

*Sisters of St. Francis Health Services*
*via Advanced Receivables Strategy*

Swedish Medical Center

Univ. Calif. Irvine Medical Center

Group Health Cooperative Health Care System

Mercy Medical Center

DCH Health Systems

Johns Hopkins Hospital

Allina Hospitals and Clinics

Prudential Financial Inc.

Beacon Medical Services

Seton Healthcare Network

University of Pittsburgh Medical Center

DePaul Medical Center

Kaiser Medical Center

McAlester Clinic
& Veteran's Affairs Medical Center

Highland Hospital

Akron Children's Hospital

Back and Joint Institute of Texas

Cleveland Clinic

*Emory University Hospital, Emory Crawford Long Hospital, Grady Memorial Hospital, Geisinger Health System, Williamson Medical Center* *via Electronic Registry Systems*

Jacobs Neurological Institute

Gulf Coast Medical Center

Westerly Hospital

Erlanger Health System

Deaconess Hospital

WellPoint's Anthem
Blue Cross Blue Shield

Health Resources, Inc.

Kaiser Permanente Colorado

South County Hospital

Providence Alaska Medical Center

Swedish Urology Group

Intermountain Health Care

Gundersen Lutheran Medical Center

Stevens Hospital
via billing company Med Data

WorkCare Orem

Concord Hospital

St. Mary's Hospital, MD

St. Vincent Hospital

*Sky Lakes Medical Center*
*via Verus Inc*

Wellpoint's Empire Blue Cross/
Blue Shield NY

*Segal Group of New York*
*via web site of Vermont state agency*

Healing Hands Chiropractic

Georgia Dept. of Community Health

# Federal Trade Commission

- Settled 14 cases “challenging **faulty data-security practices** by companies that handle sensitive consumer information.”
- They almost always require a **security audit every 2 years for the next 10-20 years**.
- Recently, Guidance Software was sanctioned because a data-security failure allowed hackers to **access sensitive credit card information** for thousands of consumers.

# We are moving past the infancy stage - clients are beginning to want/ask for privacy risk protection!

- Both accounting firms and companies are looking for tools to help them respond

# Objectives

- ✓ Trends in data privacy and security breaches
- ✓ How Generally Accepted Privacy Principles (GAPP) are evolving to a meet a need for Continuous Privacy Monitoring (CPM)
- Automating GAPP to monitor user access information to prevent Segregation of Duties (SoD) violations and sensitive access issues
- Specific security risks and data governance issues in PeopleSoft
- Business case (costs/benefits) for implementing CPM

# Privacy Regulations Are Growing in Response to Breaches

**Domestic**

- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Trade Commission
- Safe Harbor

**International**

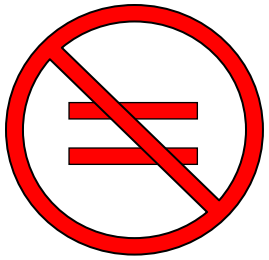
- Organization for Economic Co-Operation and Development (OECD) Guidelines
- European Union Directive
- Canada - Personal Information Protection and Electronic Documents Act (PIPEDA)
- Australia Privacy Act

**Generally Accepted Privacy Principles**

Developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA)

# Accountants Bring GAAP-like Principles to Privacy

**GAPP**
Generally Accepted ***Privacy*** Principles



**GAAP**
Generally Accepted ***Accounting*** Principles

*"The accounting industry has closed ranks around the idea that the GAPP is **the best international framework** for assessing the privacy health of an organization." – Computerworld, Dec 2007*

# GAPP is a Framework for Privacy

| | |
|---|---|
| 1) Management | The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures. |
| 2) Notice | The entity provides notice about its privacy policies and procedu[illegible]nd i[illegible]poses for which personal information is collected, used, retained, and di[illegible] |
| 3) Choice & Consent | The entity describes the choices available to the individual a[illegible] consent with respect to the collection, use, and disclosure of [illegible] |
| 4) Collection | The entity collects personal information only for the purpose[illegible] |
| 5) Use and Retention | The entity limits the use of personal information to the purposes i[illegible]ntified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes. |
| 6) Access | The entity provides individuals with access to their personal information for review and update. |
| 7) Disclosure to 3rd Parties | The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual. |
| 8) Security for Privacy | The entity protects personal information against unauthorized access (both physical and logical). |
| 9) Quality | The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice. |
| 10) Monitoring & Enforcement | The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes. |

66 Principles Split Across 10 Categories

# Auditors Are Developing Tools to Address GAPP

## GAPP

- Both External and Internal Auditors must respond to Privacy Regulation.
- GAPP provides a framework for both.

External Auditors

**AICPA/CICA "Risk Matrix"**

Provides guidance to practitioners on different types of privacy services that can be provided and the associated risk of providing these services

Internal Auditors

**Continuous Privacy Monitoring (CPM)**

Provides internal auditors and security professionals up-to-the-minute status on privacy-related information and violations

# AICPA/CICA "Risk Matrix"

| *Type of Service* | *Type of Report* | *Use Of Report* | *Needs Addressed* | *Potential Risks* | *Risk Mitigation Strategies* |
|---|---|---|---|---|---|
| Specific procedures defined by client and user(s) of report | | | | | |
| Privacy review | | | | | |
| Privacy assessment | | | | | |
| Privacy Audit | | | | | |
| Attestation report (AT101) on a service organization's controls | | | | | |
| Service auditor report | | | | | |
| Maturity models reporting | | | | | |
| Regulatory Compliance | | | | | |
| Regulatory Compliance | | | | | |
| Internal Audit | | | | | |

# Auditors Are Developing Tools to Address GAPP

## GAPP

- Both External and Internal Auditors must respond to Privacy Regulation.
- GAPP provides a framework for both.

