# Security

ORACLE®


# Oracle Hacker Days Zagreb 26.01.2010

ORACLE

Peter Kestner
Technology Director - Database Security
Oracle Core Technology EMEA

ORACLE

Oracle Day 2009

Where Experience Meets Innovation

ORACLE

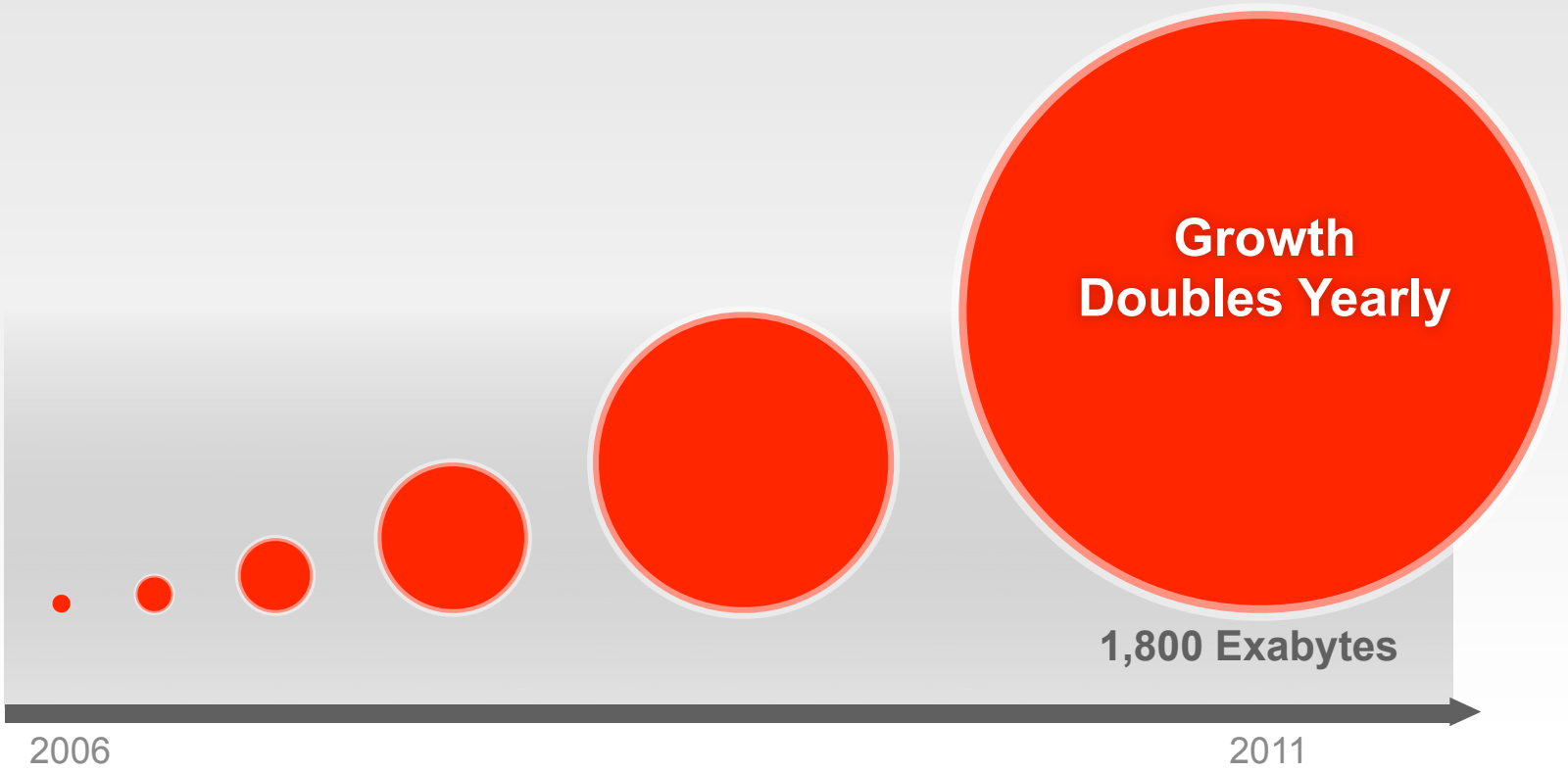
# Security

**Peter Kestner**

Technology Director – Database Security

Oracle Core Technology EMEA

# More data than ever…

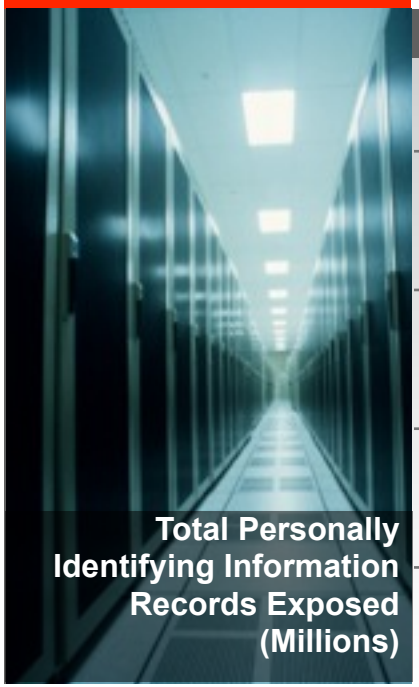


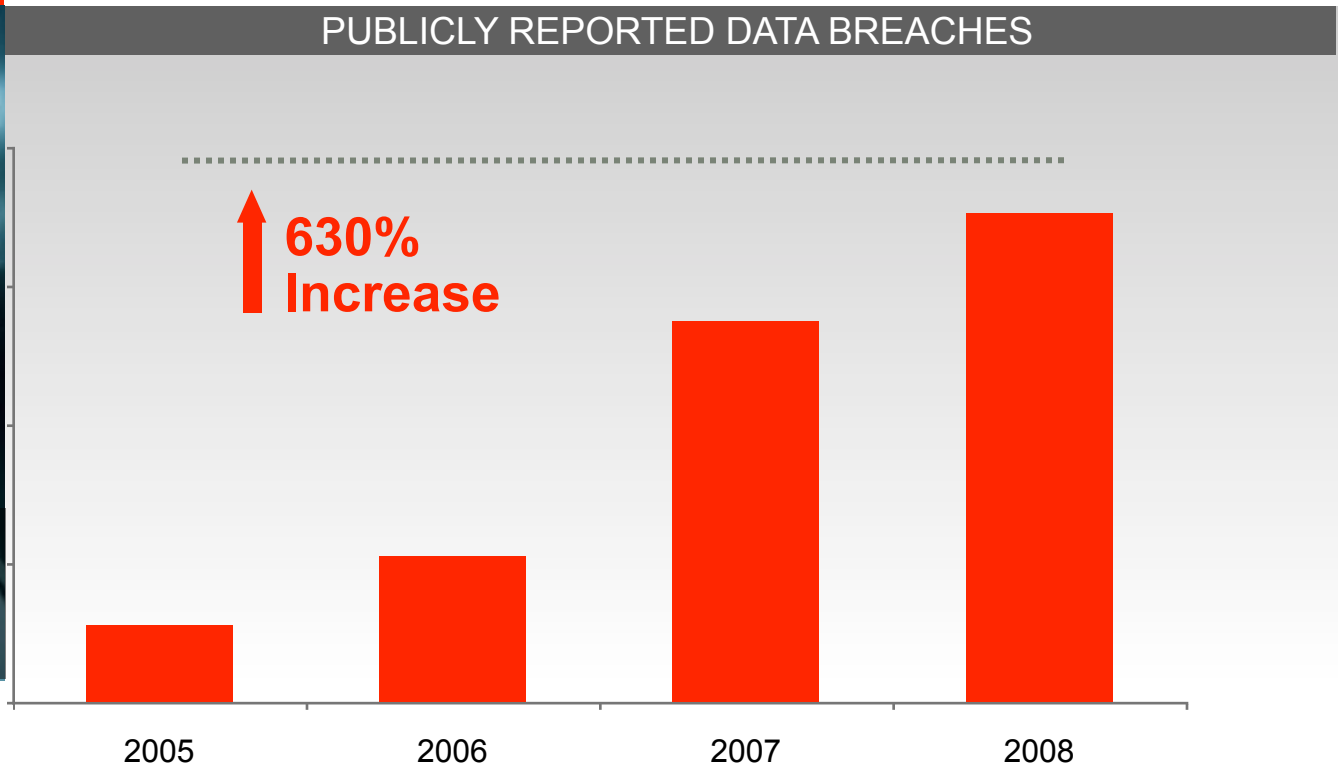

