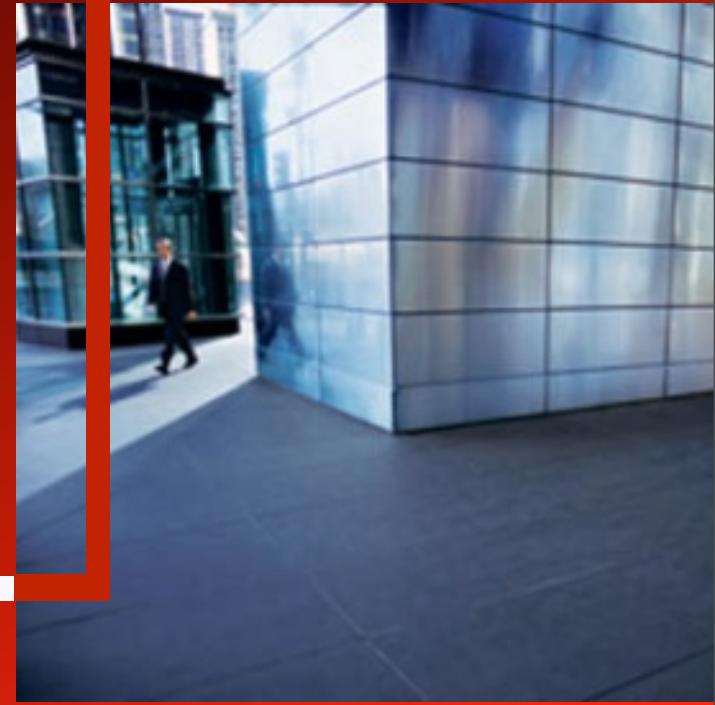


Security



ORACLE®

ORACLE



ORACLE

Oracle Hacker Days Zagreb 26.01.2010



Peter Kestner
Technology Director - Database Security
Oracle Core Technology EMEA



ORACLE®

Oracle Day 2009

Where Experience
Meets Innovation

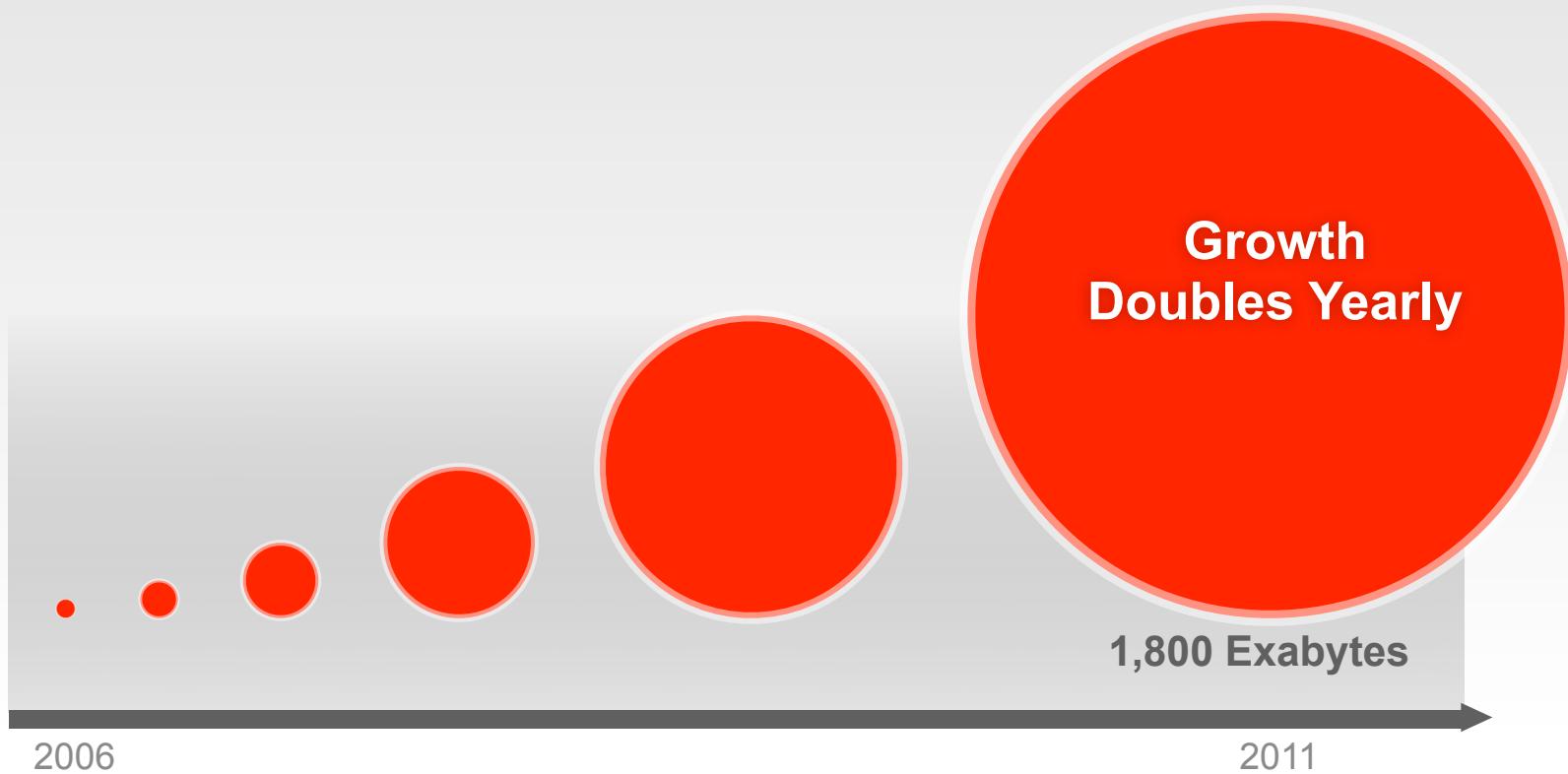


ORACLE® Security

Peter Kestner

Technology Director – Database Security
Oracle Core Technology EMEA

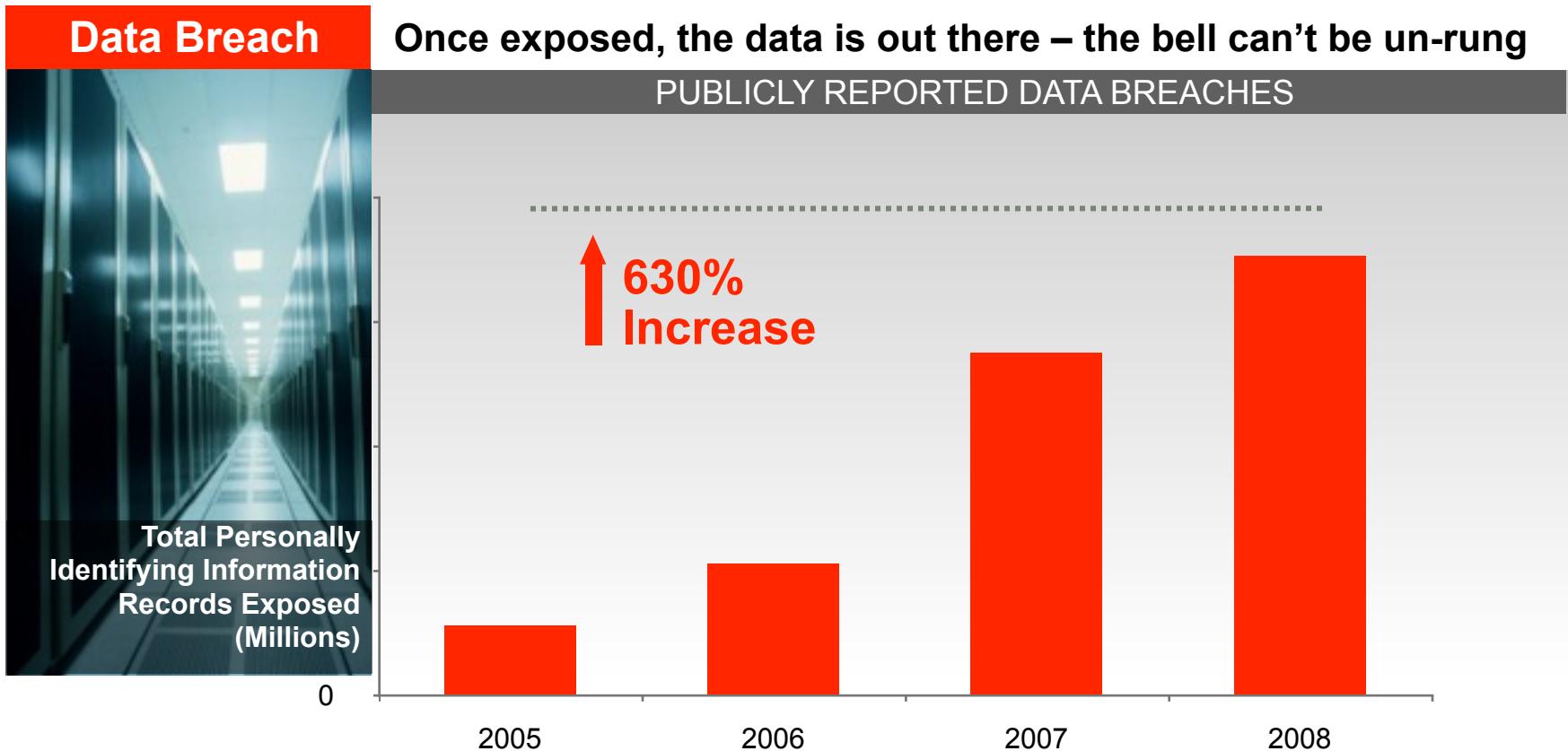
More data than ever...



