RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

The Top 10 Database Breaches of the Past Year

Speaker：Noa Bar-Yosef
Job Title：Sr. Security Strategist
Company Name：Imperva

Agenda

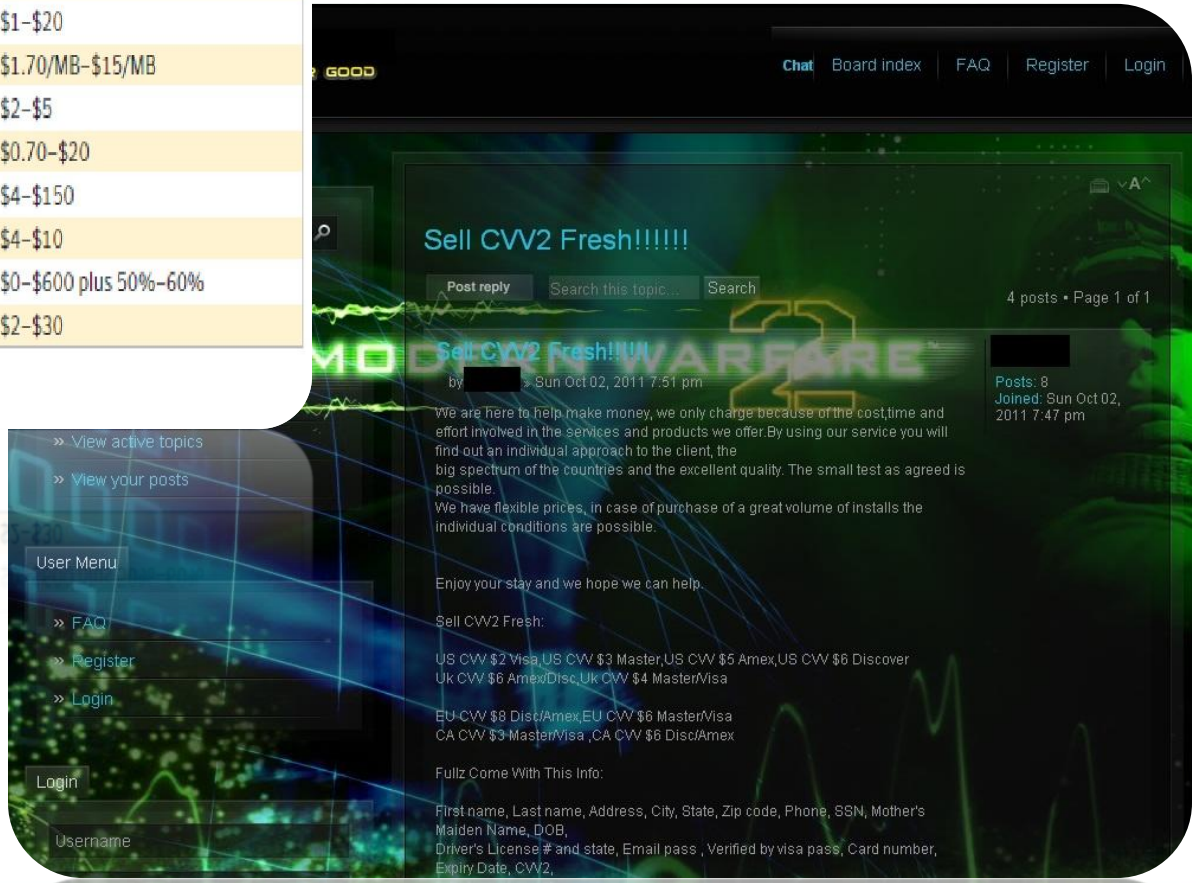
- Background
  - Databases are attractive targets
- Qualifying the problem 2009- 2011
- Top 10 database breaches of the past year
- Mitigation checklist

