INTEGRIGY

PeopleSoft - Top 10 Security Risks

December 6, 2018

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy

ERP Applications
Oracle E-Business Suite, PeopleSoft, Oracle Retail

INTEGRIGY

Databases
Oracle, Microsoft SQL Server, DB2, Sybase, MySQL

Products

AppSentry
ERP Application and Database Security Auditing Tool

Validates Security

AppDefend
Enterprise Application Firewall for the Oracle E-Business Suite and Oracle PeopleSoft

Protects Oracle EBS & PeopleSoft

Services

Verify Security

Security Assessments
ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance
SOX, PCI, HIPAA, GLBA

Build Security

Security Design Services
Auditing, Encryption, DMZ

Integrigy Research Team
ERP Application and Database Security Research

Top 10 PeopleSoft Security Risks

How was the list of Top 10 security risks developed?

- From Integrigy's on-site and remote security assessments of large PeopleSoft environment over the past 2 years
- From the Integrigy Research Team's in-depth analysis of the entire PeopleSoft technology stack including application, PeopleTools, database, web server, and application server

What is the selection criteria for the Top 10 security risks in a PeopleSoft Environment?

- What can be pragmatically addressed or should be discussed
- Risk of PeopleSoft sensitive data loss or information disclosure

Top 10 Security Vulnerabilities

1. Default Database Passwords
2. Connect ID with default password
3. No security patching
4. Direct database access by users
5. External deployment and WebLogic
6. SSL/TLS not configured
7. PPM configured but not used
8. Tuxedo network access
9. No Database or Application Auditing
10. Sensitive data not encrypted at rest

Significant Security Risks and Threats

Risks and Threats ▪ examples	**1** DB Pass	**2** Connect ID Passwd	**3** Security Patches	**4** Direct DB Access	**5** External Weblogic	**6** No SSL/TLS	**7** PPM Config	**8** Tuxedo Net Access	**9** No db-app Audit	**10** Sensitive Data Encrypt
1. Sensitive data loss (data theft) ▪ Bulk download via direct access ▪ Bulk download via indirect access	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🔴
2. Direct entering of transactions (fraud) ▪ Update a bank account number ▪ Change an application password	🔴		🔴	🔴					🟡	
3. Misuse of application privileges (fraud) ▪ Bypass intended app controls ▪ Access another user's privileges			🔴	🔴		🔴		🔴	🟡	
4. Impact availability of the application ▪ Wipe out the database ▪ Denial of service (DoS)	🔴	🟡	🔴	🔴	🔴		🟡	🟡		

1 Default Database Passwords

- **PeopleSoft Oracle database has a number of database accounts –**
  - Usually between 20 and 75 database accounts
  - Standard Oracle (7 to 24) – SYS, SYSTEM, DBSNMP, …
  - PeopleSoft – SYSADM, PS, PEOPLE
  - Interfaces and integrations
  - Named users
- **Accounts are often created with default or weak passwords**
  - Standard Oracle accounts (DBSNMP, CTXSYS, etc.) until 12c created with default passwords by default
  - Named users frequently assigned passwords like WELCOME1

1 Default Database Passwords Risk

- **Risk of a database account with a default password is based on how well-known the account is –**
  1. Standard Oracle Database accounts (DBSNMP, etc.)
  2. PeopleSoft standard account names (SYSADM, PS, etc.)
  3. Third-party software (OEM, Vertex, etc.)
  4. Custom database accounts (organizational specific)

- **An attacker will –**
  - Scan the internal network for Oracle Databases
  - Use tools like nmap to test for default passwords
  - Most tools have between 250 to 1,500 known Oracle database accounts and passwords

Default Oracle Password Statistics

Database Account	Default Password	Exists in Database %	Default Password %
SYS	CHANGE_ON_INSTALL	100%	3%
SYSTEM	MANAGER	100%	4%
DBSNMP	**DBSNMP**	**99%**	**52%**
OUTLN	**OUTLN**	**98%**	**43%**
MDSYS	MDSYS	77%	18%
ORDPLUGINS	ORDPLUGINS	77%	16%
ORDSYS	ORDSYS	77%	16%
XDB	CHANGE_ON_INSTALL	75%	15%
DIP	DIP	63%	19%
WMSYS	WMSYS	63%	12%
CTXSYS	**CTXSYS**	**54%**	**32%**