Source: IDC, 2008

ORACLE®

More breaches then ever...



Source: DataLossDB, 2009

ORACLE®

More threats than ever...



The screenshot shows the homepage of CyberInsecure.com. The header features the site's name in large white letters on a blue background, with the subtitle "Daily Cyber Threats And Internet Security News Alerts" below it. The navigation bar includes links for HOME, ARCHIVES, CONTACT, ABOUT, EMAIL SUBSCRIBE, and ADVERTISE. A news item from August 5th, 2008, is displayed, titled "Countrywide Financial Insider Steals And Sells Thousands Of Private Customer Records". The text describes how the FBI arrested a former employee and another man for stealing sensitive personal information from 2 million mortgage applicants over a two-year period.

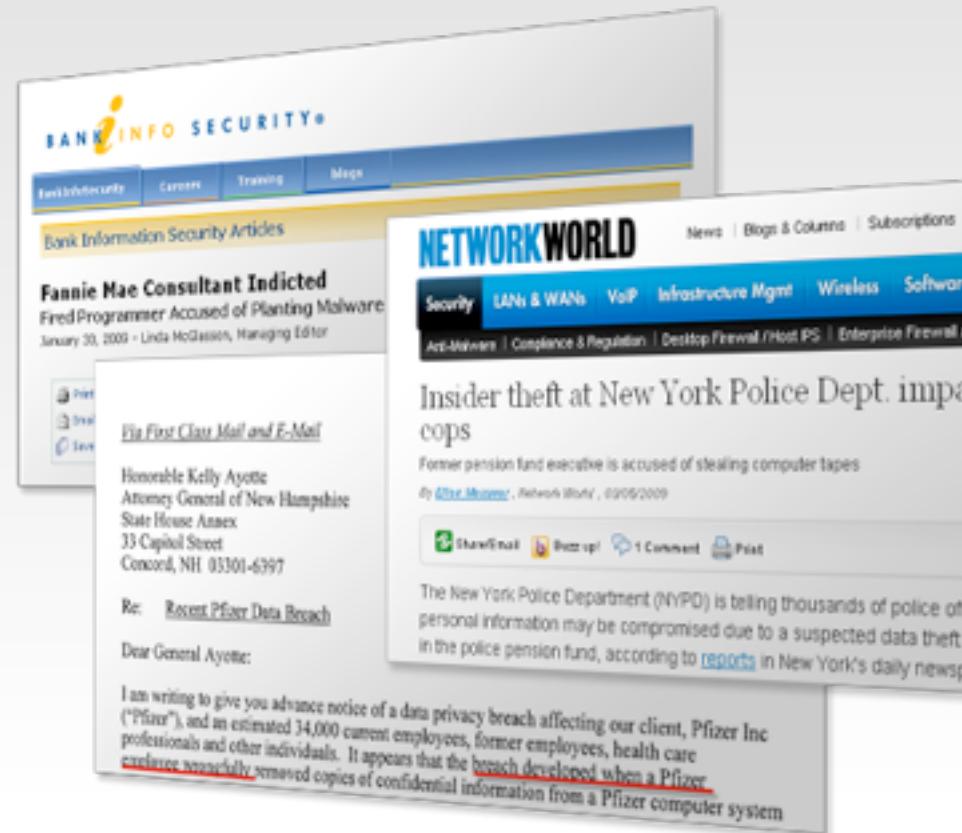
CyberInsecure.com
Daily Cyber Threats And Internet Security News Alerts

HOME ARCHIVES CONTACT ABOUT EMAIL SUBSCRIBE ADVERTISE

August 5th, 2008

Countrywide Financial Insider Steals And Sells Thousands Of Private Customer Records

The FBI on Friday arrested a former Countrywide Financial Corp. employee and another man in an alleged scheme to steal and sell sensitive personal information, including Social Security numbers, of as many as 2 million mortgage applicants. The breach in security, which occurred over a two-year



The screenshot displays two news articles. On the left, from BankInfoSecurity.com, is an article about a Fannie Mae consultant being indicted for planting malware. On the right, from NetworkWorld, is an article about insider theft at the New York Police Department. Both articles include social media sharing options and a comment section.

BANKINFOSECURITY

Bank Information Security Articles

Fannie Mae Consultant Indicted
Fred Programmer Accused of Planting Malware
January 30, 2009 - Linda McGlasson, Managing Editor

Pfizer Data Breach

Pfizer First Class Mail and E-Mail

Honorable Kelly Ayotte
Attorney General of New Hampshire
State House Annex
33 Capitol Street
Concord, NH 03301-6397

Re: Recent Pfizer Data Breach

Dear General Ayotte:

I am writing to give you advance notice of a data privacy breach affecting our client, Pfizer Inc ("Pfizer"), and an estimated 34,000 current employees, former employees, health care professionals and other individuals. It appears that the breach developed when a Pfizer executive ~~successfully~~ removed copies of confidential information from a Pfizer computer system

NETWORKWORLD

News | Blogs & Columns | Subscriptions

Security LANs & WANs VoIP Infrastructure Mgmt Wireless Software

Anti-Viruses | Compliance & Regulation | Desktop Firewall / Host IPS | Enterprise Firewall

Insider theft at New York Police Dept. impacts cops

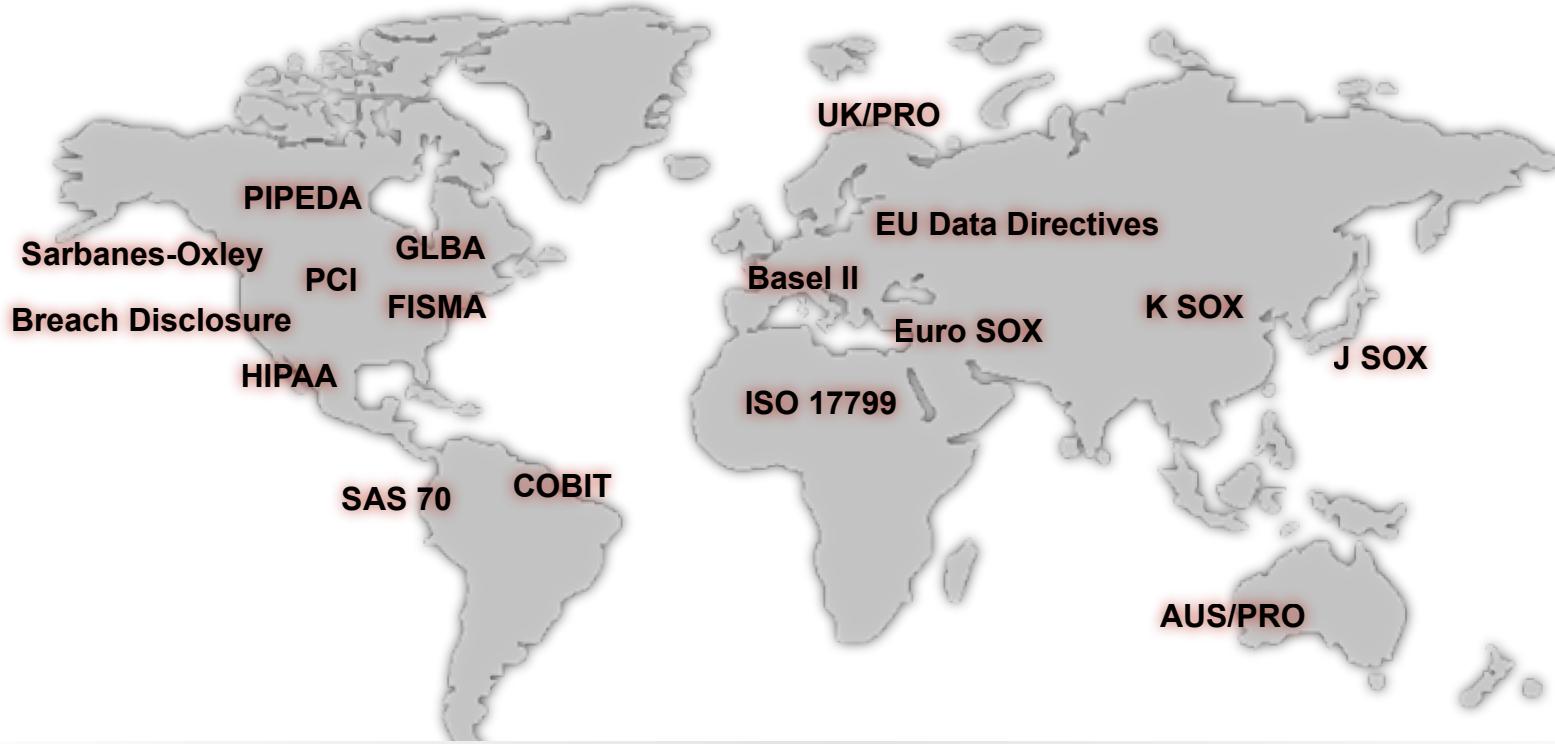
Former pension fund executive is accused of stealing computer tapes
By [Aliza Moore](#), Network World, 03/05/2009

ShareEmail Buzz up! 1 Comment Print

The New York Police Department (NYPD) is telling thousands of police officers that personal information may be compromised due to a suspected data theft in the police pension fund, according to [report](#) in New York's daily news

ORACLE®

More Regulations Than Ever...



90% Companies behind in compliance

Source: IT Policy Compliance Group, 2009.

Market Overview: IT Security In 2009



FORRESTER®

There has been a clear and significant shift from what was the widely recognized state of security just a few years ago.