BACKGROUND

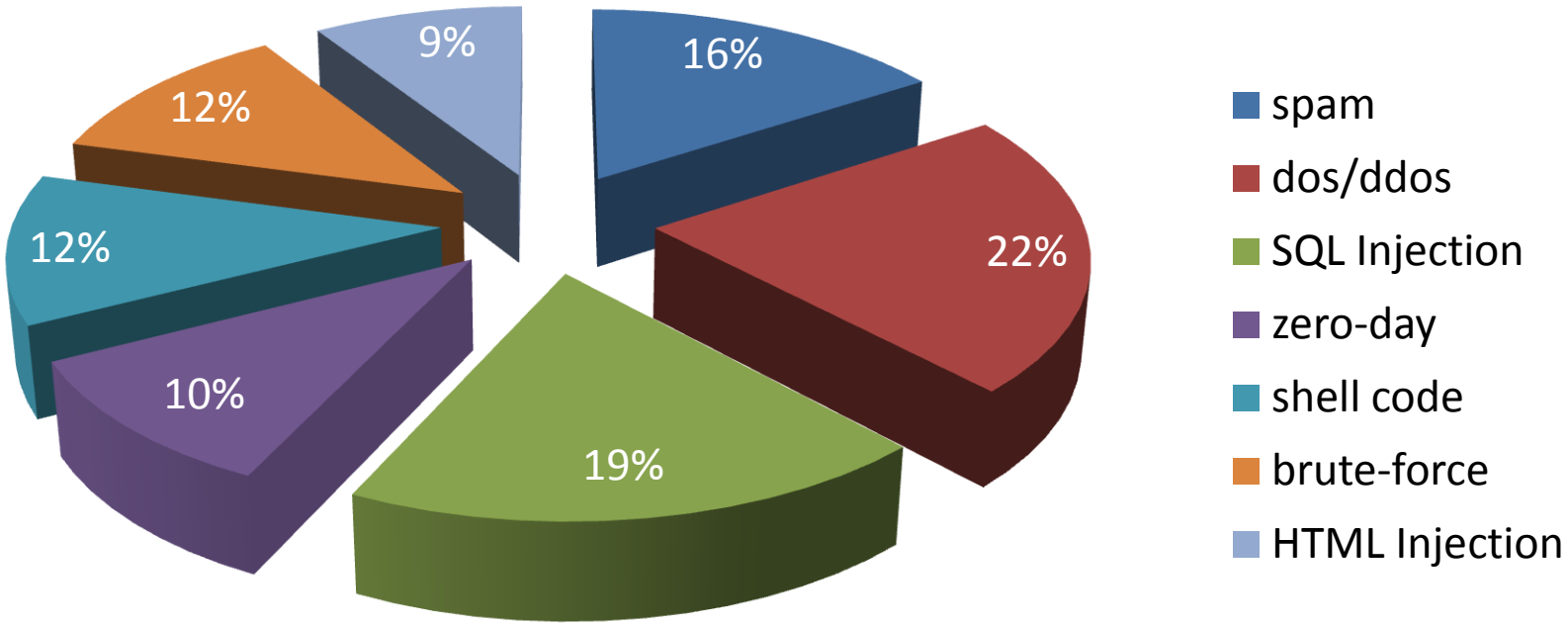
Data Has Value

Overall Rank 2009	Overall Rank 2008	Item	Percentage 2009	Percentage 2008	Range of Prices
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

Table 5. Goods and services advertised on underground economy servers
Source: Symantec

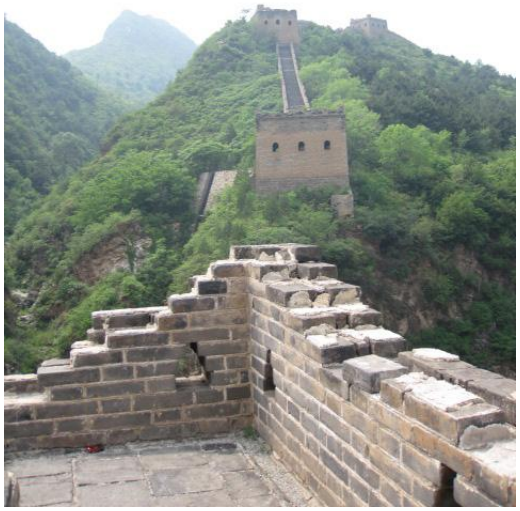


Data Has Value



Dates: July 2010 -July 2011

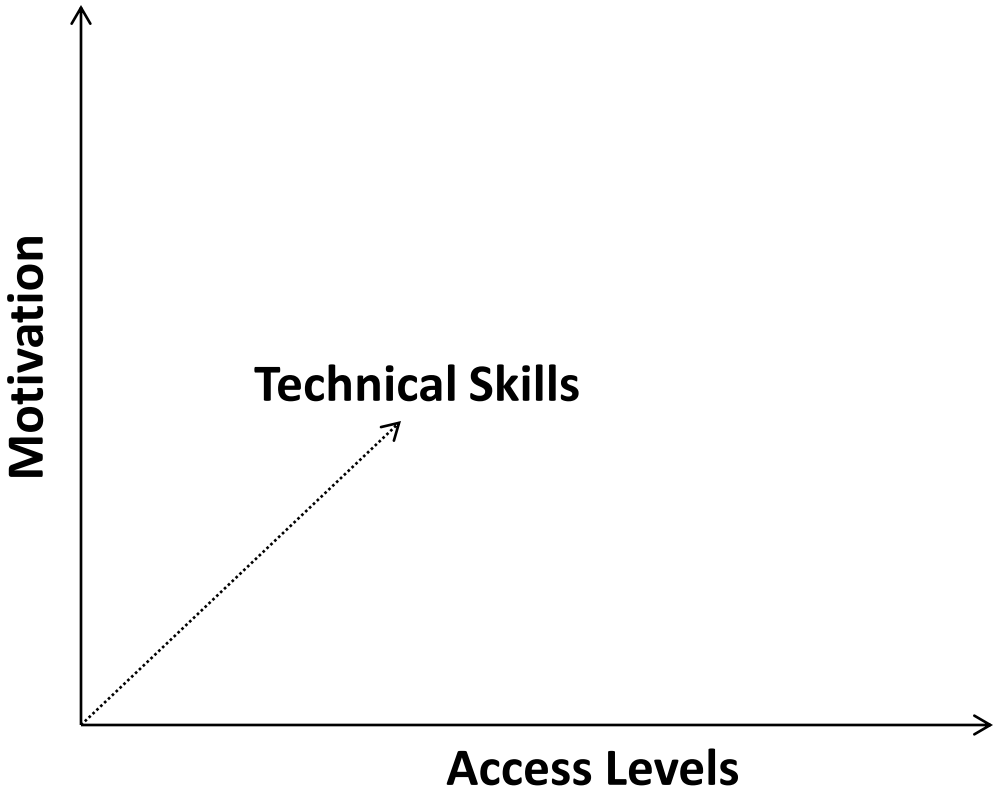
Human Nature at Work



- 70% of employees admit to accessing information they shouldn't
- 62% took data when the left
- 56% admit internal hacking
- 36% feel they own it