* Sample of 120 production databases

How to Check Database Passwords

1. **Use Oracle's DBA_USERS_WITH_DEFPWD**
   - Limited set of accounts
   - Single password for each account
2. **Command line tools (orabf, etc.)**
   - Difficult to run – command line only
3. **AppSentry**
   - Checks all database accounts
   - Uses passwords lists - > 1 million passwords
   - Allows custom passwords

2 Connect ID with default password

- **Most PeopleSoft environments use the standard Connect ID name of PEOPLE and the default password of "peop1e"**
- **PEOPLE has only limited privileges –**
  - System privileges = CREATE SESSION
  - Table privileges = SELECT on PSDBOWNER, PSACCESSPRFL, PSOPRDEFN, and PSSTATUS
  - Periodically verify no other privileges have been granted
- **When Oracle Database Critical Patch Update security patches are not applied, any database account can potentially compromise the entire database due to vulnerabilities in PUBLIC packages**

3 No Security Patching

Oracle PeopleSoft security vulnerabilities fixed between January 2005 and October 2018

458

PeopleSoft and Critical Patch Updates

PeopleSoft	▪ Patches are per application (FS, HCM, CS, ELM)
PeopleTools	▪ Point upgrades
Oracle Database	▪ Patch Set Updates – see quarterly MOS note
Tuxedo	▪ Rolling Patches
WebLogic	▪ Patch Set Updates – see MOS ID 1470197.1
Java	▪ Point upgrades

Supported Database Versions and CPUs

		PeopleTools					
		8.55	8.54	8.53	8.52	8.51	8.5
Database	12.1.0.2	✓	✓	✓	✓		
	12.1.0.1 (7/2016)		✓	✓	✓		
	11.2.0.4 (10/2020)	✓	✓	✓	✓	✓	✓
	11.2.0.3			✓	✓	✓	✓
	11.2.0.2					✓	✓
	11.1.0.7			✓	✓	✓	✓
	10.2.0.5			✓	✓	✓	✓

Do you need to apply both application and database CPUs? **Yes**

Is database security more than just applying CPUs? **Yes**

PeopleSoft and Critical Patch Updates

- **Apply Oracle Critical Patch Updates on a regular basis on all databases**
  - Reduce risk of compromise and escalation of privileges
- **October 2014 PeopleTools CPU must be applied**
  - Connect ID used to authenticate users has access to the table PSACCESSPRFL
  - Script to decrypt to Access ID password freely available on Internet
  - CPU changes encryption: 8.52.24, 8.53.17, 8.54.04

4 Direct Database Access by Users

- **Database access is a key problem**
  - Look for accounts like PS_RO, HR_READ, etc.
  - Read only accounts often created with read to all data
- **Access to sensitive data by generic accounts**
  - Granularity of database privileges (SELECT ANY TABLE vs. direct table grants)
  - Complexity of data model – 1,000's of tables
  - Number of tables/views and continuous development make it difficult to create limited privilege database accounts
  - Must use individual database accounts with roles limiting access to data along with other security

How to Review Direct Database Access

1. **Need to review who is accessing the database**
   - Must have auditing enabled to determine generic database access
   - **Oracle 12c Privilege Analysis feature now included with Enterprise Edition instead of with Database Vault**
2. **Difficult and time-consuming to review database privileges**
   - Must manually review database privileges
   - Need to understand data model, customizations, and interfaces to know what can be accessed and why with granted privileges

Integrigy #1 Security Recommendation

- **Limit direct database access whenever possible**
  - Much harder to hack database if attacker can not connect
- **Use firewalls in front of data center, network ACLs, TNS invited nodes, Oracle Connection Manager, Oracle Database Firewall, etc.**
  - DBAs should use bastion hosts to manage databases

5 External Deployment and WebLogic

Good = WebLogic is very feature rich

Bad = WebLogic is very feature rich

- **WebLogic includes many unused and unnecessary enabled by default features**
- **When deploying externally, these URLs are fully accessible unless you block them**
- **Examples –**
  - /IMServlet, /RP, /_async, /xmllink, /wls-wsat, /console, /consolehelp, bea_wls_internal, etc.