Protecting the organization's information assets is the top issue facing security programs: data security (90%) is most often cited as an important or very important issue for IT security organizations, followed by application security (86%).

The Myth of Hacking Oracle



Oracle Day 2009
Where Experience
Meets Innovation

- WHERE
- WHO
- HOW
- PROTECTION

ORACLE®

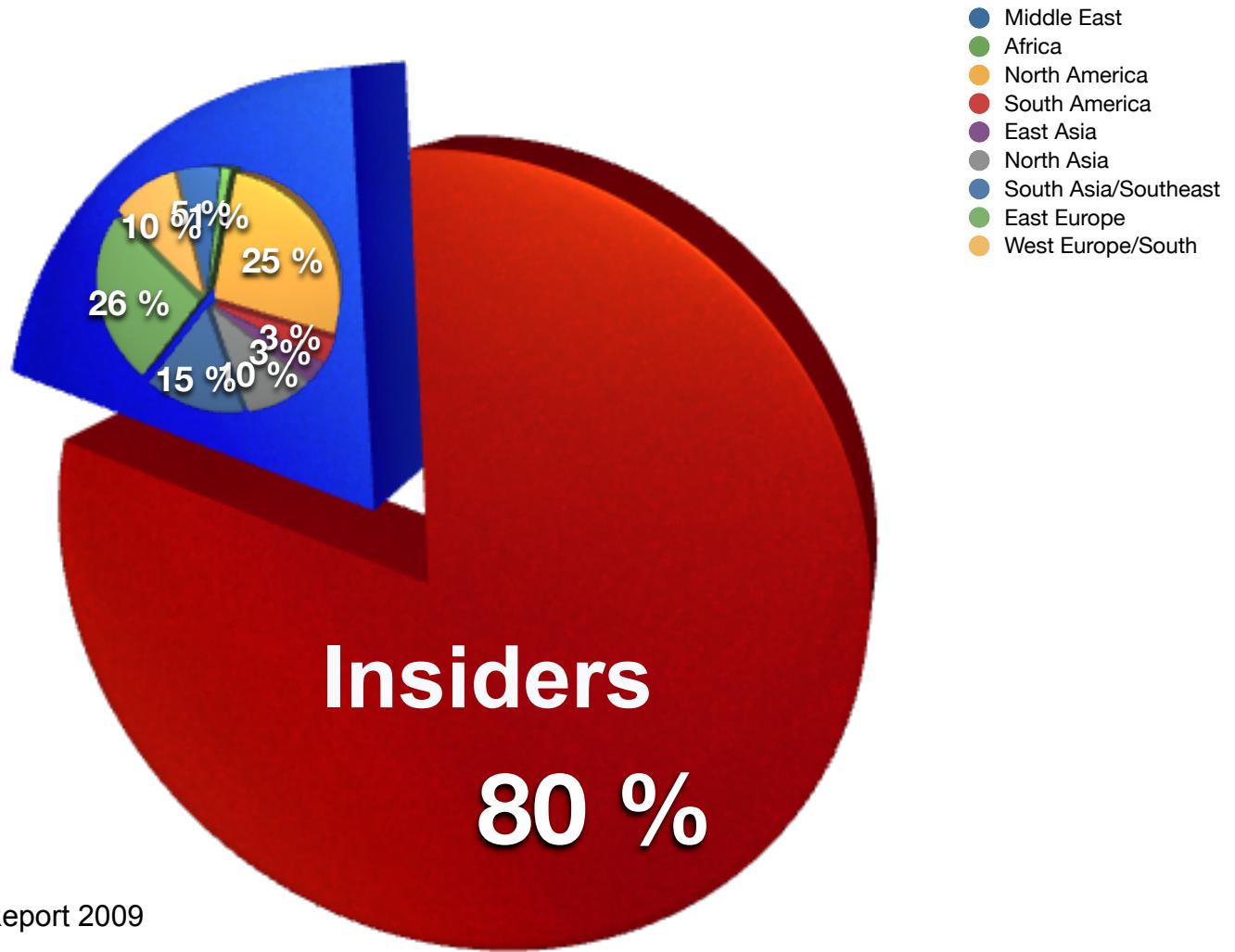
Where does the attacks come from ?

WHERE

WHO

HOW

PROTECTION



Source: Verizon Data Breach Report 2009

ORACLE®

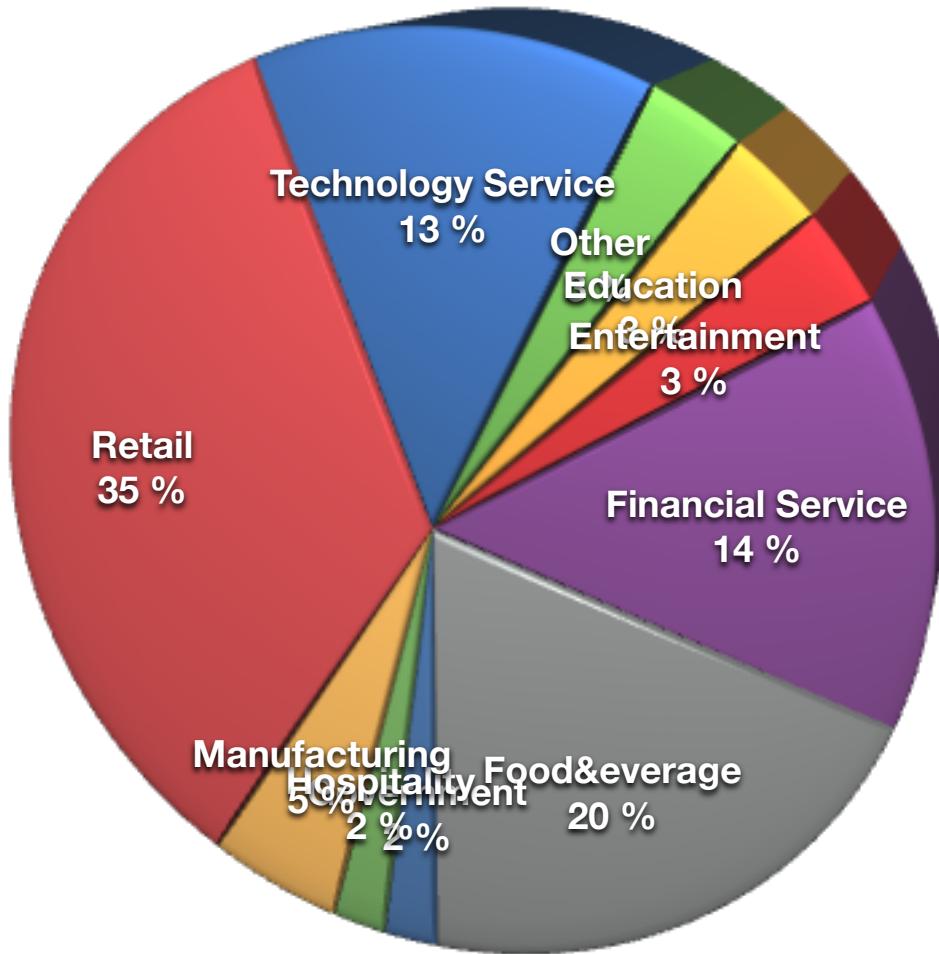
Official Statistics Industry relation

WHERE

WHO

HOW

PROTECTION



Source: Verizon Data Breach Report 2009

ORACLE®

The Myth of Hacking Oracle



Oracle Day 2009
Where Experience
Meets Innovation

- WHERE
- WHO
- HOW
- PROTECTION

ORACLE®

Who is attacking us ?



WHERE



WHO



HOW



PROTECTION

Hack3rs < 20 %

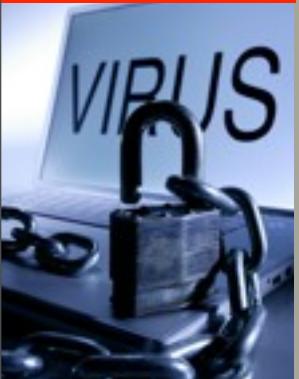
Insiders < 80 %

Information Security Has Changed



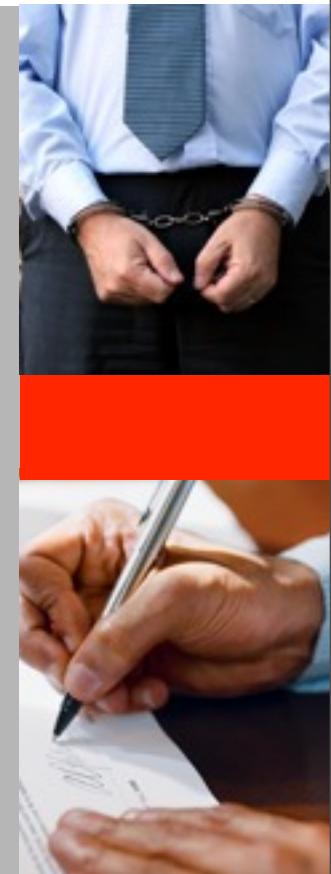
1996

- Hobby Hackers
- Web Site Defacement
- Viruses
- Infrequent Attacks



2009

- **Rentable
professional
Hackers**
- Criminals
- Denial of Service
- Identity Theft
- Constant Threat