**Source: IDC, 2008**

# More breaches then ever…

**Data Breach**

**Once exposed, the data is out there – the bell can't be un-rung**

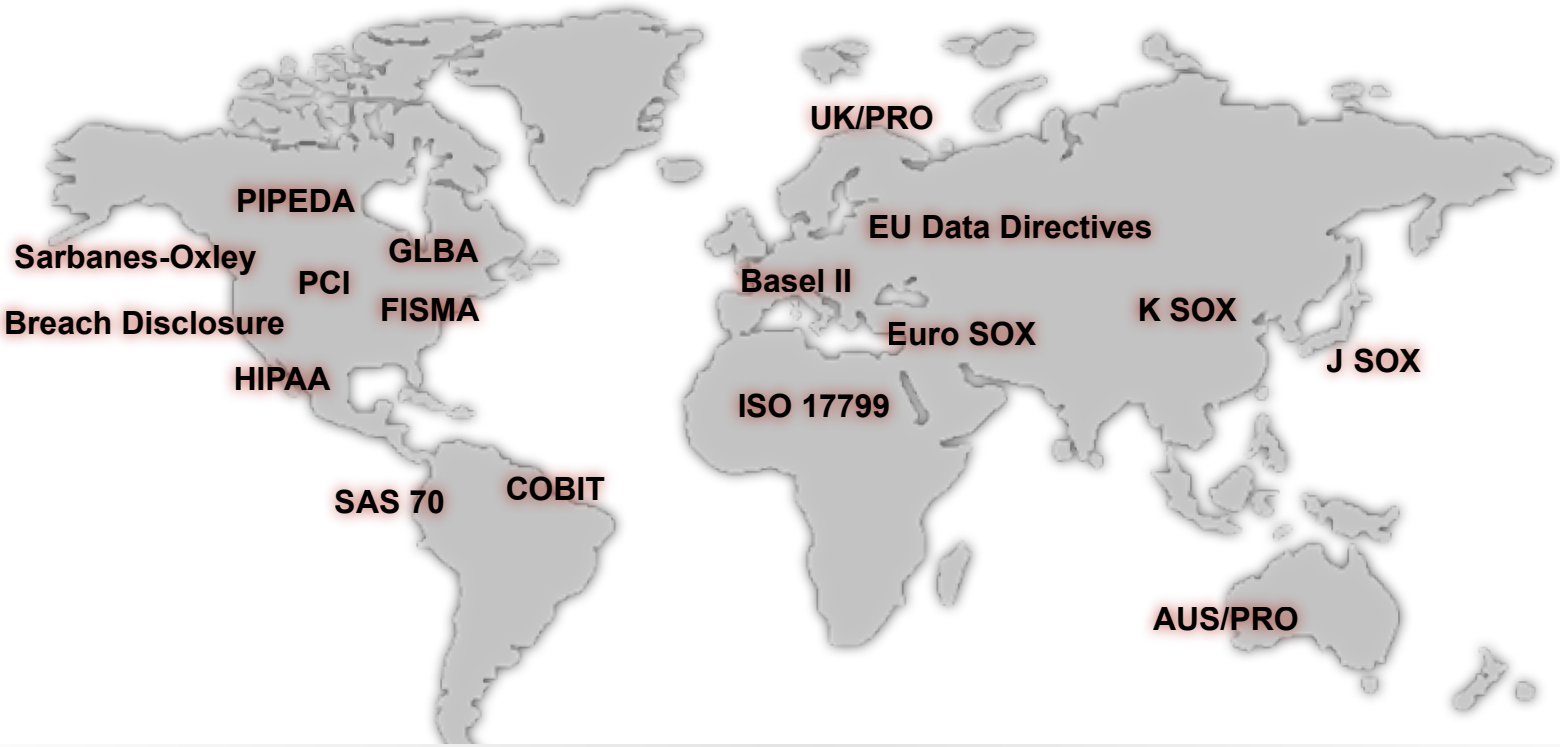



**Source: DataLossDB, 2009**

# More threats than ever…


# More Regulations Than Ever…




**90%** Companies behind in compliance

Source: IT Policy Compliance Group, 2009.

# Market Overview: IT Security In 2009


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

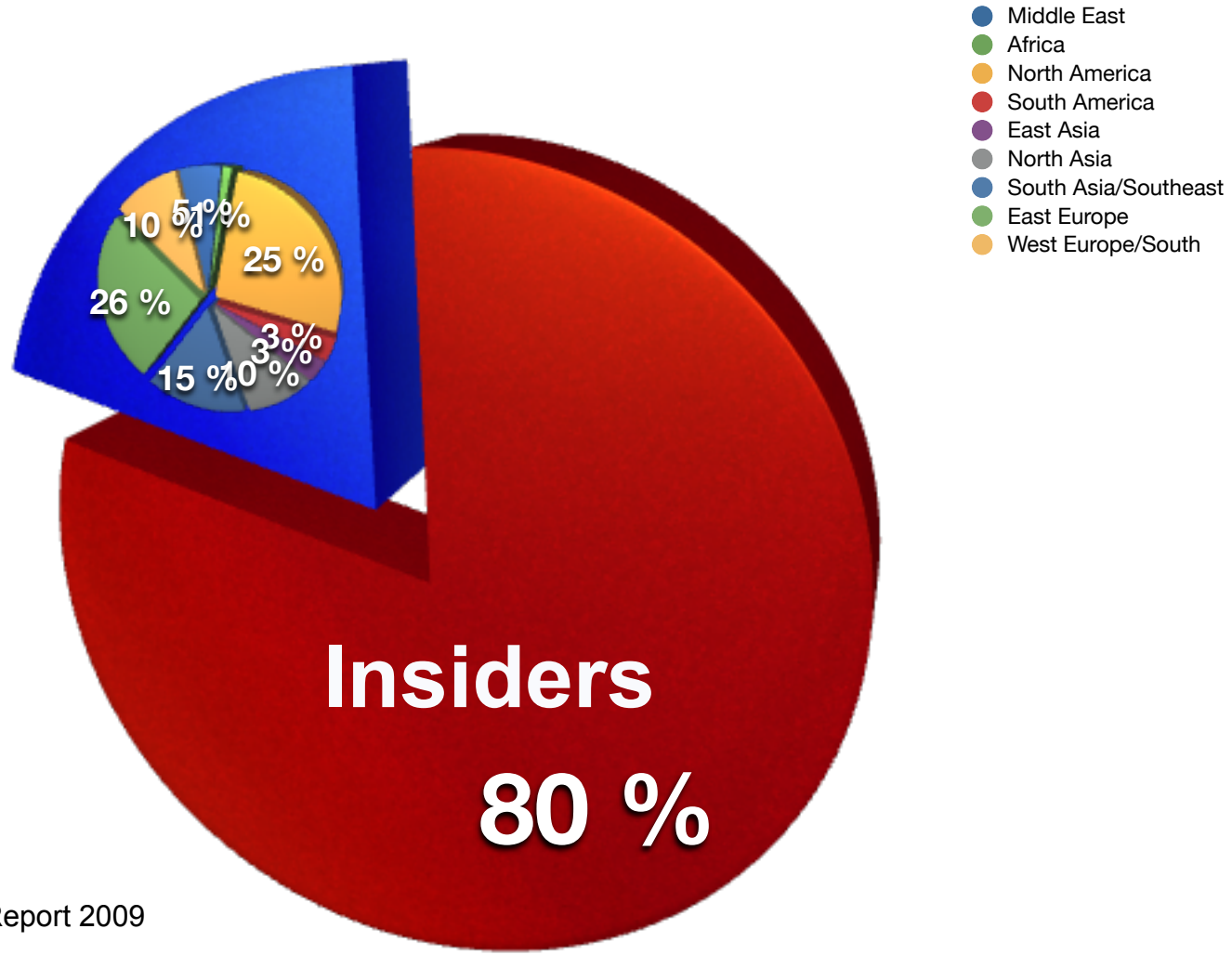
Oracle Day 2009
Where Experience Meets Innovation