5 External Deployment and WebLogic

- **When deploying externally, only allow the minimum necessary URLs**
  - Set a whitelist in the load balancer or reverse proxy
  - Minimum set would be something like /ps/*, /psp/*, /psc/*
- **Periodically test URLs such as the following –**
  - /monitor/<site>
  - /console
  - /wls-wsat/CoordinatorPortType
- **For example vulnerability, search for CVE-2017-10271**
  - Additional vulnerabilities will be found in the future

6 SSL/TLS not configured

- **SSL/TLS encrypt network traffic between the end-user browser and the PeopleSoft web server**
  - When http:// is used, all traffic is sent across the network in clear text including passwords and sensitive data
- **SSL/TLS is not enabled by default in a PeopleSoft environment**
- **Recommended not to enable SSL/TLS on the PeopleSoft web server rather use the load balancer or reverse proxy as the SSL termination point**
  - Load balancer will have a more robust TLS stack and centralized administration of certificates

6 SSL/TLS not configured

- **See the PeopleTools documentation for enabling TLS**
- **Only TLS 1.2 should be used due to issues in older versions of the protocol**
  - Disable SSLv3, TLS 1.0, and TLS 1.1
  - See MOS Note ID 664126.1 “E-SSL: Configuring Peoplesoft to Use a Specific SSL/TLS Protocol within WebLogic”
- **Review the enabled ciphers and remove old or weak ciphers**
- **If deployed externally, use a site like ssllabs.com to verify the SSL/TLS configuration**

7 PPM configured but not used

- **PeopleSoft Performance Monitor (PPM) is used to identify performance issues and analyze performance trends in the application**
- **PPM Servlet (/monitor) patched for a Java deserialization vulnerability in October 2017**
  - Other security bugs and issues exist in PPM
- **Most PeopleSoft environments do not actively use PPM but have it enabled in production**
  - Often also enabled in externally accessible environments

7 PPM configured but not used

- **Disable PPM if you are not actively using it**
  - See MOS Note ID 622778.1 “E-PerfMon: How to Completely Disable PPM on Monitored System”
  - When disabled, you will see “The Monitor Console is disabled.
  - Please contact admin to enable PPMconsole.” when accessing http://<host>:<port>/monitor/<site>
- **Block the PPM monitor URL /monitor/* at the load balancer or reverse proxy**

8 Tuxedo network access

- **Tuxedo provides network connectivity through two services**
  - Java Service Listener (JSL)
  - Workstation Service Listener (WSL)
- **Five critical security vulnerabilities, collectively referred to as "JOLTandBleed", were patched in November 2017 for the Tuxedo JOLT server (JSL and JSH)**

1. **Enable Domain Connection Password to limit connections to JSL**
2. **Disable WSL in production when not needed**
3. **Enable encryption on JSL to protect data in transit – set JSL Encryption parameter in psappsrv.cfg file**

JOLT Listener

- Enabled Domain Connection Password on the JOLT listener to limit connections to only authorized servers (PIA) and effectively block the JOLTandBleed vulnerability.

- On the application server, run psadmin.
- Select the Application Server and continue to the Administer menu.
- Select Configure this Domain (option 4). You will be asked to shutdown the domain.
- Select Custom configuration (option # will depend on PeopleTools version, usually 14 or 15).
- Continue to the Security section and select y to change a value.
- For DomainConnectionPWD, enter a password (< 8.53 = 8 characters, > 8.53 = 8 to 30 characters) and press enter.
- When asked to encrypt password, < 8.53 enter no and > 8.53 enter yes.
- Enter q to quit and return to restart the domain.

WSL – Disable in Production

- **Workstation Service Listener often not used in production and can be disabled when not needed to reduce application attack surface.**

  - On each application server, run psadmin.
  - Select the Application Server and continue to the Administer menu.
  - Select Configure this Domain (option 4). You will be asked to shutdown the domain.
  - Under Features, the feature WSL should be set to No.
  - Enter q to quit and return.
  - Restart the domain for the change to take effect.