ORACLE®

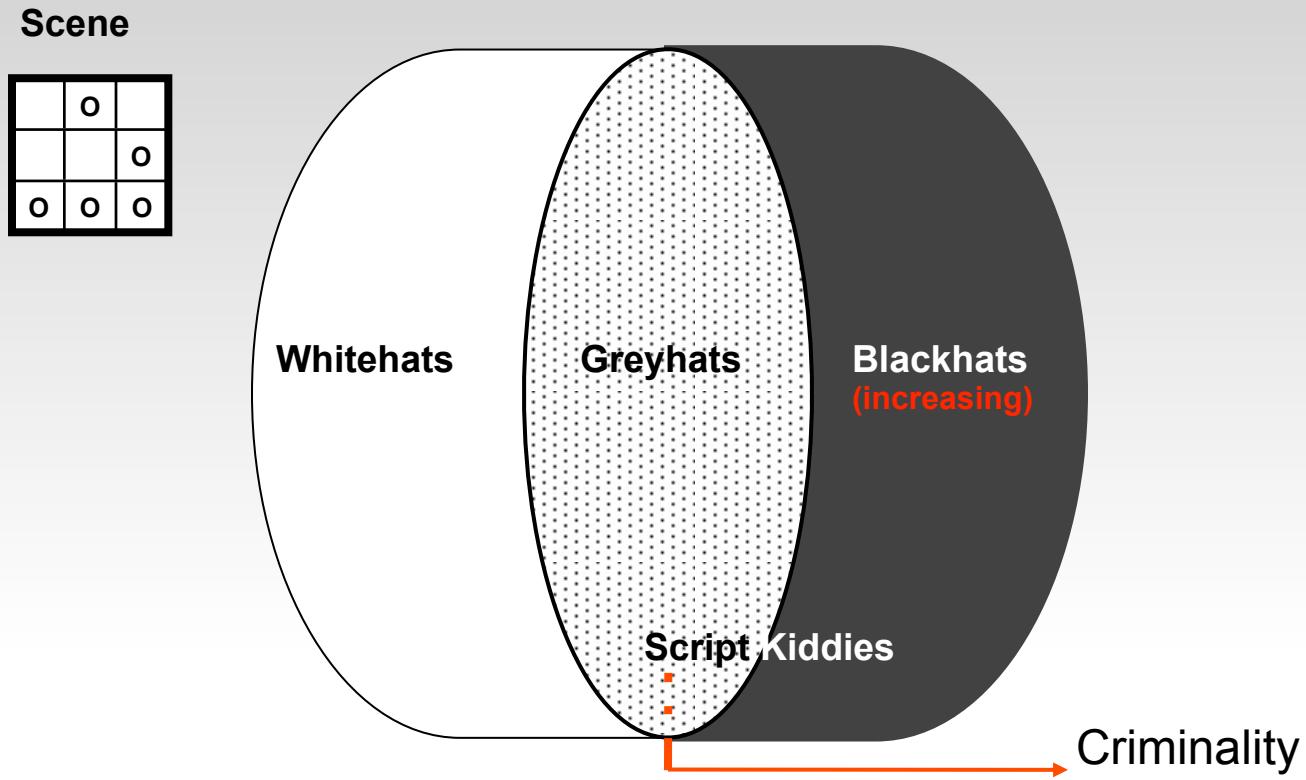
Mythos Hacker



ORACLE®



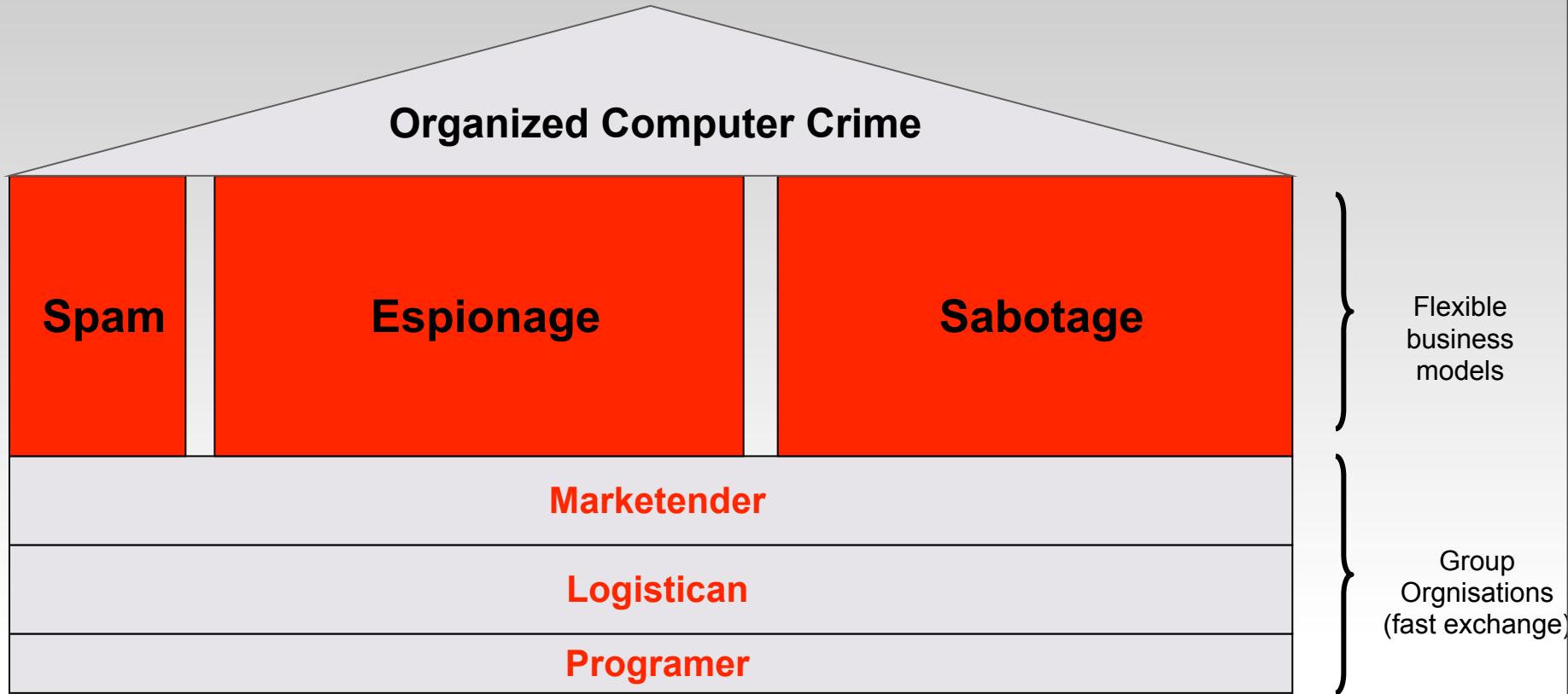
Underground naming conventions



ORACLE®



Underground organisation



Hacking Steps

Preparation Phase

- Targeting
- Information collection
- Social engeneering
- Social networking
- Underground scene consolidation

Planing Phase

- Detailed plannings
- Risk analysis
- Staffing
- Alternative plans
- Methodes
- Technics
- Choose precautions

HACK

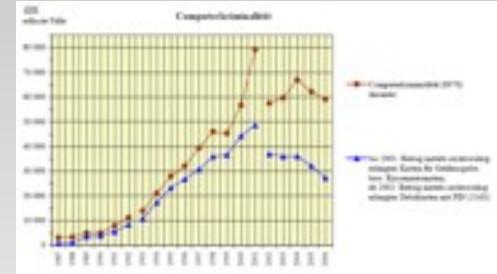
- Attack
- Backdoor installation
- Track cleaning



Official statistics Secret Service Germany



Dramatical increas of the computer crime since the last 12 years (professionalism)



Bigest damage by insiders (sabotage, spying,
Information selling)



Typical Hacker is male and over 21;
BUT starts with 14 !!!

Kod	Verbrechensgruppe	Jahreszeit		Vorjahr		Vergleichszeit	
		1998	2008	2008/99	%	1998	2008
810	Impersonation	29.540	62.184	-3.037	-4,8	40.2	40.2
8100	Rechte nachrichten erlangende Verbrechen mit PDS	37.467	51.193	-4.880	-13,1	46.0	46.9
8110	Computerkrim. (SIS/HSB)	30.252	33.873	3.621	11,3	38.9	46.7
8119	Reichweite/Ausprägungsmerkmale zu Computerkriminalität	1.633	1.786	153	9,2	1.671	1.614
8400	Fälschung/verfälschung der Daten, Übersetzung ins Rechtswort für Datensicherung (§ 296, 279 BGB)	2.449	1.983	1.448	54,5	46.7	46.7
870	Unterschlüpführung, Computerkrim. § 119a, Art. 16 Abs.	1.871	1.898	21	1,1	20.0	11,9
8700	Sabotage, Spionage	2.000	2.004	204	10,0	40.2	40.2
8710	Reichweite/Ausprägungsmerkmale zu Sabotage, Spionage (gerne Anwendung z.B. Computerkrim.)	1.929	2.085	156	23,0	46.7	46.7
8719	Sabotage/Spionage in Form physischer/technischer Zerstörung	727	871	144	19,3	38.9	38.9

Kod	Verbrechensgruppe	Jahreszeit		Vorjahr		Vergleichszeit	
		1998	2008	2008/99	%	1998	2008
810	Impersonation	18.686	36.723	18.037	48,9	32.2	76,9
8100	Rechte nachrichten erlangende Verbrechen mit PDS	7.135	7.528	393	5,5	13.8	14.9
8110	Computerkrim. (SIS/HSB)	4.940	7.623	2.683	52,2	8.3	10.8
8119	Reichweite/Ausprägungsmerkmale zu Computerkriminalität	2.340	2.423	83	3,5	1.671	1.614
8400	Fälschung/verfälschung der Daten, Übersetzung ins Rechtswort für Datensicherung (§ 296, 279 BGB)	840	763	223	26,9	31,2	38,7
870	Unterschlüpführung, Computerkrim. § 119a, Art. 16 Abs.	180	167	13	7,0	7,1	8,8
8700	Sabotage, Spionage	847	863	15	1,8	8,7	8,1
8710	Reichweite/Ausprägungsmerkmale zu Sabotage, Spionage (gerne Anwendung z.B. Computerkrim.)	1.716	1.813	197	11,5	5,7	8,8
8719	Sabotage/Spionage in Form physischer/technischer Zerstörung	537	613	176	32,4	7,1	9,1

Bei den Computerkriminalen überwiegend männliche erwachsene Täter/Innen ab 17 Jahren.