External Auditors

**AICPA/CICA "Risk Matrix"**

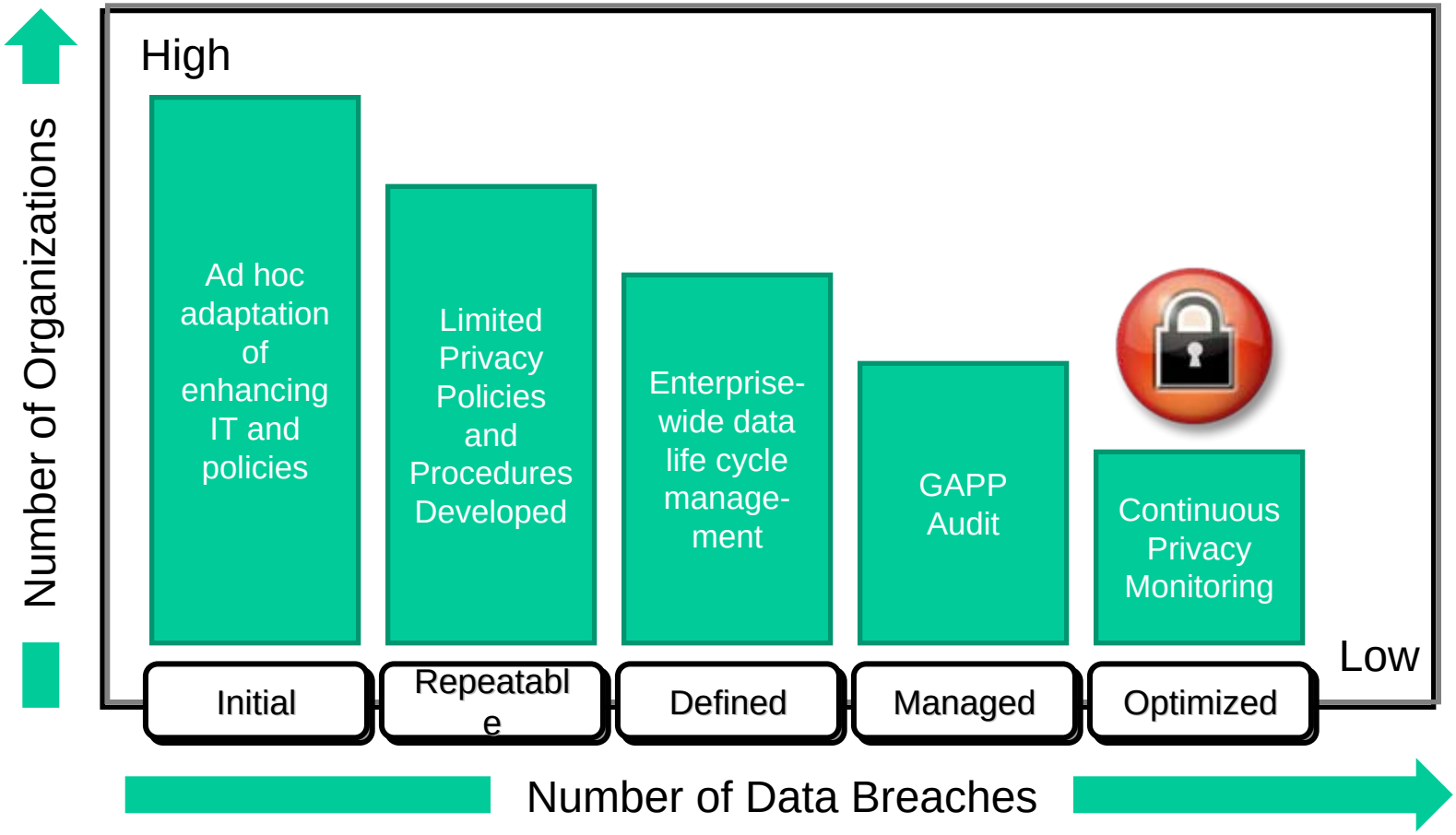
Provides guidance to practitioners on different types of privacy services that can be provided and the associated risk of providing these services

Internal Auditors

**Continuous Privacy Monitoring (CPM)**

Provides internal auditors and security professionals up-to-the-minute status on privacy-related information and violations

# CPM is Most Effective at Minimizing Breaches



# Objectives

- ✓ Trends in data privacy and security breaches
- ✓ How Generally Accepted Privacy Principles (GAPP) are evolving to a meet a need for Continuous Privacy Monitoring (CPM)
- ✓ Automating GAPP to monitor user access information to prevent Segregation of Duties (SoD) violations and sensitive access issues
- Specific security risks and data governance issues in PeopleSoft
- Business case (costs/benefits) for implementing CPM

# Approva Enables CPM of GAPP

| | |
|---|---|
| 1) Management | The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures. |
| 2) Notice | The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed. |
| 3) Choice & Consent | The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information. |
| 4) Collection | The entity collects personal information only for the purposes identified in the notice. |
| 5) Use and Retention | The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes. |
| 6) Access | The entity provides individuals with access to their personal inform |
| 7) Disclosure to 3rd Parties | The entity discloses personal information to third parties only fo notice and with the implicit or explicit consent of the indivi |
| 8) Security for Privacy | The entity protects personal information against unauthorized logical). |
| 9) Quality | The entity maintains accurate, complete, and relevant personal inf mation for the purposes identified in the notice. |
| 10) Monitoring & Enforcement | The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes. |

Automate 20% of GAPP with Approva

# Approva Enables CPM of GAPP

| | |
|---|---|
| 1) Management | 1.2.4 - Infrastructure and Systems Management<br>1.2.7 - Qualifications of Internal Personnel |
| 2) Management<br>3) Notice<br>4) Choice & Consent | Not Applicable |
| 5) Use and Retention | 5.2.2 - Retention of Personal Information |
| 6) Access | 6.2.1 - Access by Individuals to Their Personal Information<br>6.2.5 - Updating or Correcting Personal Information |
| 7) Disclosure to 3rd Parties | 7.2.2 - Protection of Personal Information with 3rd Parties |
| 8) Security for Privacy | 8.2.1 - Information Security Program 8.2.2 - Logical Access Controls<br>8.2.6 - Testing Security Safeguards |
| 9) Quality | 9.2.1 - Accuracy and Completeness of Personal Information |
| 10) Monitoring & Enforcement | 10.2.3 – Compliance Review<br>10.2.4 – Instances of Noncompliance |

# Objectives

- ✓ Trends in data privacy and security breaches
- ✓ How Generally Accepted Privacy Principles (GAPP) are evolving to a meet a need for Continuous Privacy Monitoring (CPM)
- ✓ Automating GAPP to monitor user access information to prevent Segregation of Duties (SoD) violations and sensitive access issues
- ✓ Specific security risks and data governance issues in PeopleSoft
- Business case (costs/benefits) for implementing CPM