9 No Database or Application Auditing

- **The Oracle database and PeopleSoft offer rich log and audit functionality**
  - **Most organizations do not fully take advantage**
- **Requirements are difficult**
  - Technical, Compliance, Audit, and Security
- **Integrigy has a framework**
  - Already mapped to PCI, HIPAA, SOX and 21 CFR 11

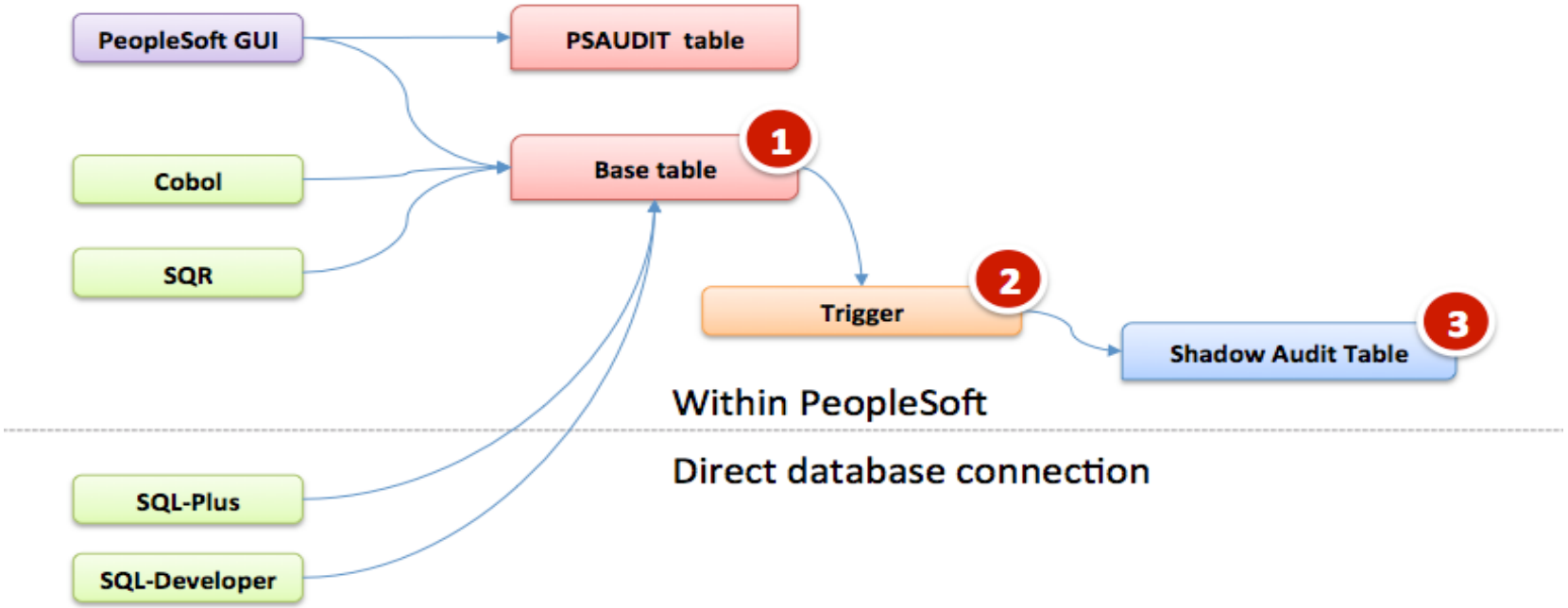
Logging and Auditing Is The Key

- **Access management success or failure largely based on logging and auditing**
  - No other way