- **WHERE**
- **WHO**
- **HOW**
- **PROTECTION**

ORACLE

# Where does the attacks come from ?

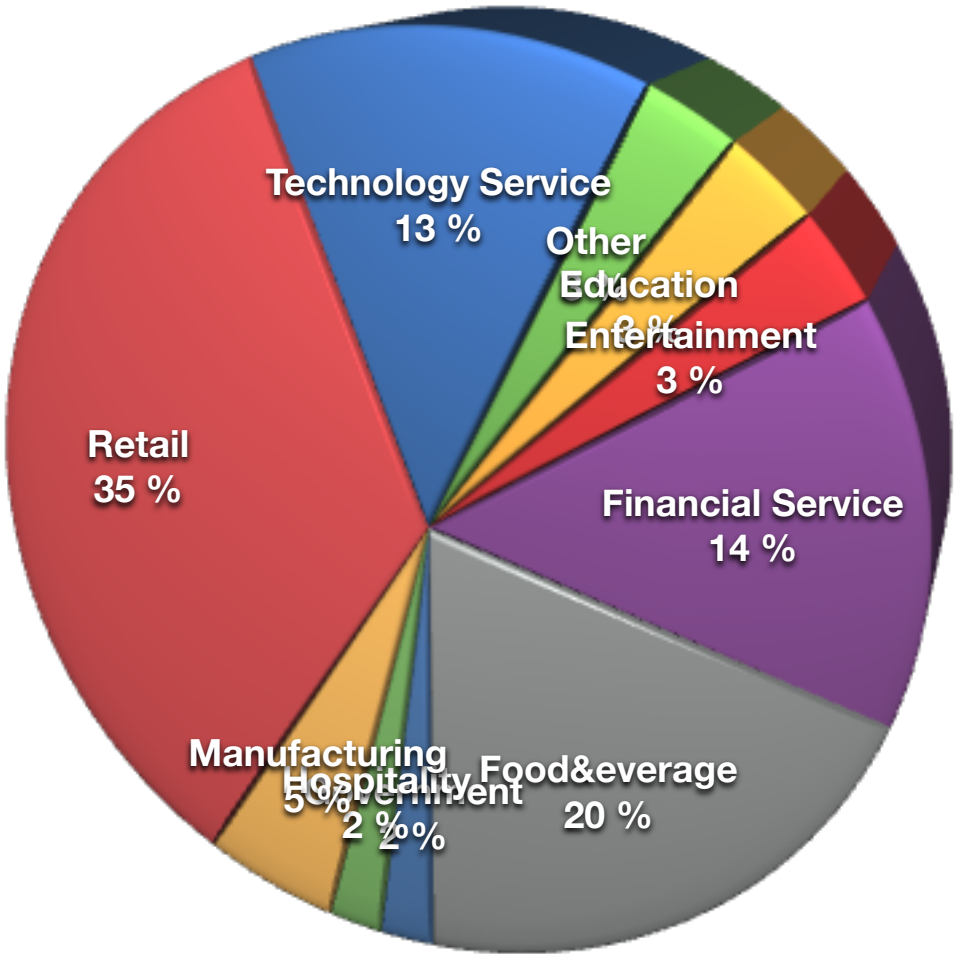
- WHERE
- WHO
- HOW
- PROTECTION




Source: Verizon Data Breach Report 2009

# Official Statistics Industry relation

- WHERE
- WHO
- HOW
- PROTECTION




Source: Verizon Data Breach Report 2009

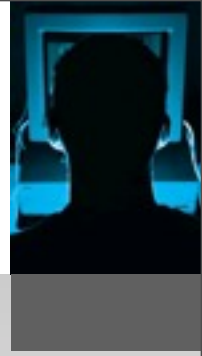
# The Myth of Hacking Oracle

Oracle Day 2009
Where Experience
Meets Innovation

- WHERE
- WHO
- HOW
- PROTECTION

ORACLE

# Who is attacking us ?



- WHERE
- WHO
- HOW
- PROTECTION

**Hack3rs ← 20 %**

**Insiders ← 80 %**

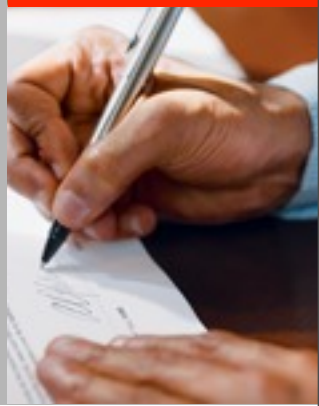
# Information Security Has Changed

**1996**

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


**2009**

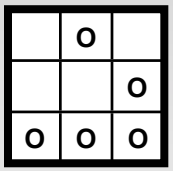
- **Rentable professional Hackers**
- Criminals
- Denial of Service
- Identity Theft
- Constant Threat