# PeopleSoft Risks in Violating GAPP

## Human Capital Management System (HCM)

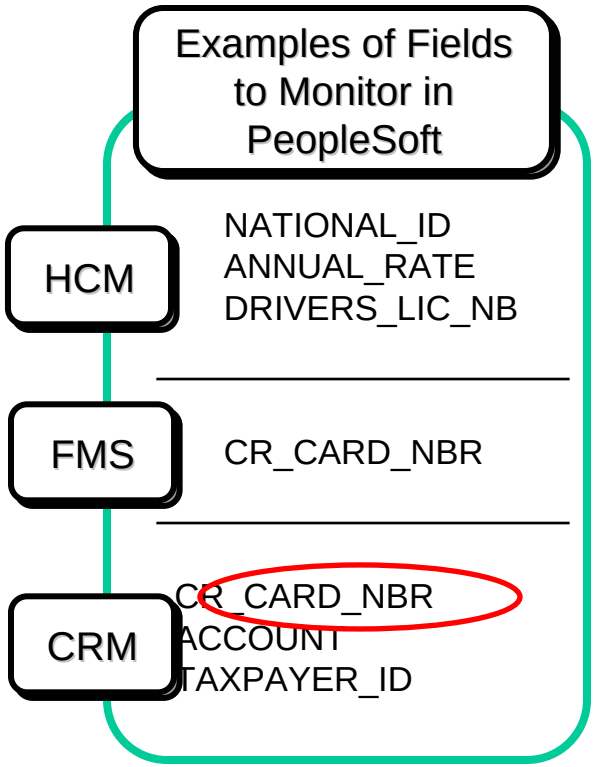
- Social security numbers, compensation, employee bank account numbers, benefits, 401(k), e-mail addresses, driver's license numbers, etc

## Financial Management System (FMS)

- Key financial transactions, credit card numbers of the organization and employees, etc

## Customer Relationship Management System (CRM)

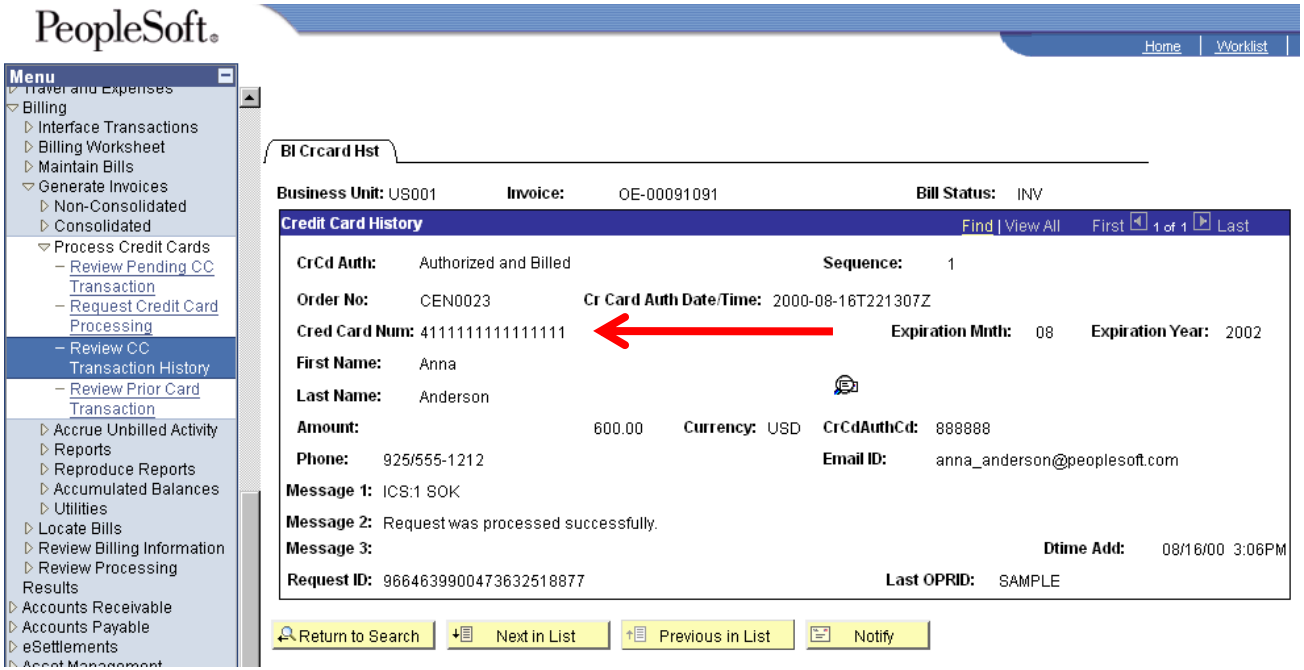
- Customer account numbers, credit card information, e-mail addresses, etc



# Access to "Review CC Transaction History"

PeopleSoft Financials/SCM 8.40.02.000

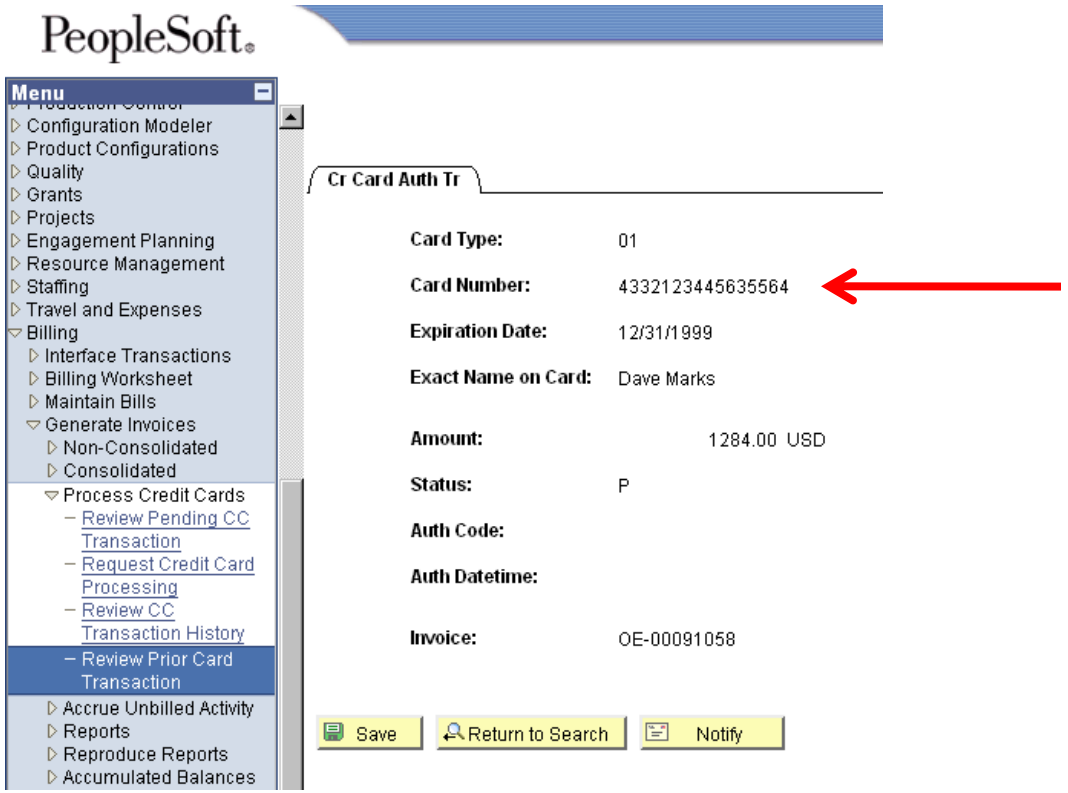
- Delivered application displays in clear text the Credit Card Number on the screen
- Approva monitors user access to the "Review CC Transaction History" page and ensure access is only granted to those who need it.