Source: February 2011 Shanghai and Beijing Street Survey of 1012 people, Imperva

Evaluating the Insider Threatscape

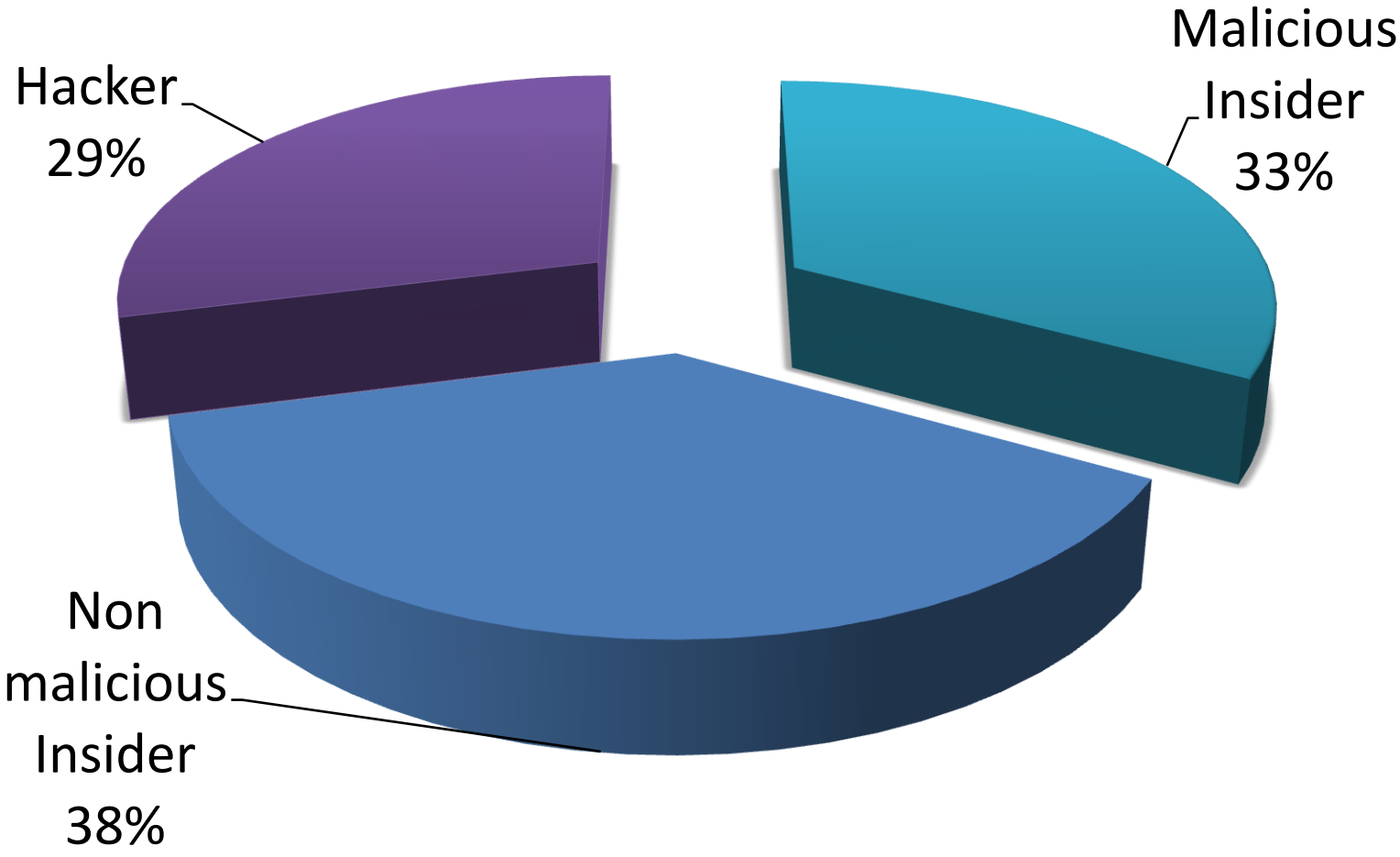


Motivations

- Accidental
- Coolness
- Ideology
- It's Mine
- Revenge
- Productivity
- Profit
- Curiosity
- Compromised Insider