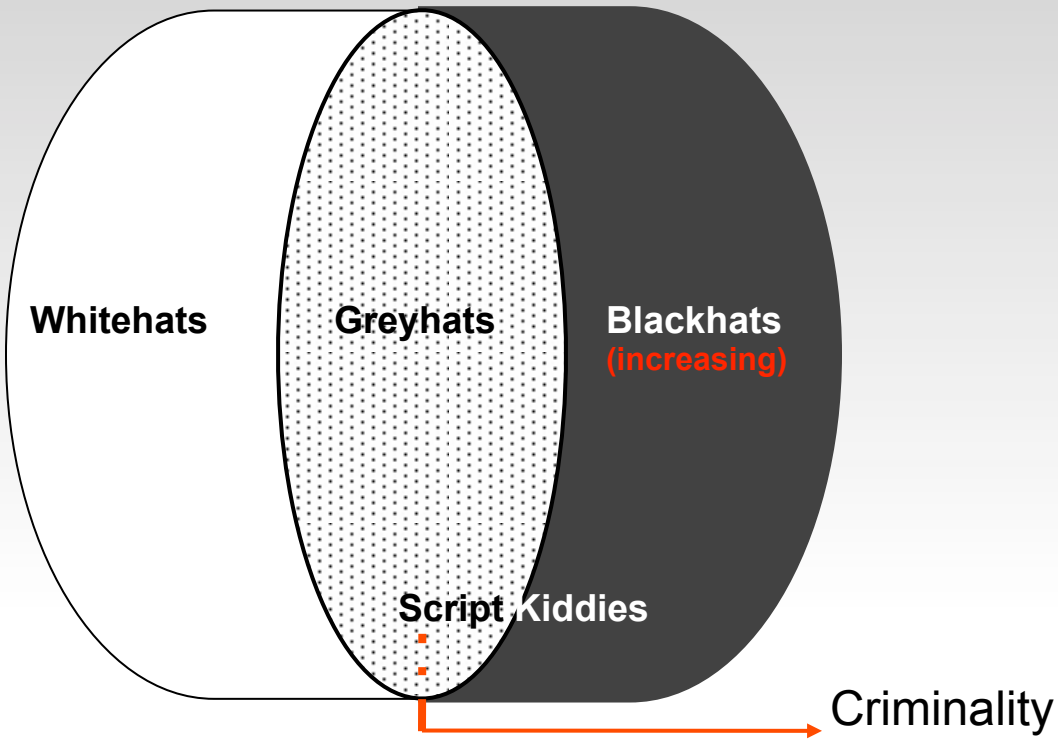


# Mythos Hacker

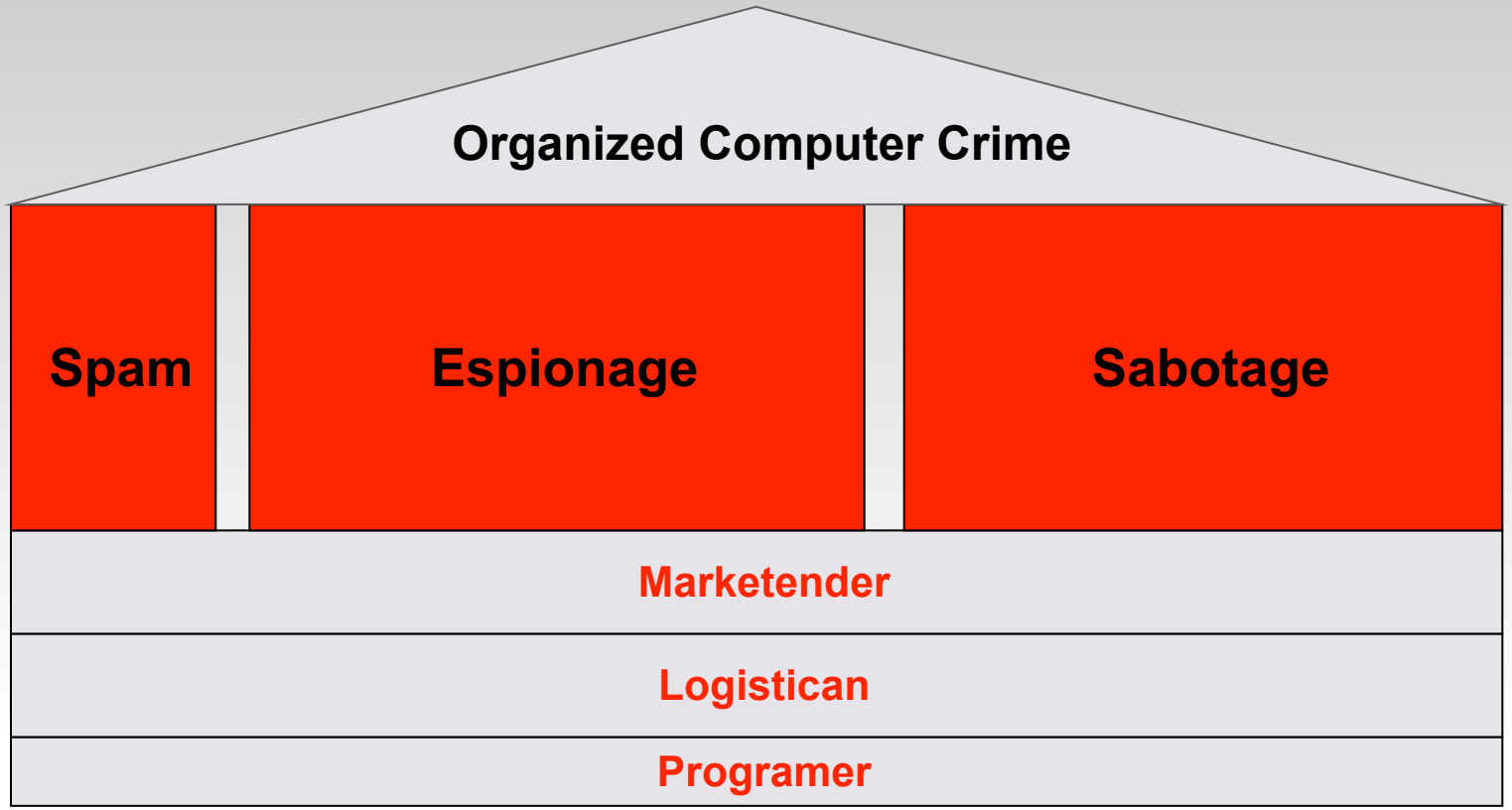
# Underground naming conventions


Scene



# Underground organisation

# Hacking Steps

**Preparation Phase**

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

**Planing Phase**

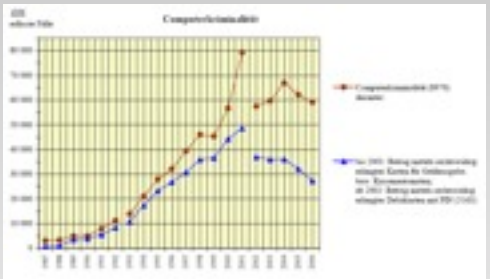
- Detailed plannings
- Risk analysis
- Staffing
- Alternative plans
- Methodes
- Technics
- Choose precautions

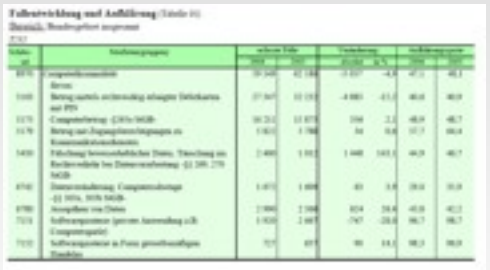
**HACK**

- Attack
- Backdoor installation
- Track cleaning

# Official statistics
# Secret Service Germany

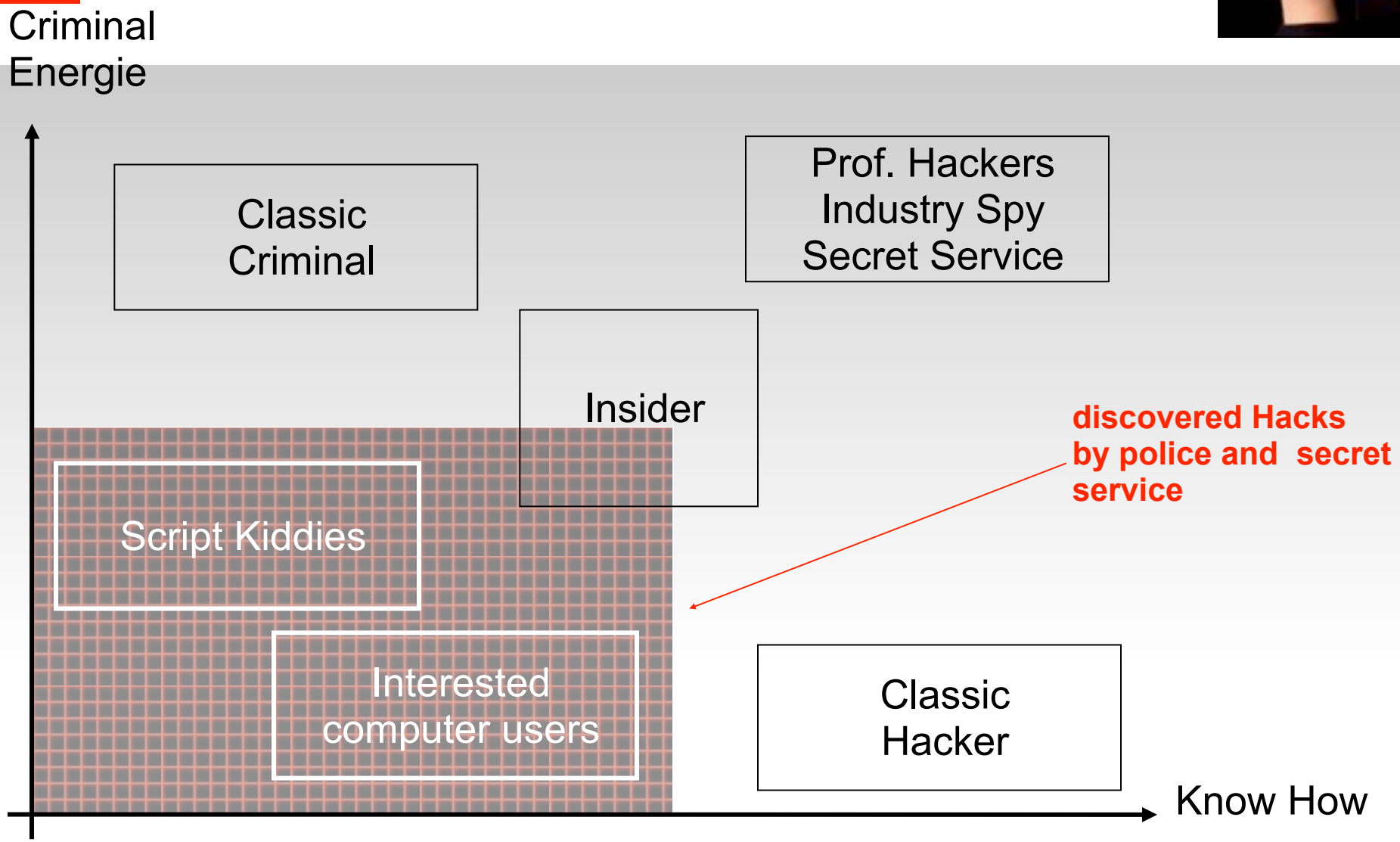
- **Dramatical increas of the computer crime since the last 12 years (professionalism)**
- **Bigest damage by insiders (sabotage, spying, Information selling)**
- **Typical Hacker is male and over 21; BUT starts with 14 !!!**