# Access to "Review Prior Card Transaction"

PeopleSoft Financials/SCM 8.40.02.000

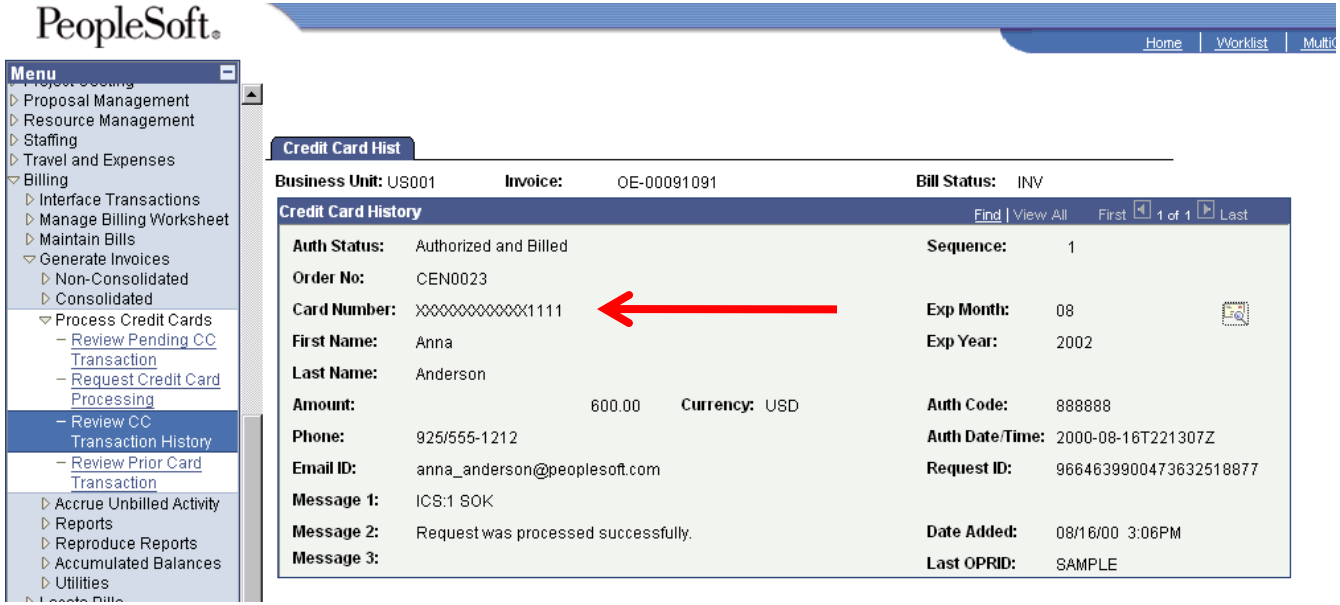
- Delivered application displays in clear text the Credit Card Number on the screen.
- Approva monitors user access to the "Review Prior Card Transaction" page and make sure access is only granted to those who absolutely need it.



# Even Newer Versions of PeopleSoft Aren't Fool Proof

PeopleSoft Financials/SCM 8.80.00.000

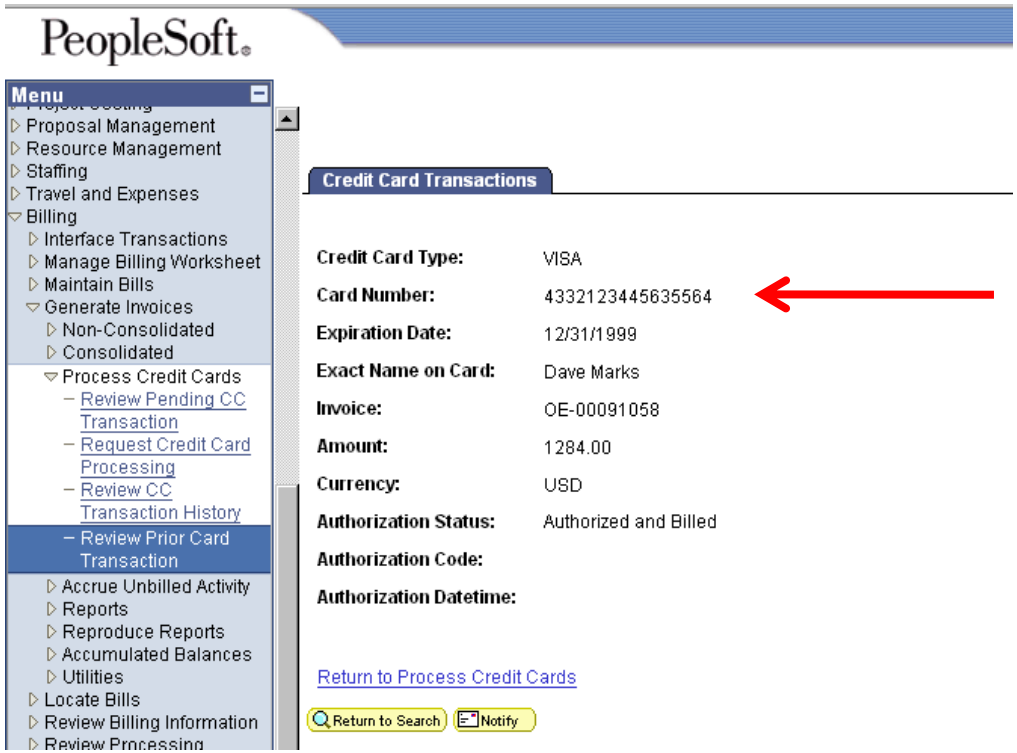
- Delivered application has begun to mask the field for greater security in some places but not all!
- Approva monitors all uses of sensitive fields such as CR_CARD_NBR to ensure appropriate access to all instances