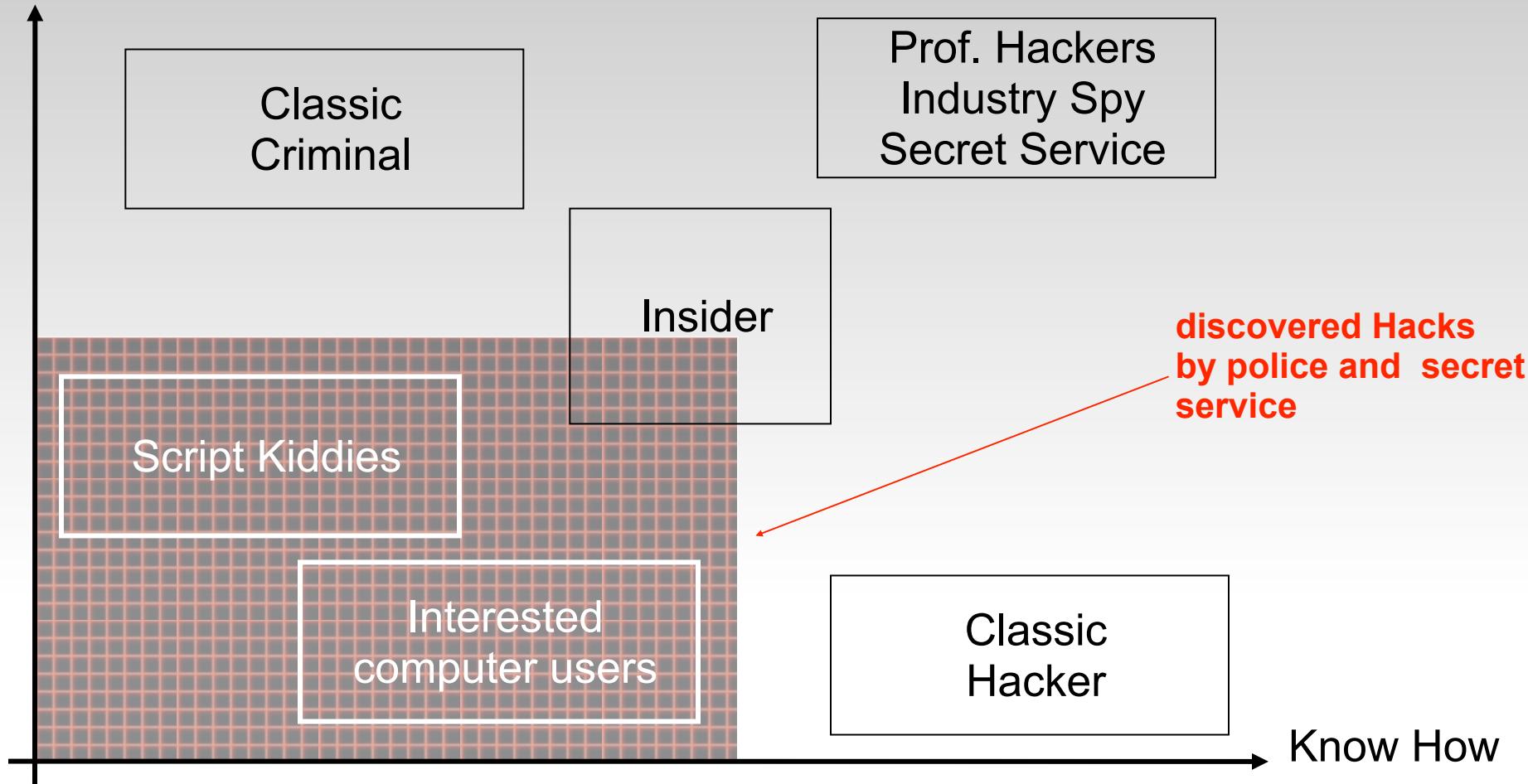
Source: BND Sicherheitsreport 2008

ORACLE®



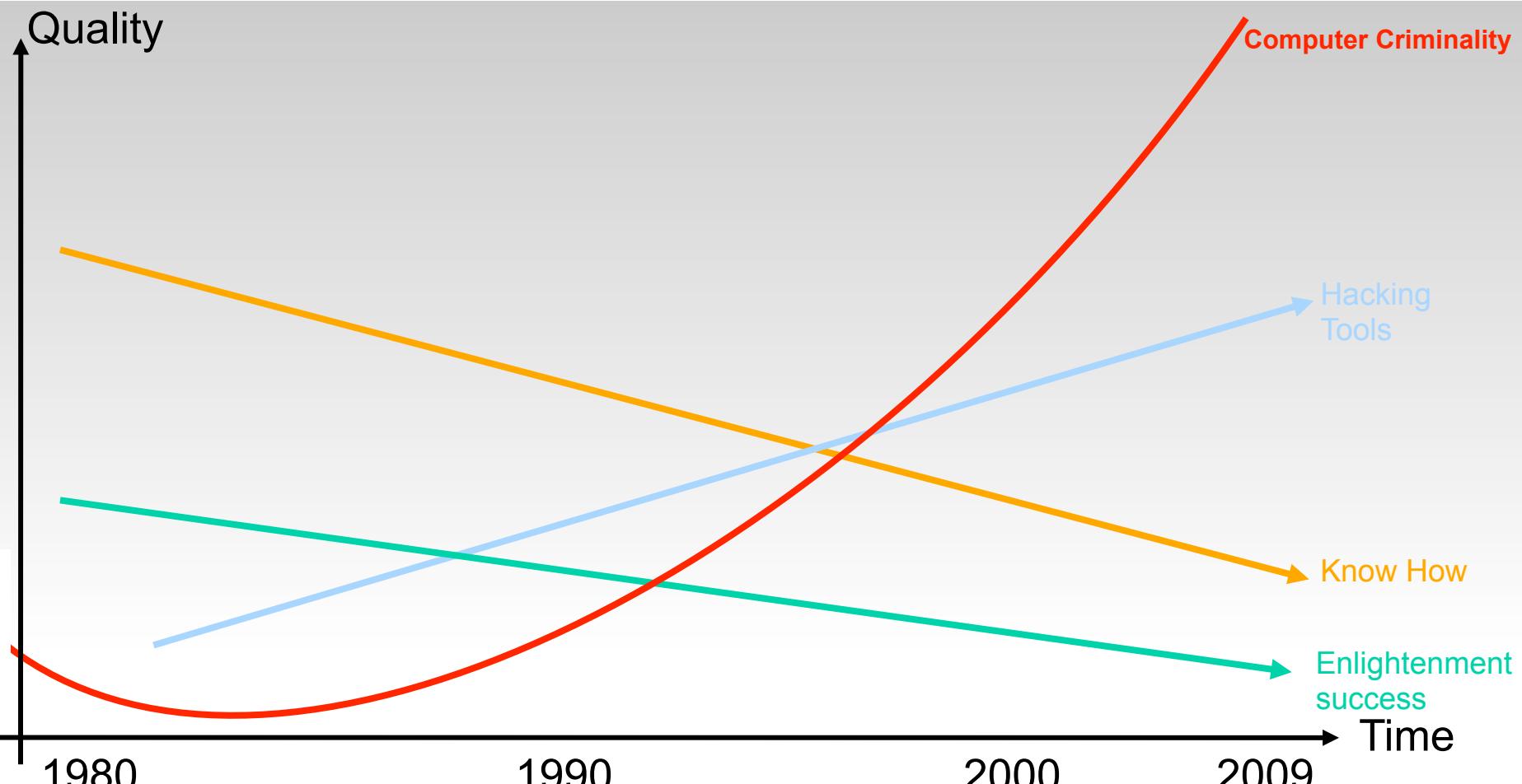
Profiling Hack3rs

Criminal
Energie



ORACLE®

Computer Crime Development



Source: BND Sicherheitsreport 2008

ORACLE®

Short Facts

87 % of all Databases are compromised over the **Operating System**

80 % of the damage is caused by **insiders**

1 % of all professional hacks are only **recognized**

10 % of all “standard hacks” are made **public**

Highscore List

Source: Black Hat Convention 2008

40sec Windows XP SP2

55sec Windows Vista

63sec Windows NT4.0 WKST, SP4

70sec Windows 2003 Server

140sec Linux Kernel 2.6.

190sec Sun Solaris 5.9 with rootkit

...

List includes also AIX, HPUX, OS2, OSX, IRIX, ...

ORACLE®

Shopping List 2007/2008

Source: heise security, DEFCON 2008, BlackHat 2008

50.000 \$ Windows Vista Exploit (4000\$ for WMF Exploit in Dec2005)

7 \$ per ebay-Account

20.000 \$ medium size BOT network

30.000 \$ unknown security holes in well known applications

25-60 \$ per 1000 BOT clients / week

ORACLE®

Crisis Shopping List 2009

Source: heise security, DEFCON 2009, BlackHat 2009

- 100.000 \$** Destruction of competitor image
- 250.000 \$** Full internal competitor database
- 25 \$** per credit card account (+sec code + valid date)
- 20.000 \$** medium size BOT network (buy or rent)
- 2000 \$** stolen VPN connection
- 5000 \$** contact to “turned around” insider

ORACLE®



WHERE

WHO

HOW

PROTECTION

Hack3rs < 20 %

Insiders < 80 %

ORACLE®

Insider examples !!!