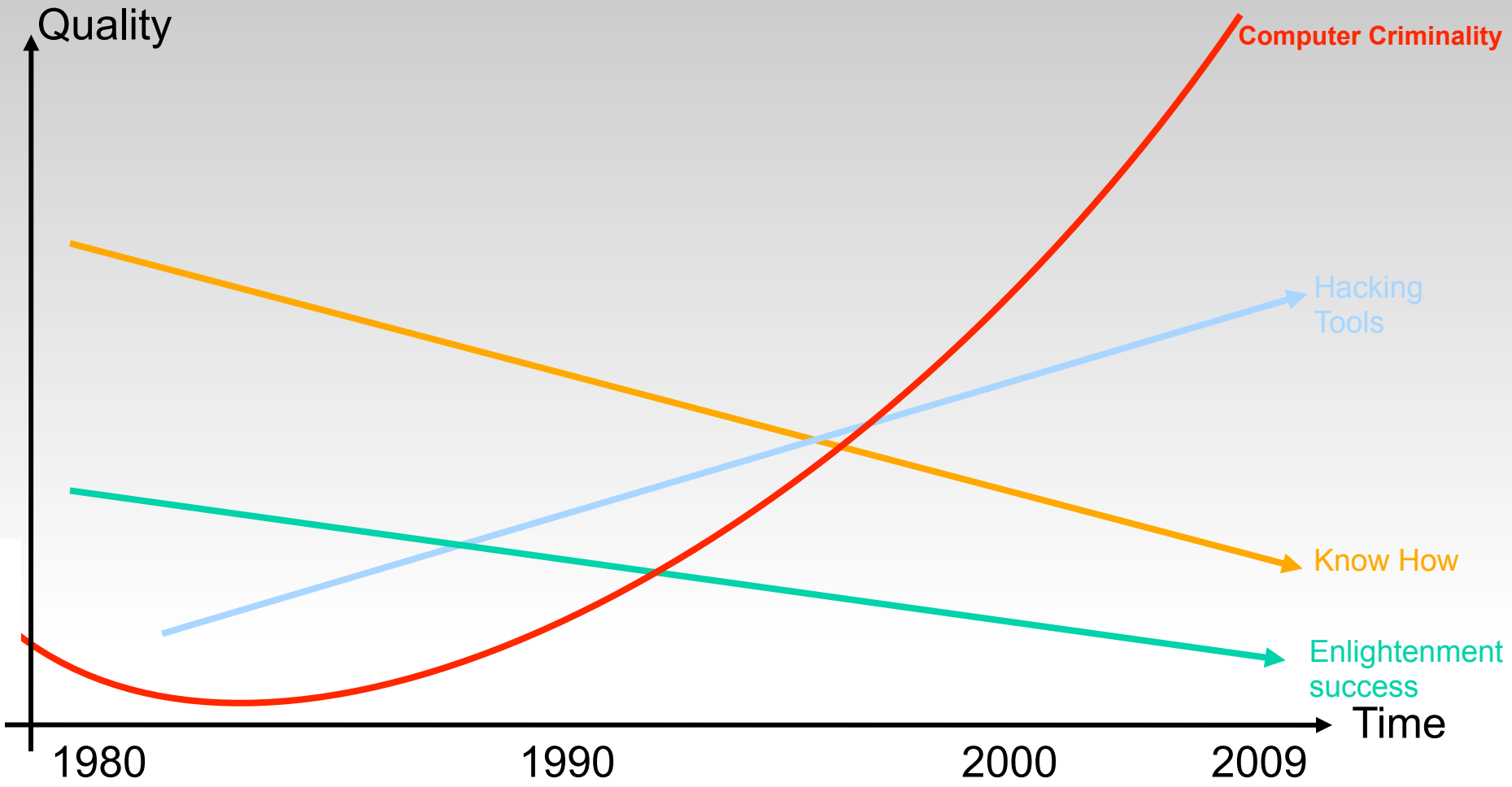


Source: BND Sicherheitsreport 2008

# Profiling Hack3rs

# Computer Crime Development




Source: BND Sicherheitsreport 2008

# 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, …**

# 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

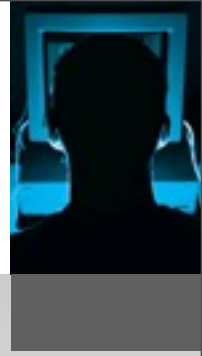
**30.000 $** unknown security holes in well known applications

**25-60 $** per 1000 BOT clients / week

# 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 |



- WHERE
- WHO
- HOW
- PROTECTION

Hack3rs ← 20 %

Insiders ← 80 %

# Insider examples !!!

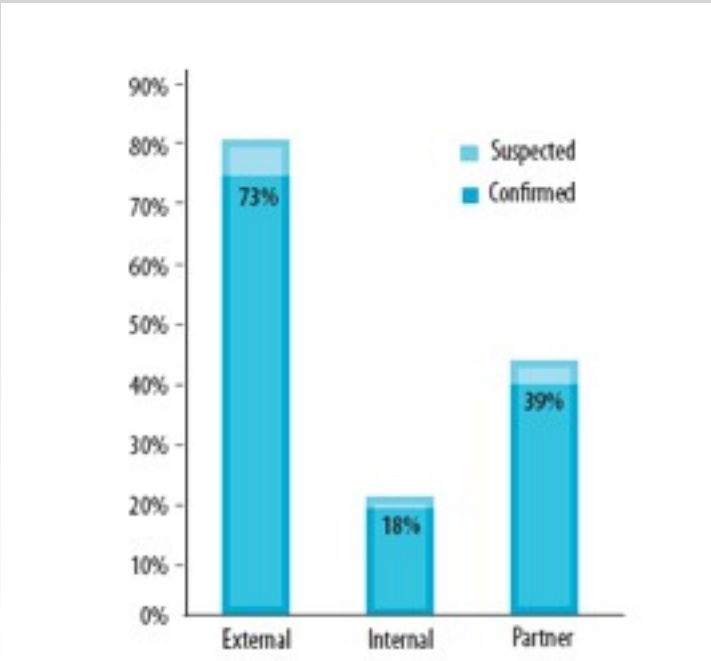
## European headlines 2008/2009:

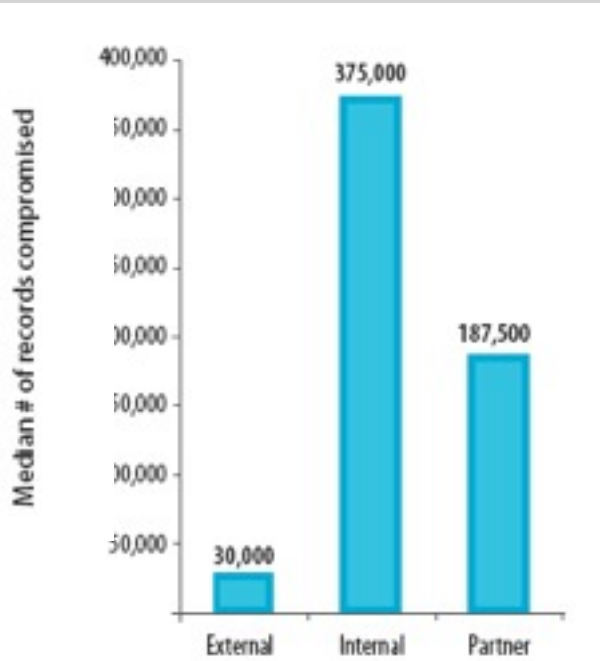
- lost top secret document about Al Quaida (public train)
- stolen data of thousand prisoners and prison guards
- personal information of 70Mio people unencrypted on DVD‘s lost
- bank employee gambled with 5.4Bio US$
- 88% of admins would steal sensitive corporate informations
- Industry espionage by 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...)

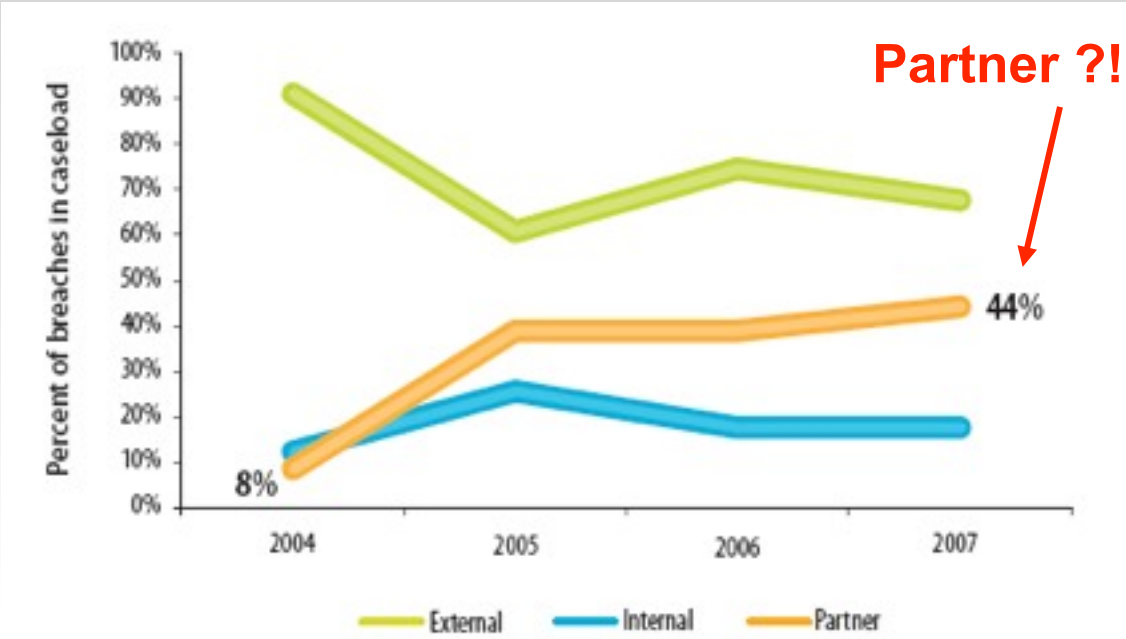
# Official Statistics Relation internal / external




Source: Verizon Data Breach Report 2009

# Official Statistics 3 years development




Source: Verizon Data Breach Report 2009

# The Myth of Hacking Oracle

Oracle Day 2009
Where Experience Meets Innovation

- WHERE
- WHO
- HOW
- PROTECTION

ORACLE

# How we get attacked

- WHERE
- WHO
- HOW
- PROTECTION

Over 80% of all hacks are done from internal







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

# 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)

>90%

-Real hacks/cracks

# The Myth of Hacking Oracle

Oracle Day 2009
Where Experience Meets Innovation

- WHERE
- WHO
- HOW
- PROTECTION

ORACLE

# Protection

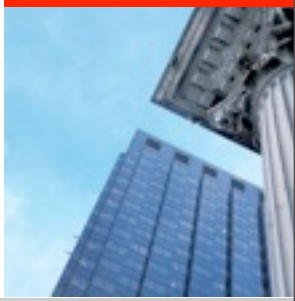
- WHERE
- WHO
- HOW
- PROTECTION

**> 90%**

**of our security problems**

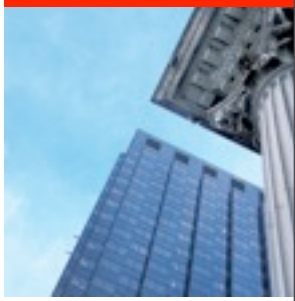
**could be solved !!!**

# 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 | Oracle Solution | Oracle Security Product |
|---|---|---|
| • External Attackers<br>• Internal Threats<br>• Image Damage<br>• Internal Security Regulations<br>• Regulatory Compliances<br>• ..<br>• . | • **Separation of duties**<br>• **Insider threat protection**<br>• **Strong access authentication**<br>• **Strong encryption (DB/OS/Net)**<br>• **Fine grained real time external auditing**<br>• **Data consolidation control**<br>• **High availability + Security combination** | • Advanced Security Options (ASO)<br>• Network encryption<br>• Transparent data encryption<br>• Strong authentication<br>• Database Vault<br>• Audit Vault<br>• Secure Backup<br>• Virtual Privat Database (VPD)<br>• Oracle Label Security (OLS)<br>• Data Masking<br>• Total Recall |

**Oracle Differentiator / no competition**

# Oracle Security Solutions Summary

## REPORTING & ALERTING

### IDENTITY AND ACCESS MANAGEMENT

| Identity Administration | Directory Services | Access Management |
|---|---|---|
| • User Provisioning<br>• Role Management<br>• Self-Service driven | • Scalable LDAP Storage<br>• Virtual Directory<br>• Directory Synchronization | • Risk-based Authorizat.<br>• Entitlements Managem.<br>• Single Sign-On<br>• Federation<br>• Inform. Rights Mgmt |

### DATABASE SECURITY

| Activity Monitoring | Access Control and Authorization | Encryption and Data Masking |
|---|---|---|
| • Unauthorized Activity Detection<br>• Automated Compliance Reports<br>• Secure Configuration Audit | • Privileged User Controls<br>• Multi-Factor Authorization<br>• Classification Control | • Transparent Data Encryption<br>• De-identification for Non-Production<br>• 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