# Data Masking is Inconsistent - Even in FMS 8.8

PeopleSoft Financials/SCM 8.80.00.000

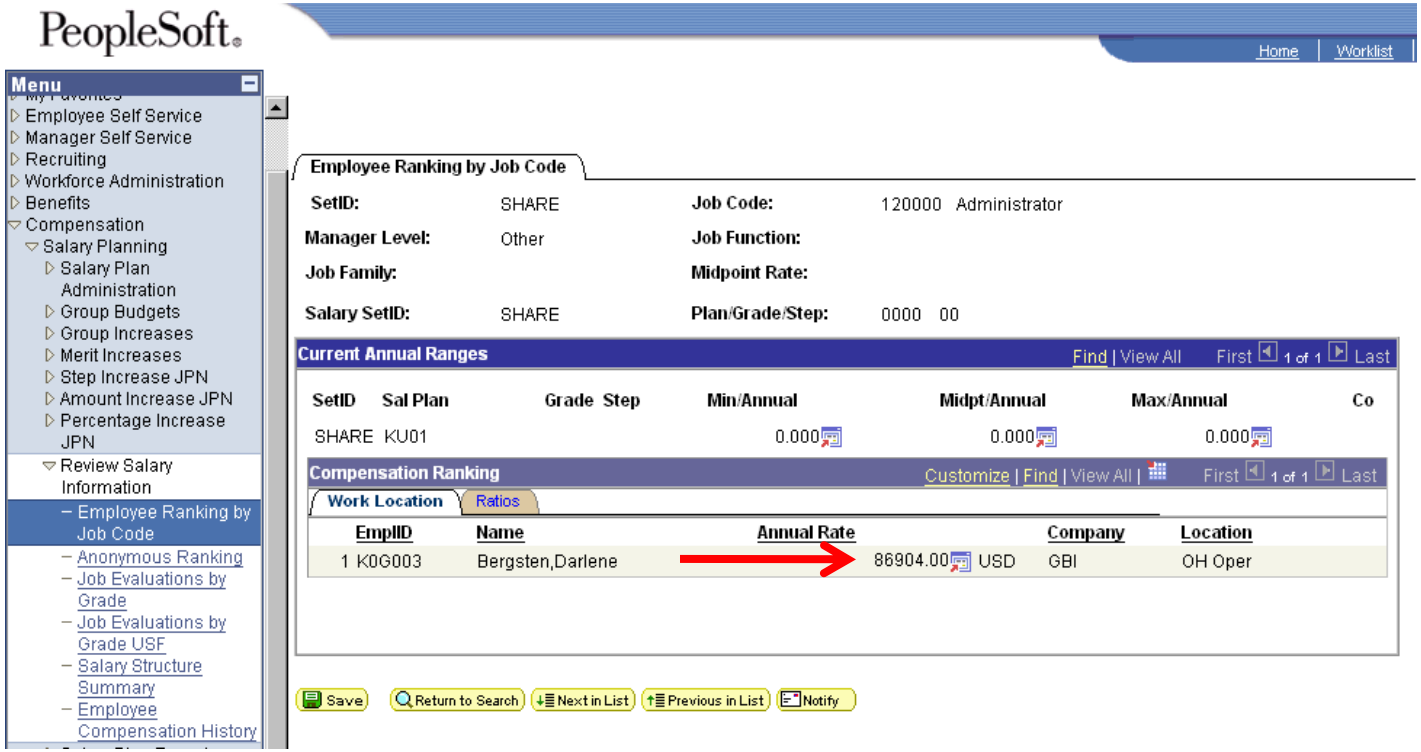
- Credit Card Number was not masked for security on the "Review Prior Card Transaction" page. The inconsistency in masking is a security risk.
- Approva monitors access to pages where masking has not been provided.



# Access to Employee Salaries

PeopleSoft HRMS 8.80.01.000

- Page displays employee Annual compensation
- Approva monitors user access to the "Employee Ranking by Job Code" page and make sure access is only granted to those who need it



# Where Approva Can Help

**Inadequate Masking / Encryption**

Approva identifies and monitors users who have access to PeopleSoft pages **where masking or encryption is not adequate**.

**Access to PeopleTools & PeopleSoft Query**

Approva monitors individuals who have access to **PeopleTools or PeopleSoft query** as these individuals have the ability to bypass the masking and or encryption with which PeopleSoft was delivered.

**Securing Sensitive Fields**

Approva **secures sensitive fields such as NATIONAL_ID, ANNUAL_RATE and CR_CARD_NBR by monitoring and reporting on pages where these fields occur**.

- PeopleSoft allows customizations but does not enforce that the masking\encryption delivered is replicated on newly created pages.
- Approva determines how many occurrences there are of a sensitive field in the system. It then monitors that number to ensure new instances have adequate protections of masking and encryption. This type of sensitive data rule is accomplished through the use of the Approva Insight Studio.

# Objectives

- ✓ Trends in data privacy and security breaches
- ✓ How Generally Accepted Privacy Principles (GAPP) are evolving to a meet a need for Continuous Privacy Monitoring (CPM)
- ✓ Automating GAPP to monitor user access information to prevent Segregation of Duties (SoD) violations and sensitive access issues
- ✓ Specific security risks and data governance issues in PeopleSoft
- ✓ Business case (costs/benefits) for implementing CPM