IT Security Threat Perception

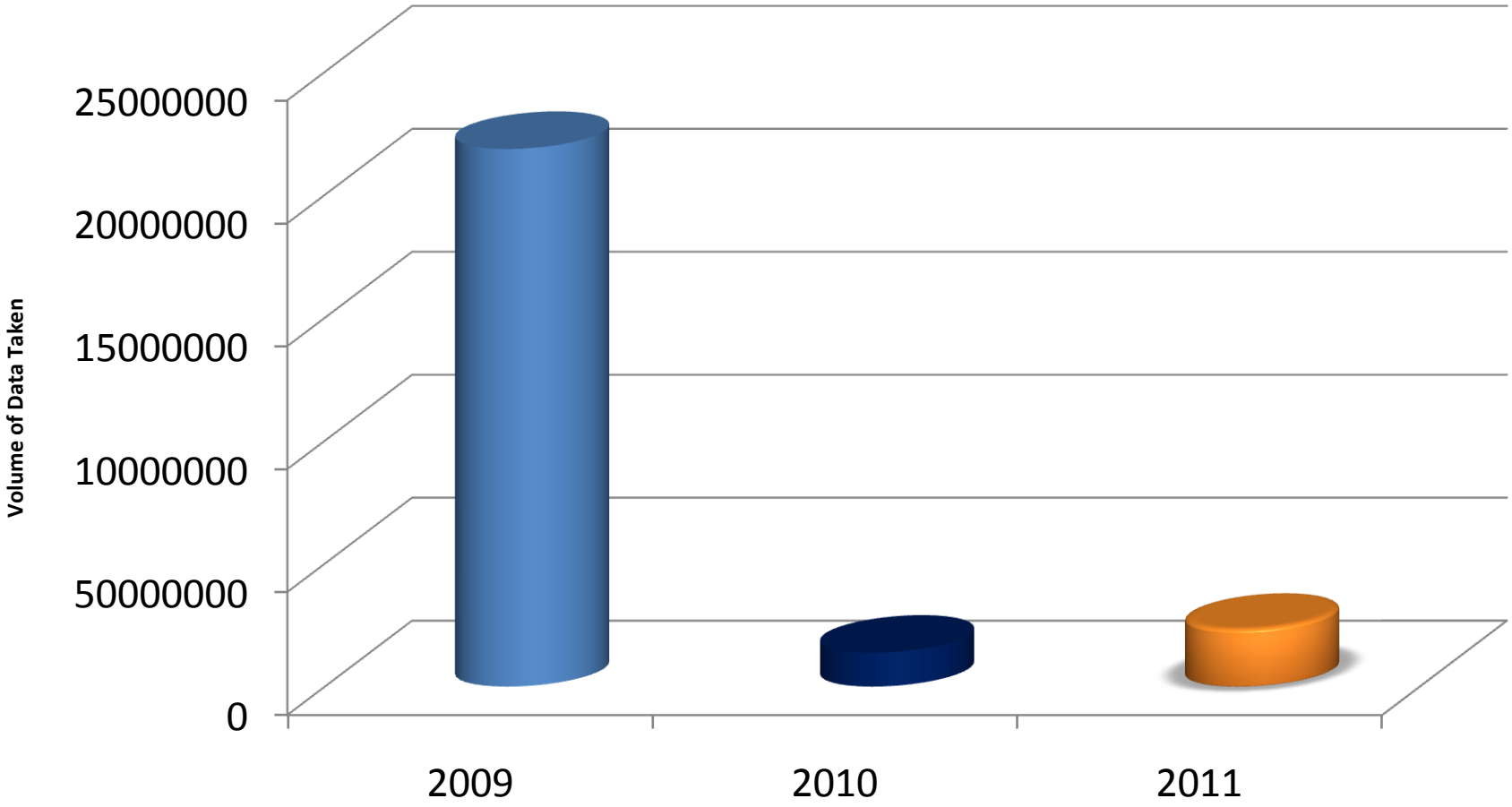
Global Survey of 1100 IT Security Professionals



Source: 2010 Securosis-Imperva survey of more than 1100 U.S. and multinational IT security practitioners. https://www.imperva.com/ld/data_security_survey.asp?