European headlines 2008/2009:

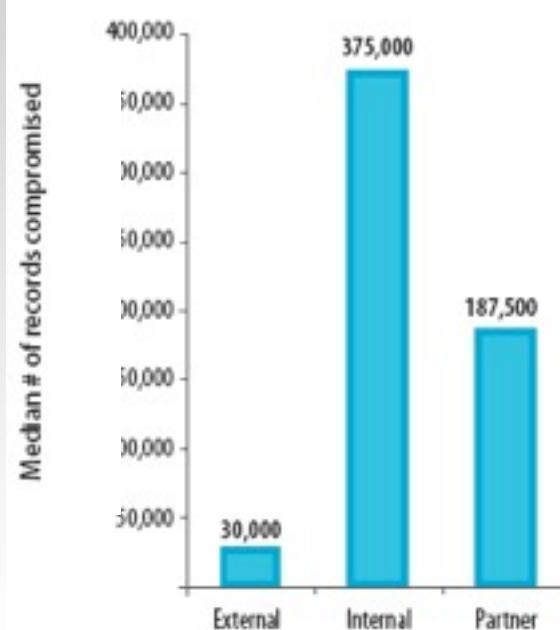
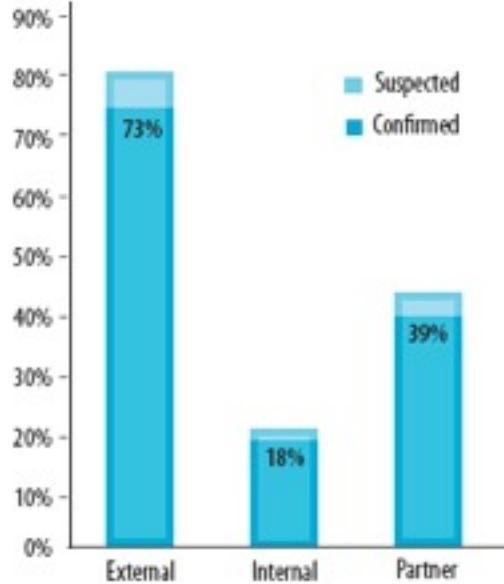
- lost top secret document about Al Quaida (public train)
- stolen data of thousand prisoners and prison guards
- personal information of 70Mio people unencrypted on DVD's lost
- bank employee gambled with 5.4Bio US\$
- 88% of admins would steal sensitive corporate informations
- Industry espionage by insiders increased dramatically
- biggest criminal network (RBN) still operating
- Tousends of stolen hardware equipement @ US Army
- US Army lost 50.000 personal data of former soliers
- Chinas „Red Dragon“ organization cracked german gov network
- Lichtenstein Affaire – Insider vs. Secret Service
- ..
- .



Insider Threat

- Outsourcing and off-shoring trend
- Large percentage of threats go undetected
 - huge internal know how
 - powerful privileges
 - track cleaning
 - „clearance“ problem
 - foreign contact persons / turnovers
- Easier exchange of sensitive data
(hacker's ebay, RBN, paralell internet, dead postboxes...)

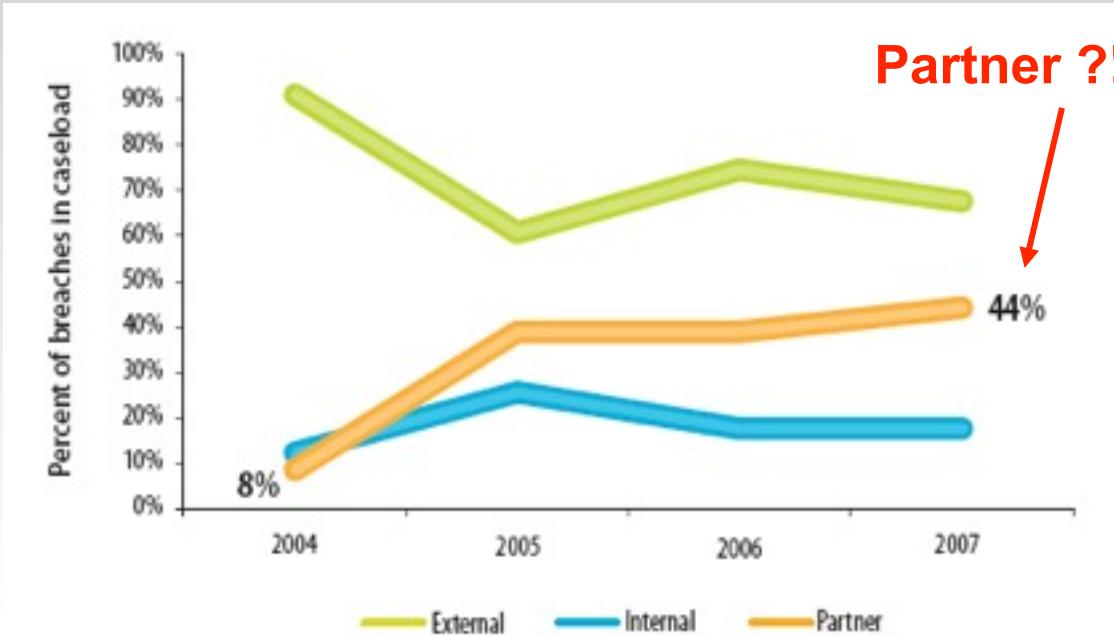
Official Statistics Relation internal / external



Source: Verizon Data Breach Report 2009

ORACLE®

Official Statistics 3 years development



Source: Verizon Data Breach Report 2009

ORACLE®

The Myth of Hacking Oracle



Oracle Day 2009
Where Experience
Meets Innovation

- WHERE
- WHO
- HOW
- PROTECTION

ORACLE®

How we get attacked

WHERE



WHO



HOW

Over 80% of all hacks are done from internal



PROTECTION



At the moment one of the most dangerous and effectives methode in the scene

ORACLE®

How we get attacked -- **REALITY**

WHERE

WHO

HOW

PROTECTION

- Standard configuration
- Misconfiguration
- Misunderstanding of security
- Human errors
- Process/Workflow errors
- “old” versions / no patches
- Known/published wholes/bugs/workarounds
- Downloadable cracking software (script kiddies)

- Real hacks/cracks

ORACLE®

The Myth of Hacking Oracle



Oracle Day 2009
Where Experience
Meets Innovation

- WHERE
- WHO
- HOW
- PROTECTION

ORACLE®

Protection

WHERE

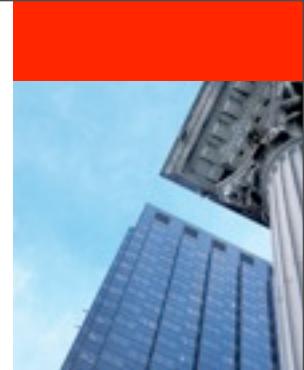
WHO

HOW

PROTECTION

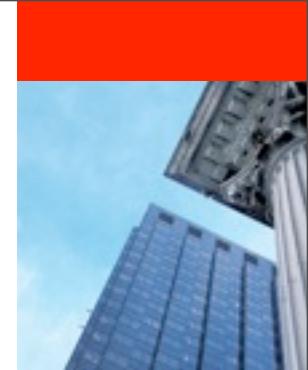
> 90%
of our security problems
could be solved !!!

Think ...



- **Security is a „race“, if you stop running you'll lose**
- **Security IS NOT a product; it's an ongoing living process**
- **Train your employees**
- **Security IS an intelligent combination of more areas**
-> „Big picture“
- **Focus on your data, not only on the technic**
- **Start with the basics**

Think about Solutions...



Problem

- External Attackers
- Internal Threats
- Image Damage
- Internal Security Regulations
- Regulatory Compliances
- ..
- ..

Oracle Solution

- **Separation of duties**
- **Insider threat protection**
- **Strong access authentication**
- **Strong encryption (DB/OS/Net)**
- **Fine grained real time external auditing**
- **Data consolidation control**
- **High availability + Security combination**

Oracle Security Product

- Advanced Security Options (ASO) 
- Network encryption
- Transparent data encryption
- Strong authentication
- Database Vault 
- Audit Vault
- Secure Backup
- Virtual Privat Database (VPD)
- Oracle Label Security (OLS)
- Data Masking
- Total Recall



 Oracle Differentiator / no competition

ORACLE®

Oracle Security Solutions Summary

REPORTING & ALERTING

IDENTITY AND ACCESS MANAGEMENT

Identity Administration	Directory Services	Access Management
<ul style="list-style-type: none">• User Provisioning• Role Management• Self-Service driven	<ul style="list-style-type: none">• Scalable LDAP Storage• Virtual Directory• Directory Synchronization	<ul style="list-style-type: none">• Risk-based Authorizat.• Entitlements Managem.• Single Sign-On• Federation• Inform. Rights Mgmt

DATABASE SECURITY

Activity Monitoring	Access Control and Authorization	Encryption and Data Masking
<ul style="list-style-type: none">• Unauthorized Activity Detection• Automated Compliance Reports• Secure Configuration Audit	<ul style="list-style-type: none">• Privileged User Controls• Multi-Factor Authorization• Classification Control	<ul style="list-style-type: none">• Transparent Data Encryption• De-identification for Non-Production• Built-In Key Management