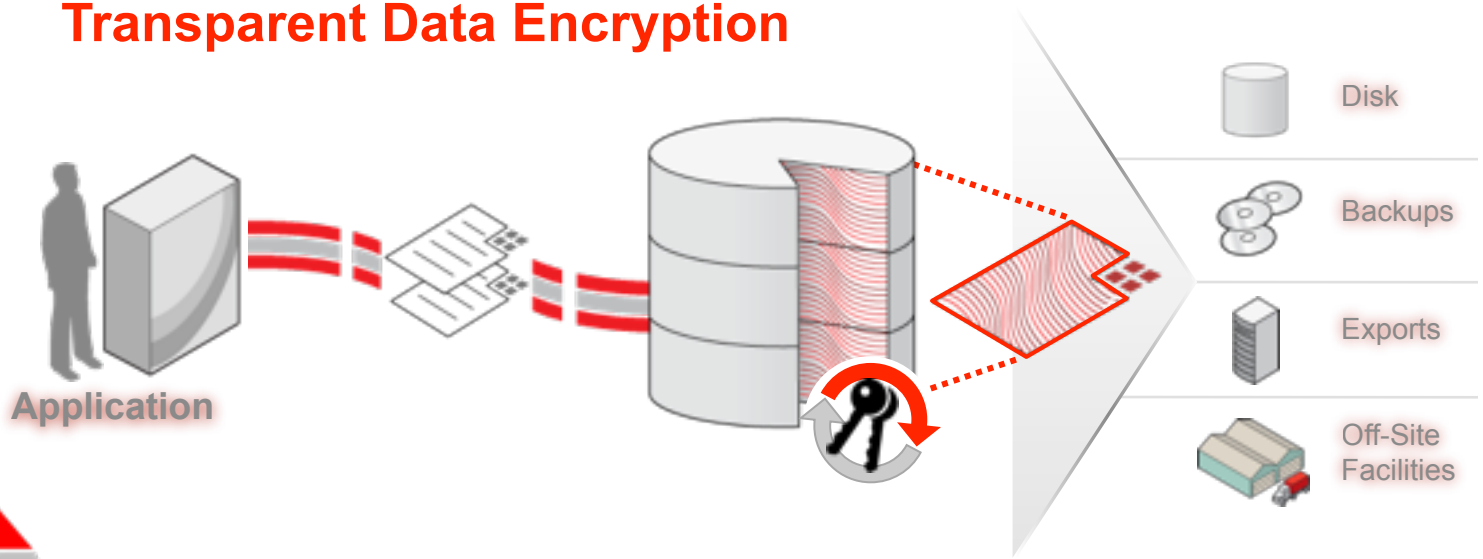
- Advanced Security
- Secure Backup
- Data Masking

# Security

ORACLE®

# Oracle Advanced Security

## Transparent Data Encryption

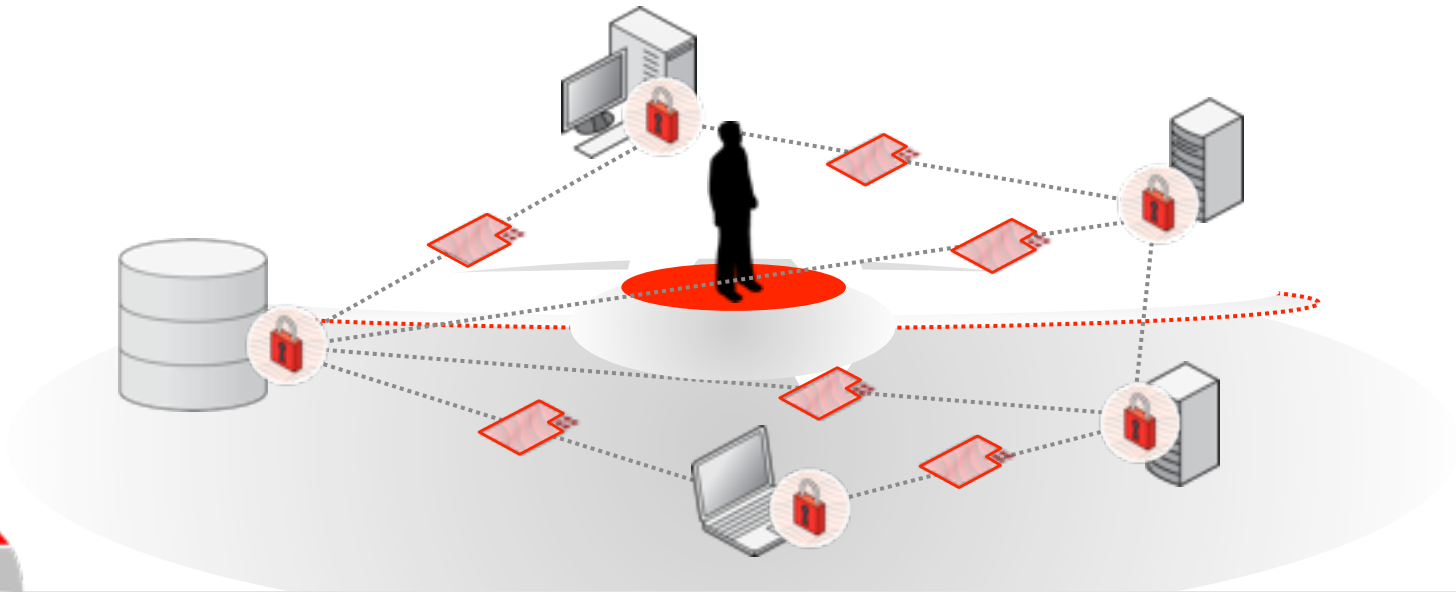




- Complete encryption for data at rest
- No application changes required
- Efficient encryption of all application data
- Built-in key lifecycle management

# Oracle Advanced Security

## Network Encryption & Strong Authentication



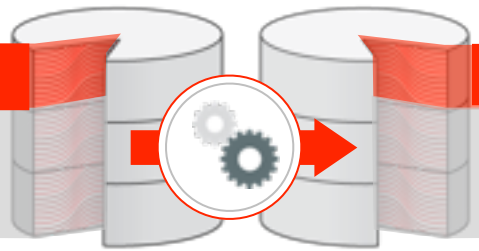

- Standard-based encryption for data in transit
- Strong authentication of users and servers (e.g. Kerberos, Radius)
- No infrastructure changes required
- Easy to implement

# Oracle Data Masking

## Irreversible De-Identification

**Production**

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



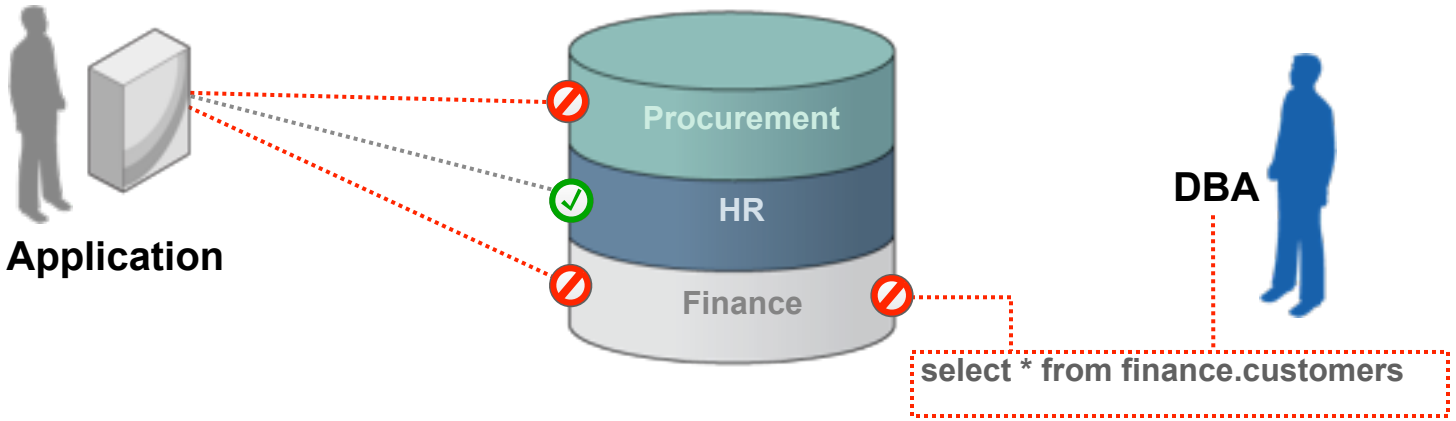
**Non-Production**

| 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 Database Vault

## Separation of Duties & Privileged User Controls

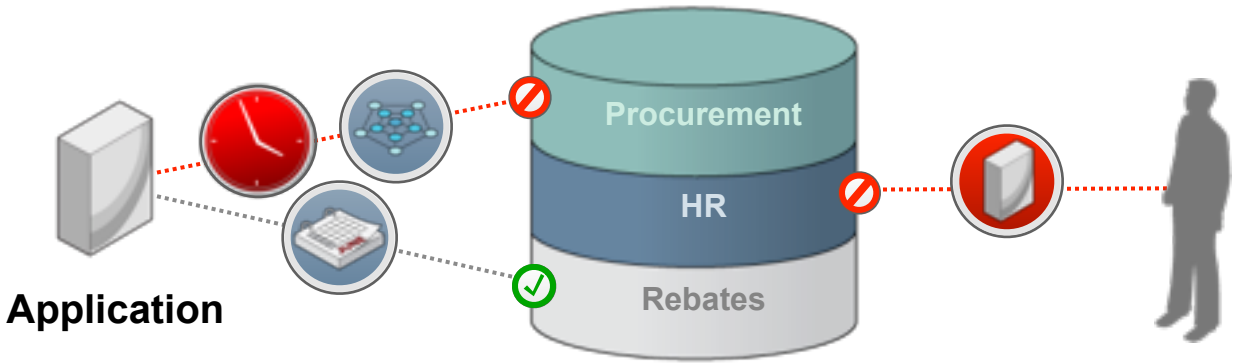




- DBA separation of duties
- Limit powers of privileged users
- Securely consolidate application data
- No application changes required