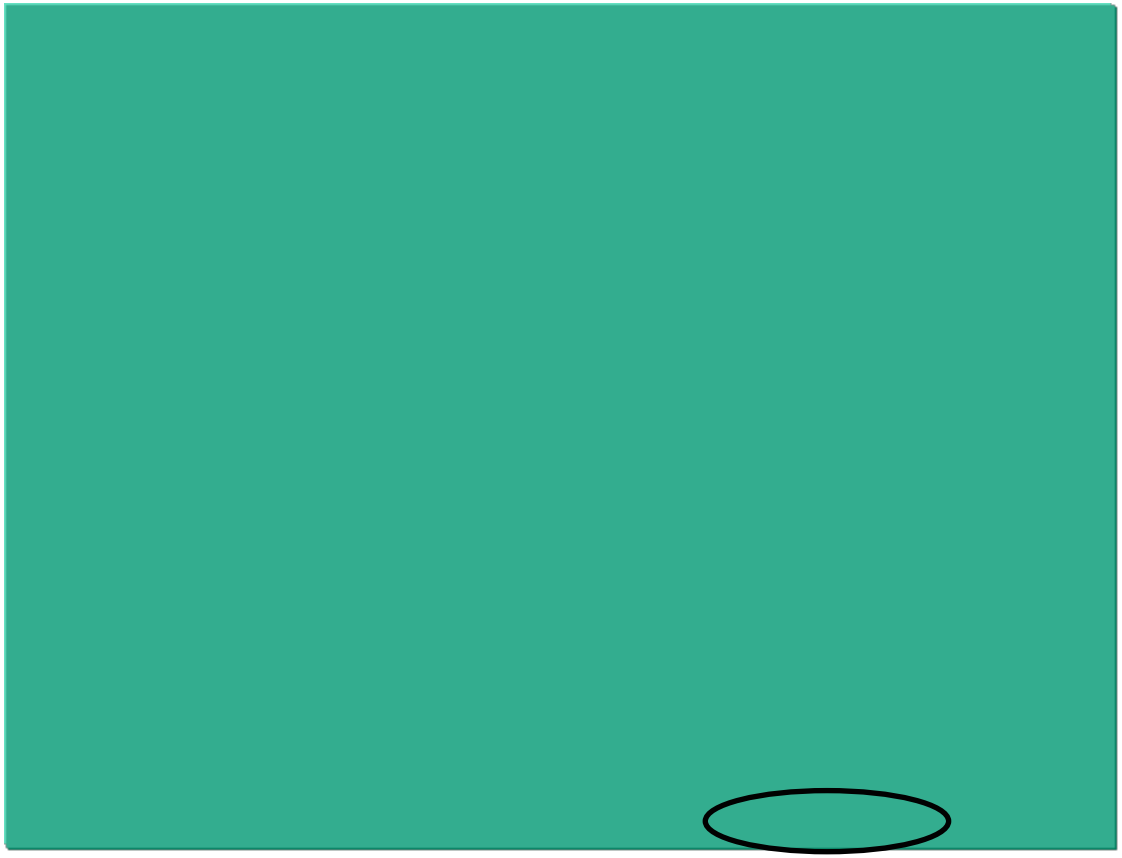
# Data Privacy Breaches are Pricey

**Avg. Cost of Breach $11.5MM**

- Darwin (insurance underwriters) created an **online calculator which estimates costs**

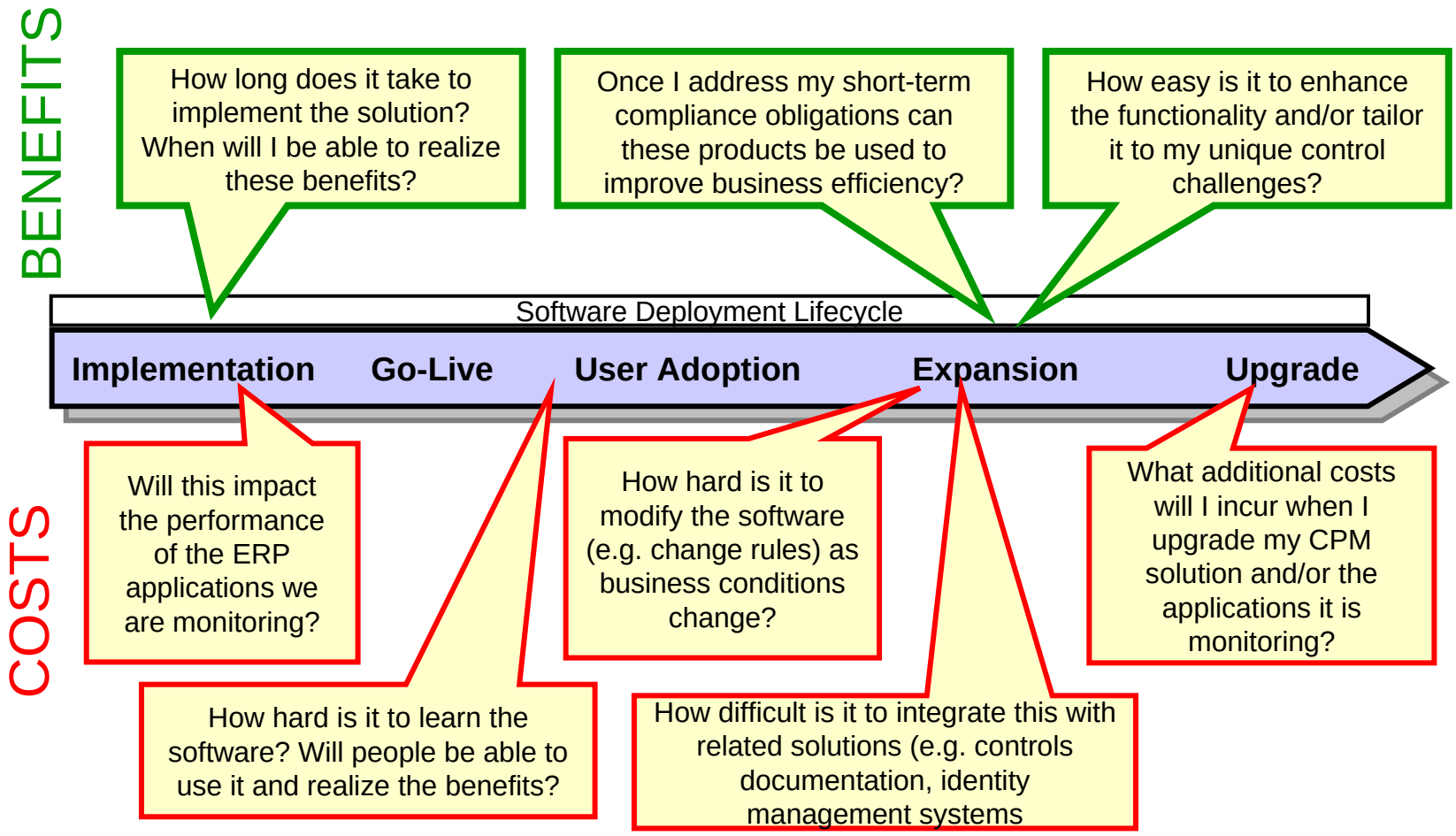
  http://www.tech-404.com/calculator.html

- The average number of records compromised in a data security breach is ~**99,000**, according to research by the Ponemon Institute.



*Calculator located at www.tech-404.com*

# CPM Solution Benefits and Costs



# Even Before a Breach, CPM Returns More Benefit Than Cost

| Key Cost Categories | Magnitude of Benefits | | | |
|---|---|---|---|---|
| | Year 1 | Year 2 | Year 3 | Total |
| Design & Configuration of Controls | $$ | N/A | N/A | $$ |
| Remediation of Access Violations | $$$ | N/A | N/A | $$$ |
| Ongoing & Continuous Privacy Monitoring | $ | $ | $ | $$$ |
| Internal & External Audit Costs for GAPP | $ | $ | $ | $$$ |
| Total | $$$$$ | $$ | $$ | $$$$$ |

# Are You Ready?

- "70% of all security incidents come from insiders"
- "80% of threats come from insiders and 65% go *undetected*"
- "An insider attack against a large company causes an average of $2.7MM in damages, where the average outside attack costs only $57,000… Almost 50 times as costly."