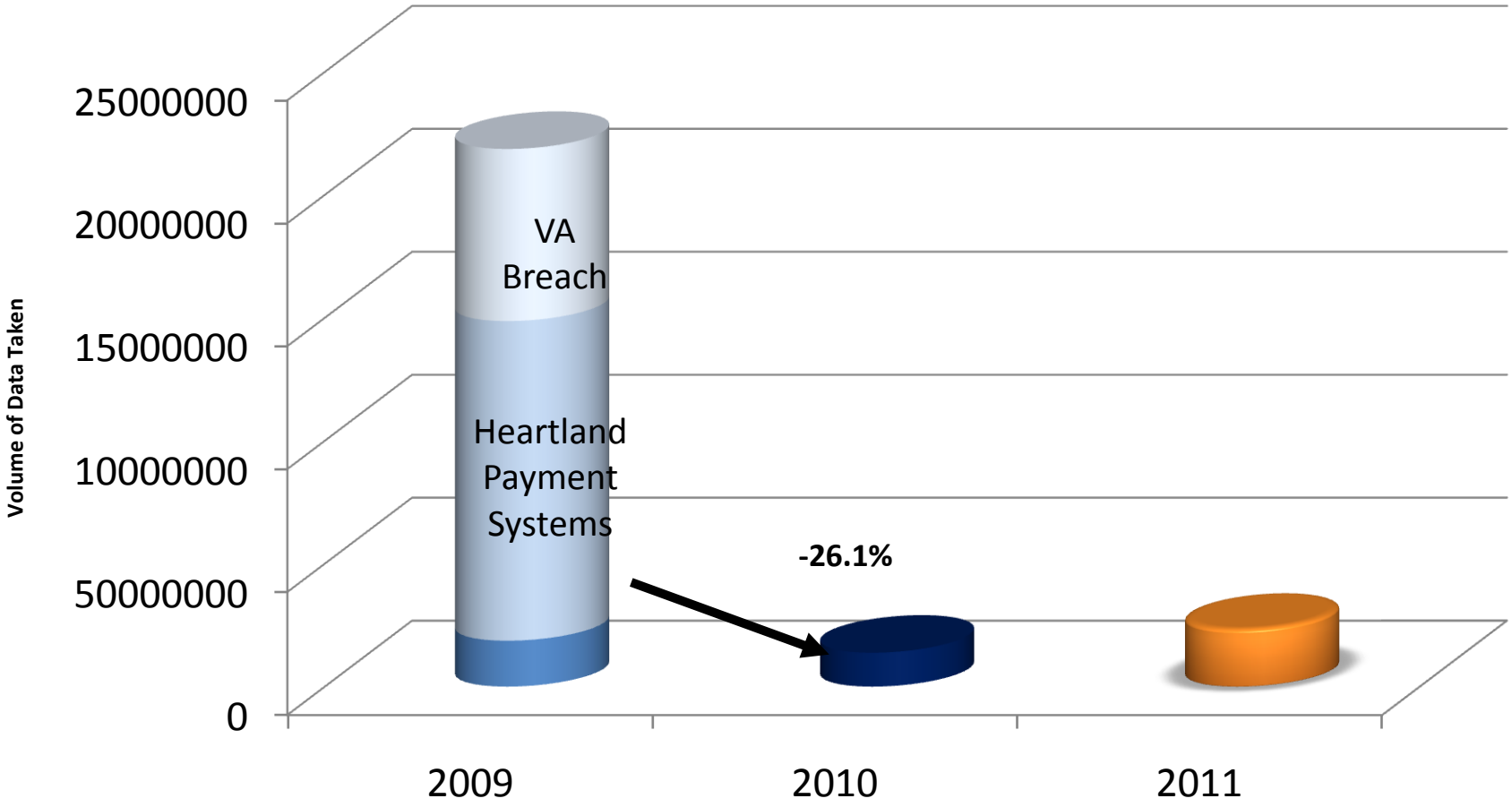
LOOKING BACK

Data Breach Volume: 2009- 2011



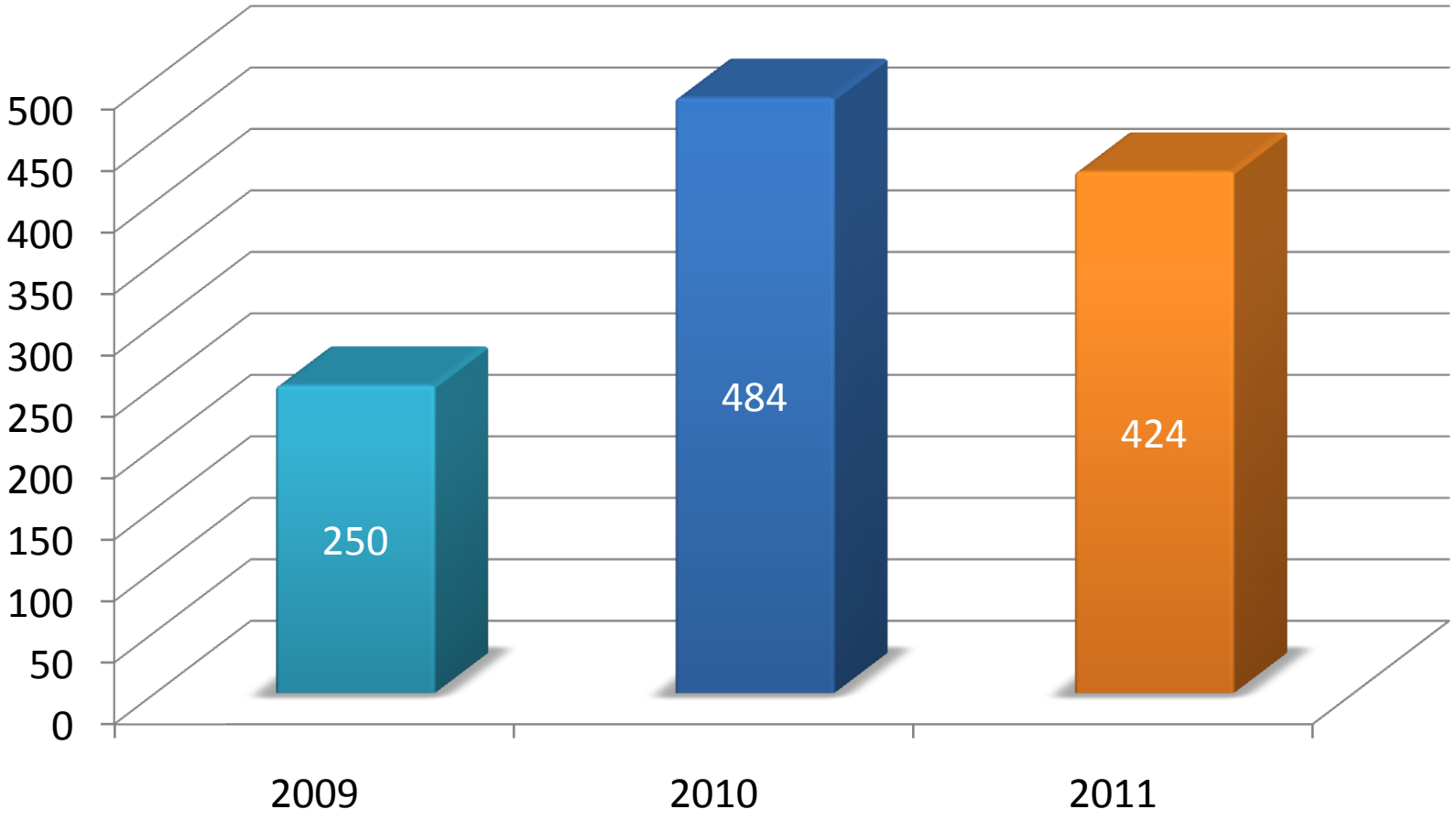
Source: http://www.privacyrights.org/data-breach