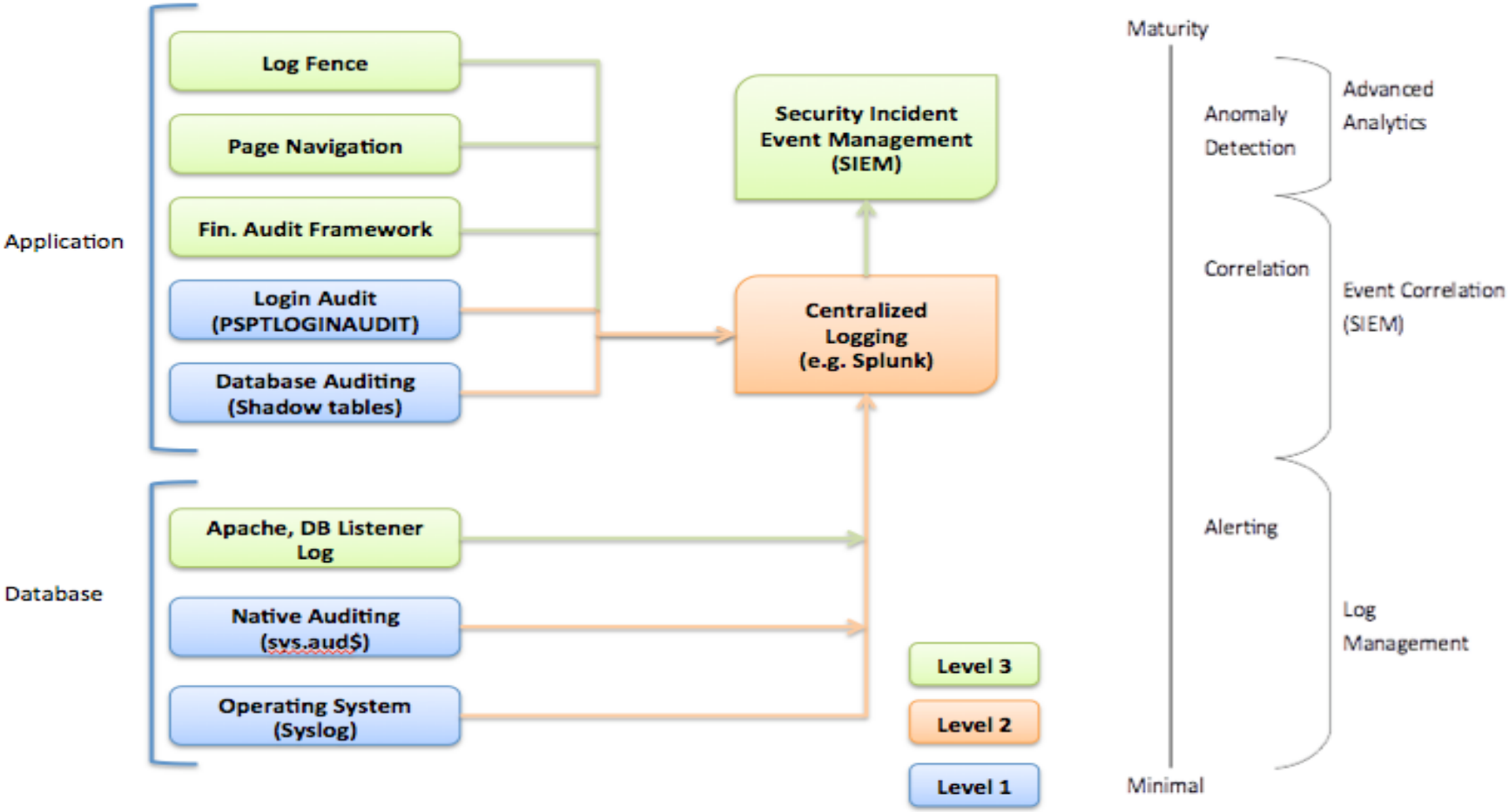
- **Constantly log activity**
  - Focus on key events
  - Audit with reports
  - Alert in real-time