# Question & Answer

Marilyn Prosch, Ph.D., CIPP
Marilyn.Prosch@ASU.edu
(602) 543.6219

THUNDERBIRD SCHOOL OF GLOBAL MANAGEMENT
ASU ARIZONA STATE UNIVERSITY

Monica Nelmes Elliott
Monica.Elliott@Approva.net
(703) 956.8320

approva

# Appendix

# Additional Resources

- "Mind the GAPP: Accountants bring GAAP-like principles to the privacy sphere," Computerworld, December 2007 - http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9051459

- "ESI Year in Review - 2007," on information security incidents occurring at colleges and universities in 2007, February 10, 2008 - http://www.adamdodge.com/esi/yir_2007

- Industry breakdown of breaches in 2006 - http://www.privacyrights.org/ar/DataBreaches2006-Analysis.htm

- Online calculator to estimate cost of a data privacy breach - www.tech-404.com/calculator.html

# GAPP & Approva – #1 Management

| Reference | Management Criteria | Illustrations and Explanations of Criteria |
|---|---|---|
| 1.2.4 | **Infrastructure and Systems Management**<br><br>Internal personnel or advisers review the design, acquisition, development, implementation, configuration, and management of:<br>• Infrastructure<br>• Systems<br>• Applications<br>• Web sites<br>• Procedures<br><br>and changes thereto for consistency with the entity's privacy policies and procedures and address any inconsistencies. | Procedures are in place to:<br><br>• Govern the development, acquisition, implementation, and maintenance of information systems and the related technology used to collect, use, retain, disclose and destroy personal information.<br>• Ensure that the entity's business continuity management processes are consistent with its privacy policies and procedures.<br>• Classify the sensitivity of classes of data, and **determine the classes of users who should have access to each class of data. Users are assigned user-access profiles based on their need for access and their functional responsibilities as they relate to personal information.**<br>**• Assess planned changes to systems and procedures for their potential effect on privacy.**<br>**• Test changes to system components to minimize the risk of an adverse effect on the systems that process personal information.** All test data are anonymized.<br>**• Require the documentation and approval by the privacy officer, business unit manager and IT management before implementing the changes to systems and procedures that handle personal information**, including those that may affect security. Emergency changes may be documented and approved on an after-the-fact basis.<br><br>**The information technology (IT) department maintains a listing of all software and the respective level, version, and patches that have been applied.**<br><br>**Procedures exist to provide that only authorized, tested, and documented changes are made to the system.** |
| | **Changes in Business and Regulatory Environments**<br><br>For each jurisdiction in which the entity operates, the effect on **privacy of changes in the following factors is identified and addressed:**<br>• Business operations and processes<br>• People<br>• Technology<br>• Legal<br>• Contracts, including service level agreements | The entity has an ongoing process in place to monitor, assess, and address the effect on privacy of changes in:<br>• Business operations and processes<br>• People assigned responsibility for privacy and security matters<br>• Technology (prior to implementation)<br>• Legal and regulatory environments<br>• Contracts, including service level agreements with third parties (Changes that alter the privacy and |

# GAPP & Approva – #5 Use & Retention

| Reference | Management Criteria | Illustrations and Explanations of Criteria |
|---|---|---|
| 5.2.2 | **Retention of Personal Information**<br><br>Personal information is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise. Personal information no longer retained is disposed and destroyed of in a manner that prevents loss, misuse, or unauthorized access. | The entity:<br><br>• Documents its retention policies and disposal procedures.<br>• Erases or destroys records in accordance with the retention policies, regardless of the method of storage (for example, electronic or paper-based).<br>• Retains, stores, and disposes of archived and backup copies of records in accordance with its retention policies.<br>**• Ensures that personal information is not kept beyond the standard retention time unless there is a justified business reason for doing so.**<br>• Locates and removes specified personal information about an individual as required, for example, removing credit card numbers after the transaction is complete.<br>• Regularly and systematically destroys, erases, or makes anonymous personal information no longer required to fulfill the identified purposes or as required by laws and regulations.<br><br>Contractual requirements should be considered when establishing retention practices.<br><br>Some laws specify the retention period for personal information; for example, HIPAA has a six-year retention period from the date of creation or last in effect for personal information. There may be other statutory record retention requirements; for example, certain data may need to be retained for tax purposes or in accordance with employment laws. |

# GAPP & Approva – #6 Access

| Reference | Management Criteria | Illustrations and Explanations of Criteria |
|---|---|---|
| 6.2.1 | **Access by Individuals to Their Personal Information**<br><br>Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information. | Procedures are in place to:<br><br>• Determine whether the entity holds or controls personal information about an individual.<br>• Communicate the steps to be taken to gain access to the personal information.<br>• Respond to an individual's request on a timely basis.<br>• Provide a copy of personal information, upon request, in printed or electronic form that is convenient to both the individual and the entity.<br>**• Record requests for access, actions taken, including denial of access, and unresolved complaints and disputes.** |
| 6.2.5 | **Updating or Correcting Personal Information**<br><br>Individuals are able to update or correct personal information held by the entity. If practical and economically feasible to do so, the entity provides such updated or corrected information to third parties that previously were provided with the individual's personal information. | The entity:<br><br>• Describes the process an individual must follow to update or correct personal information records (for example, in writing, by phone, by e-mail, or by using the entity's Web site).<br>**• Verifies the accuracy and completeness of personal information that an individual updates or changes (for example, by edit and validation controls, and forced completion of mandatory fields).**<br>**• Records the date, time, and identification of the person making the change if the entity's employee is making a change on behalf of an individual.**<br>• Notifies third parties to whom personal information has been disclosed of amendments, erasures, or blocking of personal information, if it is possible and reasonable to do so. |

# GAPP & Approva – #7 Disclosure to 3rd Parties

| Reference | Management Criteria | Illustrations and Explanations of Criteria |
|---|---|---|
| 7.2.2 | **Protection of Personal Information with 3rd Parties**<br><br>Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy policies. | Systems and procedures are in place to:<br><br>• Provide a level of protection of personal information equivalent to that of the entity when information is provided to a third party (that is, by contract or agreement).<br>• Affirm that the level of protection of personal information by third parties is equivalent to that of the entity, for example, by obtaining assurance (for example, an auditor's report), contractual obligation, or other representation (for example, written annual confirmation).<br>**• Limit the third party's use of personal information to purposes necessary to fulfill the contract.**<br>• Communicate the individual's preferences to the third party.<br>• Refer any requests for access or complaints about the personal information transferred by the entity to a designated privacy executive, such as a corporate privacy officer.<br>• Specify how and when third parties are to dispose of or return any personal information provided by the entity. |