Data Breach Volume: 2009- 2011



Source: http://www.privacyrights.org/data-breach

Data Breach Incidents: 2009-2011



Source: http://www.privacyrights.org/data-breach

TOP 10 DATABASE BREACHES

Bank of America

#10

#10: The Details

- **The breach**
  - Size: About 300 records
  - Financial impact: $10M loss to Bank of America
  - Data stolen: Names, addresses, Social Security numbers, phone numbers, bank account numbers, driver's license numbers, birth dates, email addresses, mother's maiden names, PINs and account balances
- **Date:** May 2011
- **Source:** LA Times
- **Why Significant:** Illustrates excessive privilege abuse

Excessive Privilege Abuse

Definition

- Users (or applications) granted database access privileges in excess of “business need-to-know”

Analysis

- Hard to obtain a true list of required privileges
- Database ACL semantics are too limited

Consequence

- Any “minor” breach becomes a major incident!

#9

#9: The Details

- **The breach**
  - Size: Dozen celebrities
  - Financial Impact: $1M in fines paid by UCLA hospital
  - Data stolen: Jackson's medical information sold to the media by hospital staff (along with other celebrities).
- **Date:** July 2011
- **Source:** Mintz Levin (a legal blog)
- **Why Significant:** Abuse of legitimate privilege

Legitimate Privilege Abuse

Definition	• Abuse legitimate DB privileges for unauthorized purposes
Analysis	• Use simple and available desktop tools • Retrieve large quantities of data • Store sensitive data locally • Can make unauthorized changes
Consequence	• Data theft • Data loss • Embezzlement

Oak Ridge National Labs

#8

#8: The Details

- **Breach**
  - Size: Unknown
  - Financial Impact: Undisclosed, but high.
  - Data stolen: Military, government IP as well as data. Supercomputers shut down.
- **Date:** April 2011
- **Source:** Network World
- **Why Significant:** Privilege escalation courtesy spear phishing.

Privilege Elevation

Definition

- External entity or internal user maliciously gains excessive access bi vulnerability, poor password or stolen credentials.

Analysis

- Susceptible objects (Stored procedures and built-in functions, SQL statements)
- Types of vulnerabilities (Buffer overflow, SQL Injection)

Consequence

- A minor breach becomes a major incident
- Built-in access control becomes ineffective

Medical Records Leaked

#7

#7: The Details

- **The breach**
  - Size: 300,000 medical records
  - Financial impact: Unknown
    - Criminals: Blackmail and public humiliation.
    - Noncriminals: "The information can also be used by insurance companies to inflate rates, or by employers to deny job applicants."
  - Data stolen: comprehensive medical records
- **Source:** Chicago Tribune, September 2011
- **Why Significant:**
  - Foreshadows issues with broader digitization of electronic health records
  - Weak audit—Thought to be from a hospital outsourced partner

Weak Audit

Definition	• Audit policies that rely on built-in database mechanisms suffer a number of weaknesses
Analysis	• Let's talk about it…
Consequence	• Regulatory problems • Data is not there when you need it