IT MANAGEMENT & INTEGRATION

ORACLE®

Database Defense-in-Depth



Monitoring

- Configuration Management
- Audit Vault
- Total Recall

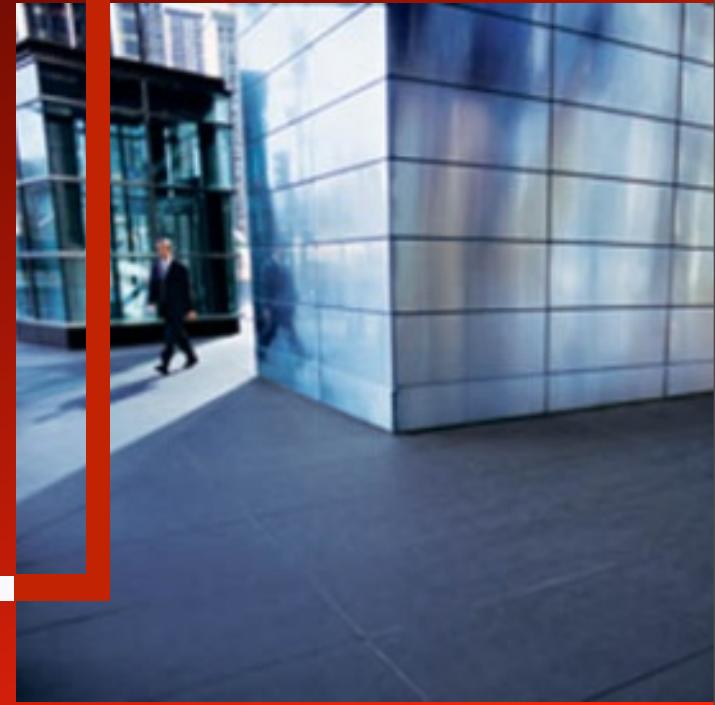
Access Control

- Database Vault
- Label Security

Encryption & Masking

- Advanced Security
- Secure Backup
- Data Masking

Security

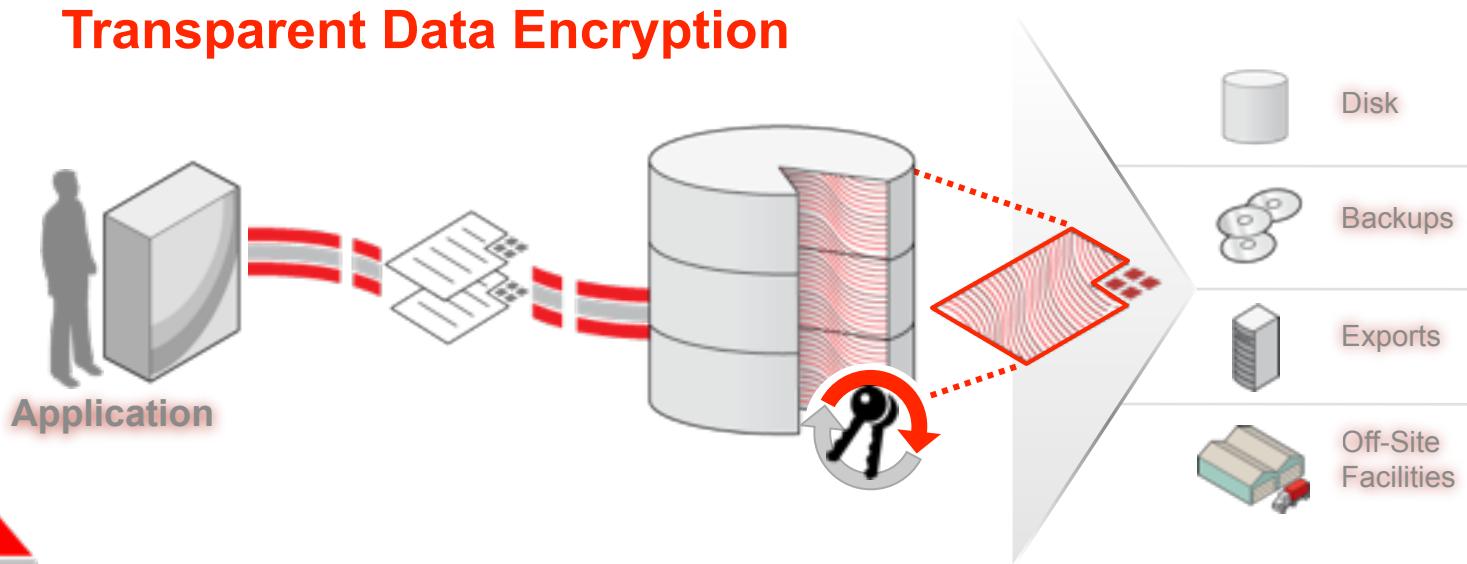


ORACLE®

ORACLE

Oracle Advanced Security

Transparent Data Encryption



- Complete encryption for data at rest
- No application changes required
- Efficient encryption of all application data
- Built-in key lifecycle management



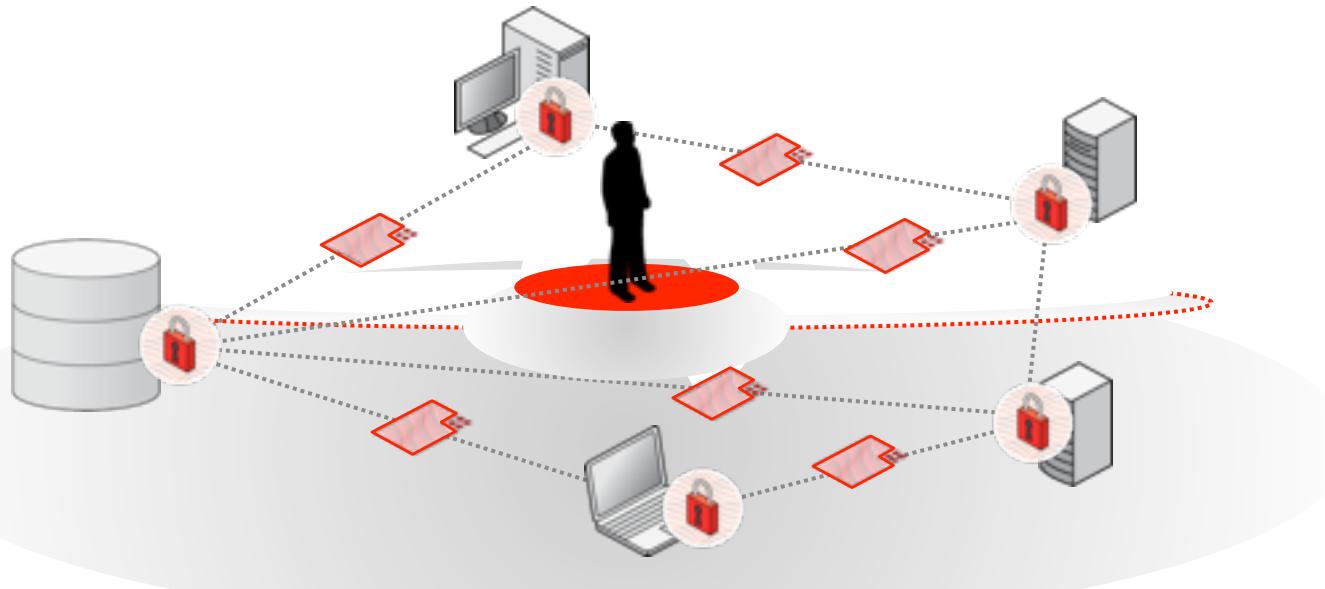
ORACLE

Oracle Confidential

39

Oracle Advanced Security

Network Encryption & Strong Authentication



- Standard-based encryption for data in transit
- Strong authentication of users and servers (e.g. Kerberos, Radius)
- No infrastructure changes required
- Easy to implement

ORACLE®

Oracle Confidential

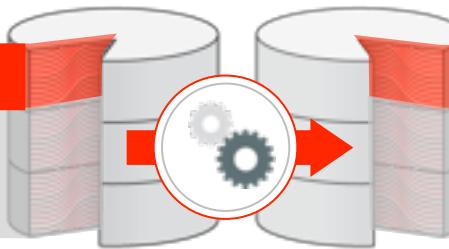
40

Oracle Data Masking

Irreversible De-Identification

Production

LAST_NAME	SSN	SALARY
AGUILAR	203-33-3234	40,000
BENSON	323-22-2943	60,000



Non-Production

LAST_NAME	SSN	SALARY
ANSKEKSL	111-23-1111	60,000
BKJHHEIEDK	222-34-1345	40,000



- Remove sensitive data from non-production databases
- Referential integrity preserved so applications continue to work
- Sensitive data never leaves the database
- Extensible template library and policies for automation