# Oracle Database Vault

## Multi-Factor Access Control Policy Enforcement

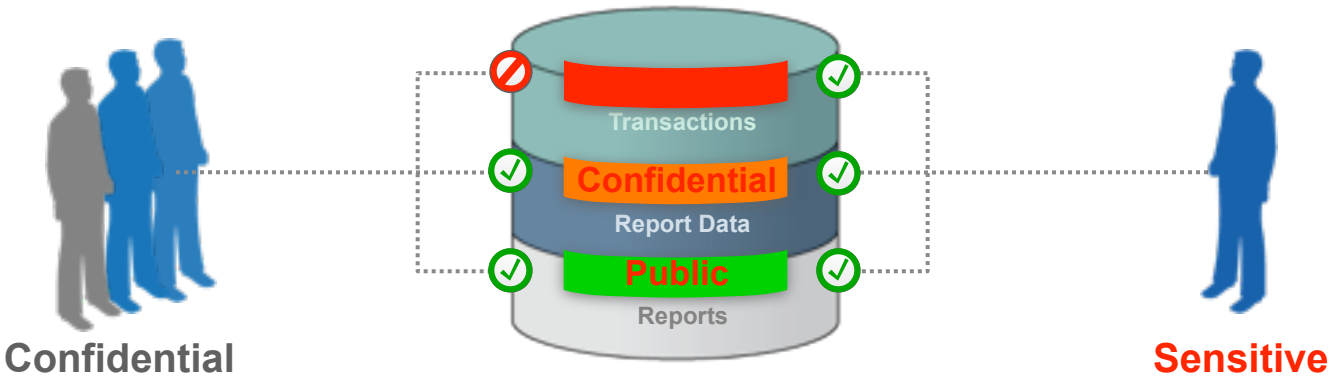




- Protect application data and prevent application by-pass
- Enforce who, where, when, and how using rules and factors
- Out-of-the box policies for Oracle applications, customizable

# Oracle Label Security

## Data Classification for Access Control

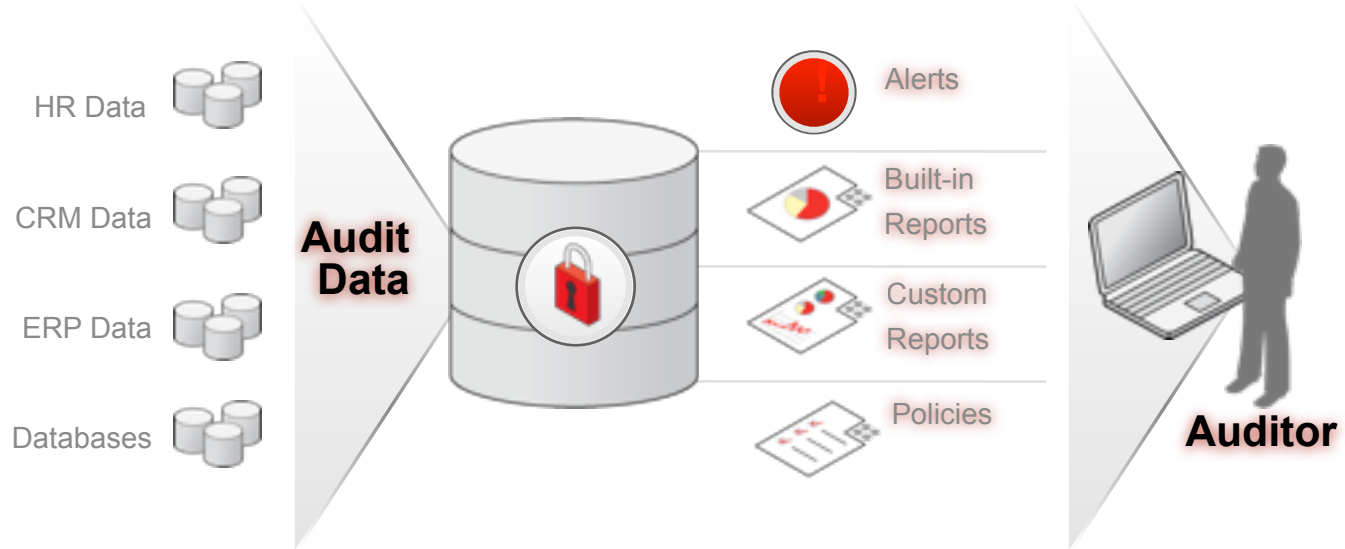




- Classify users and data based on business drivers
- Database enforced row level access control
- Users classification through Oracle Identity Management Suite
- Classification labels can be factors in other policies

# Oracle Audit Vault

## Automated Activity Monitoring & Audit Reporting



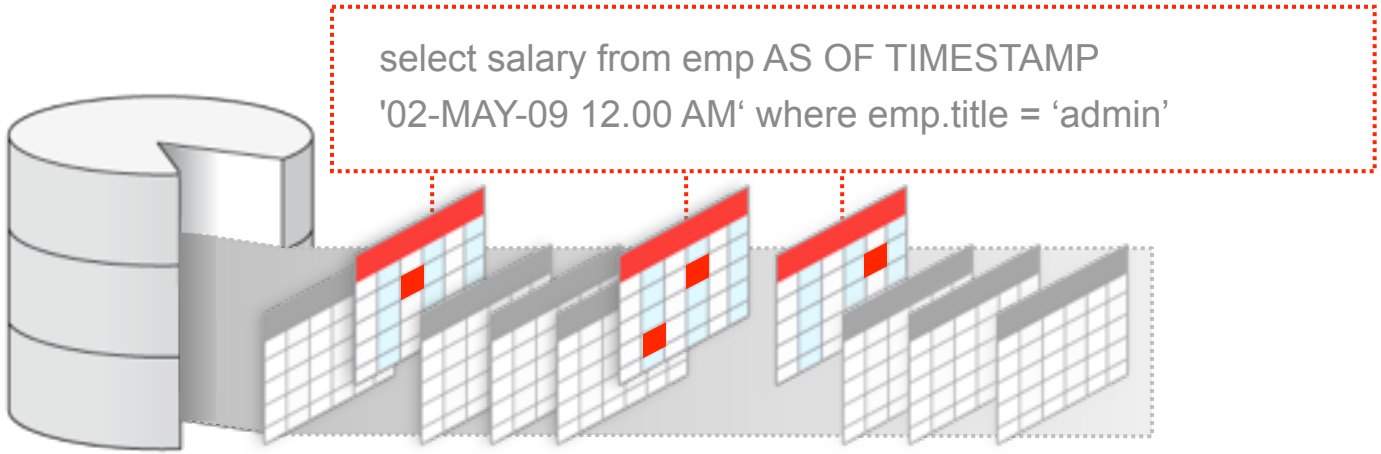


- Consolidate audit data into secure repository
- Detect and alert on suspicious activities
- Out-of-the box compliance reporting
- Centralized audit policy management

ORACLE IBM Microsoft SYBASE

# 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