Weak Audit

Performance degradation and DBA attention span

Knowing what matters in the mountain of audit data

Limited Granularity

Weak Audit

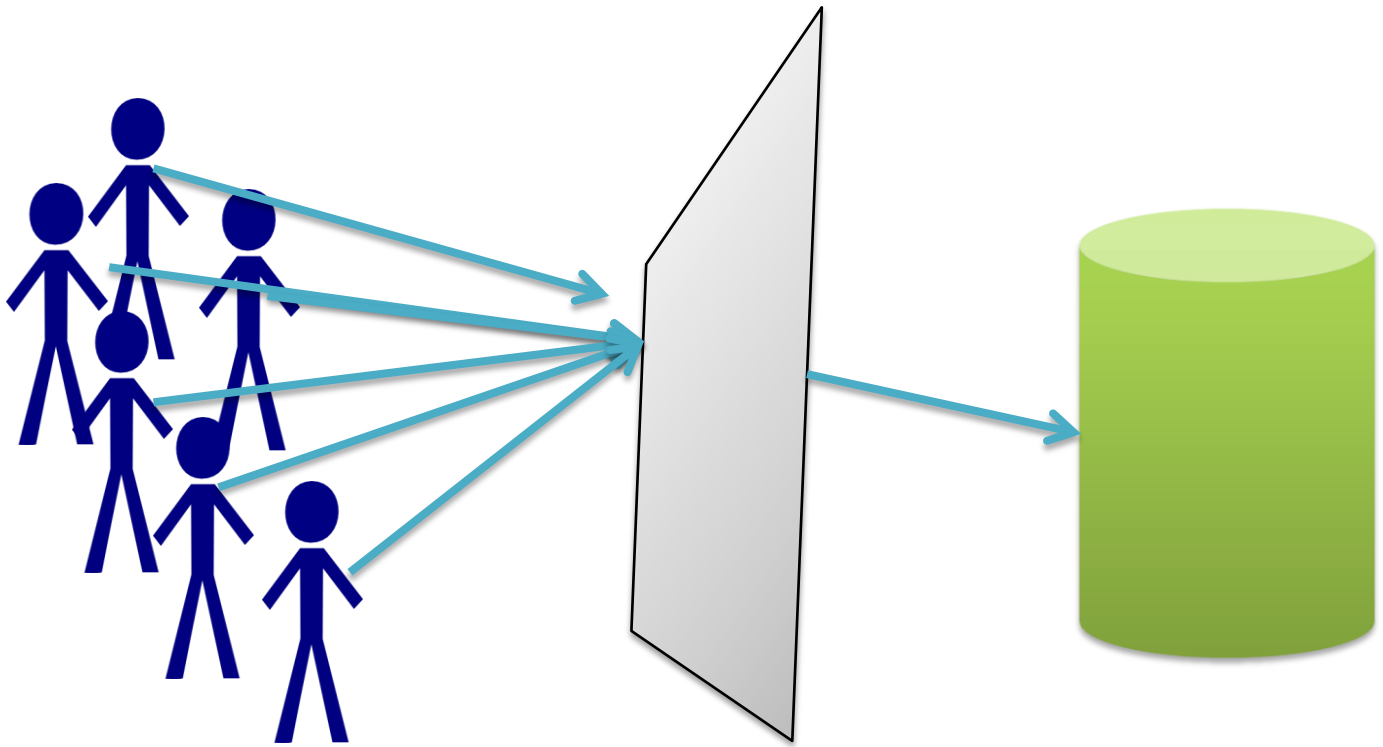
Proprietary

Vulnerable to database attacks

No End to End User-Tracking

Weak Audit

No End-to-End User Tracking



Groupon India

#6

#6: The Details

- The breach
  - Size: Groupon India publishes 300,000 user passwords
  - Financial Impact: Unknown
  - Data stolen: usernames and unencrypted passwords
- Date: June 2011
- Source: The Register
- Why Significant?
  - Google hacking

Publically Exposed Sensitive Data

Definition	• Sensitive data resides in “forbidden” locations (for example, on a Web- facing server)
Analysis	• Migration of data • Server mis-configurations
Consequence	• Data exposed to unauthorized users (and to world!)

#5

#5: The Details

- The breach
  - Size: Many employees locked out of systems due to changed passwords
  - Financial Impact: $17K
  - Data stolen: passwords changed
- Date: December 2010, sentenced January 2011
- Source: The Register
- Why Significant? Denial of service

Denial of Service

Definition	• Attacks that deny service availability to legitimate users
Analysis	• Vulnerabilities • Data tampering • Resource orientated
Consequence	• Critical for modern day organizations • Paralyzing the entire operation of an organization or part of it

#4

Dishonorable mention:
(loses 4.6M records on backup rive)

SAIC®
From Science to Solutions

#4: The Details

- The breach
  - Size: 1.6M records
  - Financial Impact: Unknown
  - Data stolen: addresses, dates of birth, NHS numbers and GP practice codes
- Date: September 2011
- Source: Public Service
- Why Significant? Backup data exposure

Backup Data Exposure

Definition	• Unencrypted data on Back-up Tapes and Disk
Analysis	• Many recent incidents where backup media is lost or stolen
Consequence	• Exposure of huge amounts of sensitive information

Bay House School in Hampshire

#3

#3: The Details

- The breach
  - Size: Undisclosed
  - Financial Impact: Unknown
  - Data stolen: personal details of pupils, including addresses, photographs and sensitive medical information
- Date: August 2011
- Source: Computer Weekly
- Why Significant? Weak authentication

Weak Authentication

Definition

- Weak account names and/or passwords

Analysis

- Account name often adhere to some organizational standard (e.g. John.Smith, Jane.Doe, JSmith, J.Doe)
- Bad (or rather predictable) choice of passwords by users