Use Database Auditing

Field auditing only audits GUI and cannot audit PeopleTools activity

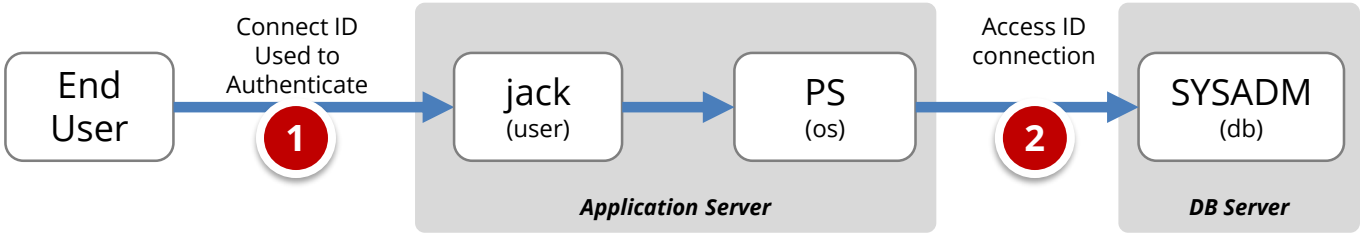


PeopleSoft Audit Framework Roadmap



Application End User Tracking – Solution

EnableDBMonitoring allows database auditing to capture web application end-users and correlate the application end-user to SQL statements.



Use CLIENT_INFO for DAM solutions (e.g. Splunk)					
DB User	OS User	Client IP	Program	SQL	Application User
SYSADM	PS	192.168.1.11	PSAPPSRV.exe	select * from ps_person	jack

select sid,serial#,username, program, module, client_info from v$session

Sensitive data not encrypted at rest

- Storage (Data at rest)
  - **Disk, storage, media level encryption**
  - Encryption of data at rest such as when stored in files or on media
- Access (Data in use)*
  - **Application or database level encryption**
  - Encryption of data with access permitted only to a subset of users in order to enforce segregation of duties
- Network (Data in motion)
  - **Encryption of data when transferred between two systems**
  - SQL*Net encryption (database)

Misconceptions about Database Storage Encryption

- **Not an access control tool**
  - Encryption does not solve access control problems
  - Data is encrypted the same <u>regardless</u> of user
  - Coarse-grained file access control only
- **No malicious employee protection**
  - Encryption does not protect against malicious privileged employees and contractors
  - DBAs have full access
- **Key management determines success**
  - Access to Oracle wallets (TDE) controls everything
  - You and only you can should control the keys
- **More is not better**
  - Performance cost of encryption
  - Cannot encrypt everything

PeopleTools Application Encryption

- **Encrypt, decrypt, sign, and verify fields in a database or external files**
  - Obtain library (e.g. PGP). Open source OpenSSL provided.
  - Develop API glue code to library (if not OpenSSL or PGP)
  - Write PeopleCode to invoke
- **Note full table encryption (PTENCRYPTPET/PTDECRYPTPET) " is not intended for widespread usage"**
  - Used to encrypt encryption keys (DOC ID 1382024.1)
- **PeopleTools Application Designer option for field "column" level encryption with Oracle TDE**

http://docs.oracle.com/cd/E66686_01/pt855pbr0/eng/pt/tsec/concept_UnderstandingPeopleSoftEncryptionTechnology-c07784.html

What is Oracle TDE?

- **<u>Transparent</u> database encryption**
  - Requires no application code or database structure changes to implement
  - Only major change to database function is the Oracle Wallet must be opened during database startup
  - Add-on feature licensed with Advanced Security Option
- **Column or Full Tablespace**
- **Column encryption restrictions (not Tablespace)**
  - Cannot be a foreign key or used in database constraint
  - Only simple data types like number, varchar, date, …
  - Less than 3,932 bytes in length

What does TDE do and not do?

- **TDE only encrypts "data at rest"**
- **TDE protects data if following is stolen or lost -**
  - disk drive
  - database file
  - backup tape of the database files
- **An authenticated database user sees no change**
- **Does TDE meet legal requirements for encryption?**
  - California SB1386, Payment Card Industry Data Security
  - Ask your legal department

PeopleSoft Oracle TDE Support

- **Supports both Column and Tablespace Encryption**
  - Column 'field' encryption supported from Application Designer (e.g. Social Security Number field is tagged for encryption)
  - No changes required for Tablespace encryption
- **Certifications**
  - PeopleTools release 8.46 and higher on Oracle 10gR2 and higher can use TDE column encryption
  - PeopleTools release 8.48 and higher on Oracle 11g and higher can use TDE tablespace encryption
- **More information –**
  - http://www.oracle.com/technetwork/database/security/rp-tse-ptools-8-134112.pdf

Contact Information

Stephen Kost

Chief Technology Officer

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

blog: **integrigy.com/oracle-security-blog**

youtube: **youtube.com/integrigy**