# GAPP & Approva – #8 Security for Privacy (1 of 3)

| Reference | Management Criteria | Illustrations and Explanations of Criteria |
|---|---|---|
| 8.2.1 | **Information Security Program**<br><br>A security program has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction. | The entity's security program addresses the following matters related to protection of personal information:<br><br>• **Periodic risk assessments**<br>• **Identification and documentation of the security requirements of authorized users**<br>• **Allowing access, the nature of that access, and who authorizes such access**<br>• **Preventing unauthorized access by using effective physical and logical access controls**<br>• **The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access**<br>• Assignment of responsibility and accountability for security<br>• Assignment of responsibility and accountability for system changes and maintenance<br>• **Implementing system software upgrades and patches**<br>• **Testing, evaluating, and authorizing system principles before implementation**<br>• Addressing how complaints and requests relating to security issues are resolved<br>• Handling errors and omissions, security breaches, and other incidents<br>• Procedures to detect actual and attempted attacks or intrusions into systems and to proactively test security procedures (for example, penetration testing)<br>• Allocating training and other resources to support its security policies<br>• Provision for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies<br>• Disaster recovery plans and related testing<br>• Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts<br>• A requirement that users, management, and third parties confirm (initially and annually) their understanding of and agreement to comply with the entity's privacy policies and procedures related to the security of personal information<br><br>**The entity's security program prevents access to personal information** in computers, media, and paper-based information that are no longer in active use by the organization (e.g., computers, media and paper-based information in storage, sold, or otherwise disposed of). |

# GAPP & Approva – #8 Security for Privacy (2 of 3)

| Reference | Management Criteria | Illustrations and Explanations of Criteria |
|---|---|---|
| 8.2.2 | **Logical Access Controls**<br><br>Logical access to personal information is restricted:<br>• Authorizing and registering internal personnel and individuals<br>• Identifying and authenticating internal personnel and individuals<br>• Making changes and updating access profiles<br>• Granting system access privileges and permissions<br>• Preventing individuals from accessing other than their own personal or sensitive information<br>• Limiting access to personal information to only authorized internal personnel based upon their assigned roles and responsibilities<br>• Distributing output only to authorized internal personnel<br>• Restricting logical access to offline storage, backup data, systems, and media<br>• Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)<br>• Preventing the introduction of viruses, malicious code, and unauthorized software | Systems and procedures are in place to:<br><br>**• Establish the level and nature of access that will be provided to users based on the sensitivity of the data and the user's legitimate business need to access the personal information.**<br>**• Authenticate users, for example, by user name and password, certificate, external token, or biometrics.**<br>**• Require the user to provide a valid ID and password to be authenticated by the system before access is granted to systems handling personal information.**<br>**• Require enhanced security measures for remote access, such as additional or dynamic passwords, dial-back controls, digital certificates, secure ID cards, virtual private network (VPN), or properly configured firewalls.**<br>• Implement intrusion detection and monitoring systems.<br><br>User authorization processes consider:<br><br>• How the data is accessed (internal or external network), as well as the media and technology platform of storage.<br>• Access to paper and backup media containing personal information.<br>• Denial of access to joint accounts without other methods to authenticate the actual individuals. |

# GAPP & Approva – #8 Security for Privacy (3 of 3)

| Reference | Management Criteria | Illustrations and Explanations of Criteria |
|---|---|---|
| 8.2.6 | **Testing Security Safeguards**<br><br>Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually. | Systems and procedures are in place to:<br>• **Regularly test the effectiveness of the key administrative, technical, and physical safeguards protecting personal information.**<br>• **Periodically undertake independent audits of security controls using either internal or external auditors.**<br>• Test card access systems and other physical security devices at least annually.<br>• Document and test disaster recovery and contingency plans at least annually to ensure their viability.<br>• Periodically undertake threat and vulnerability testing, including security penetration reviews and Web vulnerability and resilience.<br><br>The frequency and nature of the testing of security safeguards will vary with the entity's size and complexity, the nature and scope of its activities, and the sensitivity of personal information. Some security regulations (for example, GLBA-related rules for safeguarding information) require an entity to:<br>• **Conduct regular tests of key** controls, systems, and procedures by independent third parties or by staff independent of those that develop or maintain security (or at least have these independent parties review results of testing).<br>• Assess and possibly adjust its information security at least annually. |

# GAPP & Approva – #9 Quality

| Reference | Management Criteria | Illustrations and Explanations of Criteria |
|---|---|---|
| 9.2.1 | **Accuracy and Completeness of Personal Information**<br><br>Personal information is accurate and complete for the purposes for which it is to be used. | Systems and procedures are in place to:<br><br>• Edit and validate personal information as it is collected, created, maintained, and updated.<br>• Record the date when the personal information is obtained or updated.<br>• Specify when the personal information is no longer valid.<br>• Specify when and how the personal information is to be updated and the source for the update (for example, annual reconfirmation of information held and methods for individuals to proactively update personal information).<br>• Indicate how to verify the accuracy and completeness of personal information obtained directly from an individual, received from a third party (see 4.2.3, “Collection From Third Parties”), or disclosed to a third party (see 7.2.2, “Protection of Personal Information”).<br>• Ensure personal information used on an ongoing basis is sufficiently accurate and complete to make decisions, unless there are clear limits to the need for accuracy.<br>• Ensure personal information is not routinely updated, unless such a process is necessary to fulfill the purposes for which it is to be used.<br><br>The entity undertakes periodic assessments to check the accuracy of personal information records and to correct them, as necessary. |

# GAPP & Approva – #10 Monitoring & Enforcement

| Reference | Management Criteria | Illustrations and Explanations of Criteria |
|---|---|---|
| 10.2.3 | **Compliance Review**<br><br>Compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts is reviewed and documented and the results of such reviews are reported to management. If problems are identified, the entity's privacy policies and procedures are enforced. | Systems and procedures are in place to:<br><br>• Annually review compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts.<br>**• Document periodic reviews, for example, internal audit plans, audit reports, compliance checklists, and management sign-off, are maintained.**<br>**• Report the results of the compliance review and recommendations for improvement to management, and implement a remediation plan.**<br>**• Monitor the resolution of issues and vulnerabilities noted in the compliance review to ensure that appropriate corrective action is taken on a timely basis (that is, privacy policies and procedures are revised, as necessary).** |
| 10.2.4 | **Instances of Noncompliance**<br><br>Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective measures are taken on a timely basis. | Systems and procedures are in place to:<br><br>• Notify employees of the need to report privacy breaches and security vulnerabilities in a timely manner.<br>• Inform employees of the appropriate channels to report security vulnerabilities and privacy breaches.<br>**• Document instances of noncompliance with privacy policies and procedures.**<br>• Monitor the resolution of security vulnerabilities and privacy breaches to ensure appropriate corrective measures are taken on a timely basis.<br>• Mitigates, to the extent practicable, any harm caused by the use or disclosure of personal information by the third party in violation of the entity's privacy policies and procedures (for example, notify individuals affected, attempt to recover information disclosed to others, void and reissue new account numbers).<br>• Identify trends that may require revisions to privacy policies and procedures. |