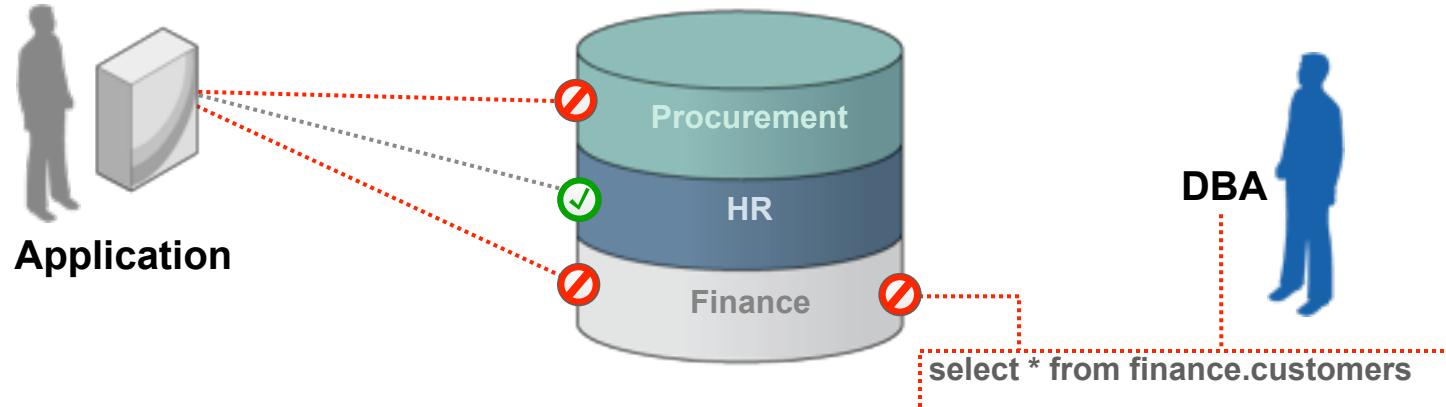
ORACLE®

Oracle Confidential

41

Oracle Database Vault

Separation of Duties & Privileged User Controls



- DBA separation of duties
- Limit powers of privileged users
- Securely consolidate application data
- No application changes required



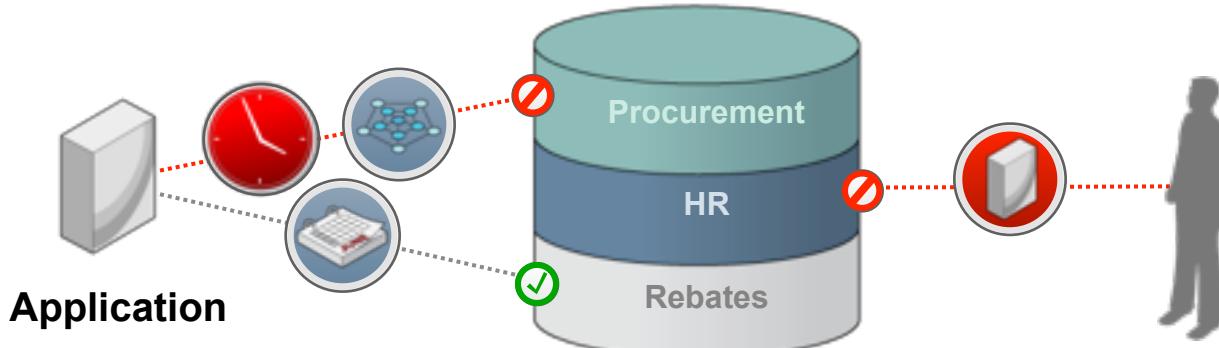
ORACLE®

Oracle Confidential

42

Oracle Database Vault

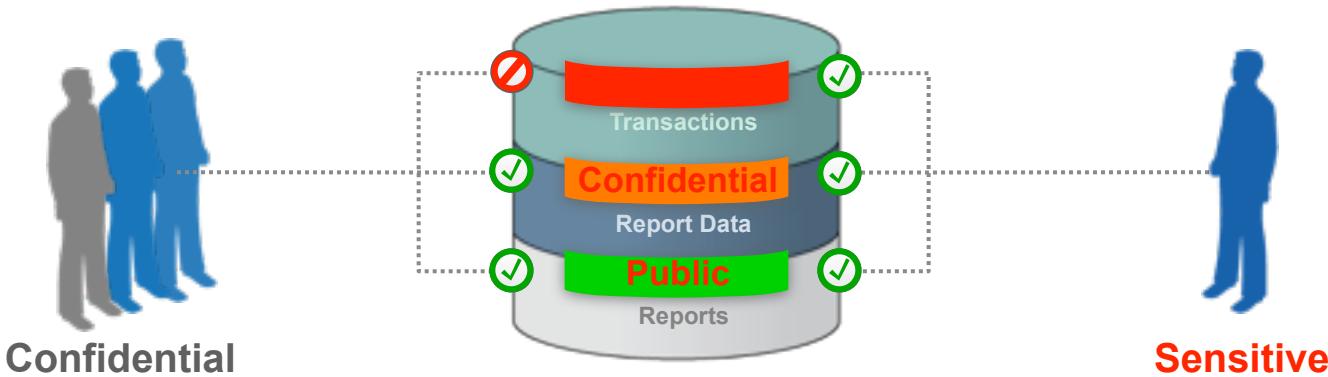
Multi-Factor Access Control Policy Enforcement



- Protect application data and prevent application by-pass
- Enforce who, where, when, and how using rules and factors
- Out-of-the box policies for Oracle applications, customizable

Oracle Label Security

Data Classification for Access Control



- Classify users and data based on business drivers
- Database enforced row level access control
- Users classification through Oracle Identity Management Suite
- Classification labels can be factors in other policies

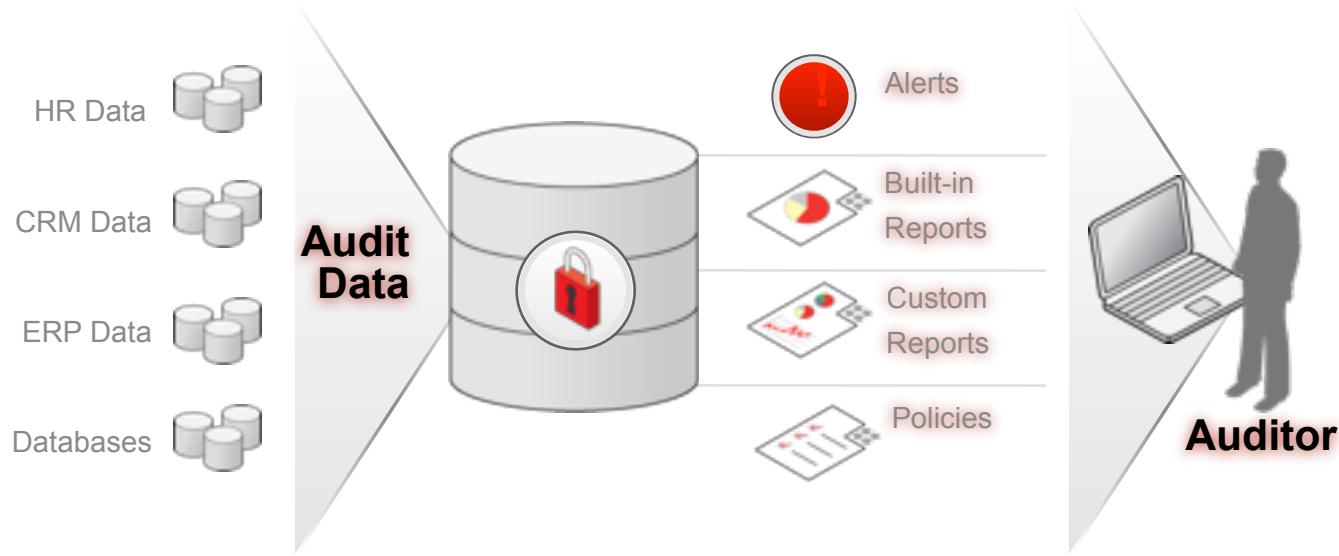
ORACLE®

Oracle Confidential

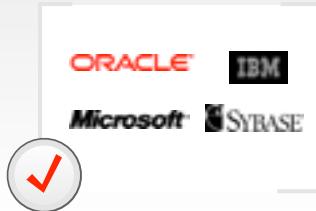
44

Oracle Audit Vault

Automated Activity Monitoring & Audit Reporting



- Consolidate audit data into secure repository
- Detect and alert on suspicious activities
- Out-of-the box compliance reporting
- Centralized audit policy management

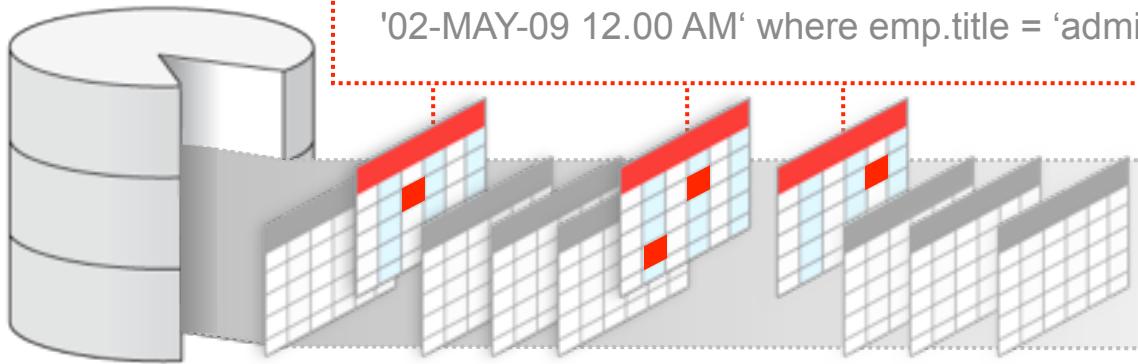


ORACLE®

Oracle Confidential

Oracle Total Recall

Secure Change Management



- Transparently track data changes
- Efficient, tamper-resistant storage of archives
- Real-time access to historical data
- Simplified forensics and error correction

Database Defense-in-Depth



Monitoring

- Configuration Management
- Audit Vault
- Total Recall

Access Control

- Database Vault
- Label Security

Encryption & Masking

- Advanced Security
- Secure Backup
- Data Masking