Consequence

- Credential theft
- Brute force attacks are feasible

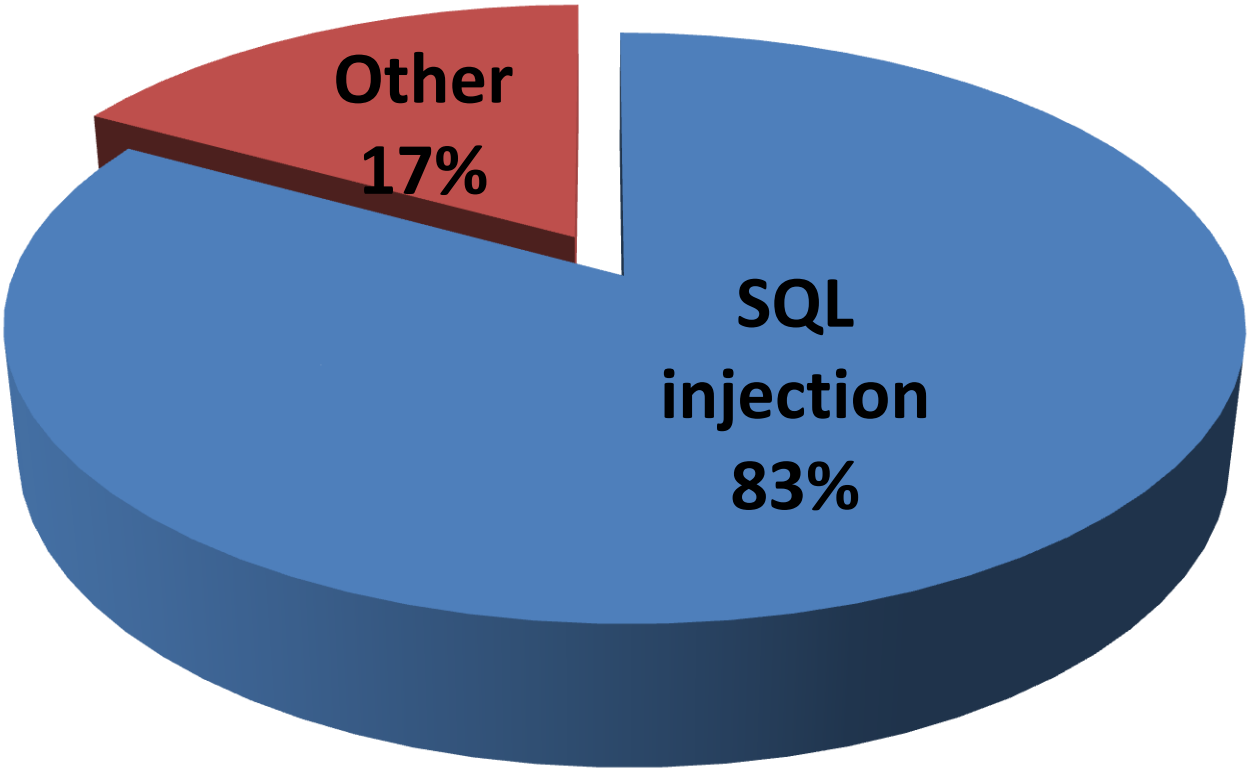
Sony

&

Military, Government Websites

Tie for #1

Reason for Data Loss from Hacking: 2005- 2011



Total=315,424,147 records
(856 breaches)

#1a: Military, Government Websites

Website Hacking
LR ID: [redacted]

Offers | Services | Proofs | Free Logins | Payment method

Site	Details	Level of Control	Traffic	Price
http://gs.mil.al/	ARMY Forces of republic of albania	Full SiteAdmin Control + High value informations	unknown	$499
http://www.scguard.army.mil/	Souce Carolina National Guard	MySQL root access + High value informations	unknown	$499
http://cecom.army.mil/	The United States Army | CECOM	Full SiteAdmin Control/SSH Root access	unknown	$499
http://pec.ha.osd.mil/	The Department of defense pharmacoeconomic Center	Full SiteAdmin Control/Root access, High value informations!	unknown	$399
http://www.woodlands.edu.uy/	Wooldlands School Uruguay.	Full SiteAdmin Control!	5200	$33
http://s-u.edu.in/	Singhania University	Full SiteAdmin Control.	unknown	$55
http://www.nccu.edu.tw/	National Chengchi University.	Students/Exams user/pass and full admin access!	56093	$99
http://www.terc.tp.edu.tw/	Taipei City East Special Education Resource Center	Full SiteAdmin Control.	74188	$88
http://itcpantaleo.gov.it/	Italian Official Government Website.	Full SiteAdmin Control.	292942	$99
http://donmilaninapoli.gov.it/	Istituto Statale Don Lorenzo Milani	Full SiteAdmin Control.	292942	$99
http://itcgcesaro.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	$99
http://itimarconi.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	$99
http://primocircolovico.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	$99
http://www.utah.gov/	American State of Utah Official Website.	Full SiteAdmin Control.	173146	$99
http://www.uscb.edu/	University of South Carolina Beaufort.	Full SiteAdmin Control.	1123	$88
http://michigan.gov/	American State of Michigan Official Website.	MySQL root access/Valuable information.	205070	$55

- Daily updated -
Click here to check for proof of the hacked sites.

Email me or add me in MSN at [redacted]@gmail.com

#1a: The Details

- The breaches
  - Size: Dozens of websites for sale
  - Financial Impact: Unknown, several sites down
  - Data stolen: Admin login
- Date: January 2011
- Source: http://krebsonsecurity.com/2011/01/ready-for-cyberwar/
- Why Significant? SQL injection gives birth to a business.

How Do You Spell APT?

"Amid all of the media and public fascination with threats like Stuxnet and weighty terms such as "cyberwar," it's easy to overlook the more humdrum and persistent security threats, such as Web site vulnerabilities. But none of these distractions should excuse U.S. military leaders from making sure their Web sites aren't trivially hackable by script kiddies."

—Brian Krebs

#1b- Sony: The Details

- The breaches
  - Size: 100M (12M unencrypted)
  - Financial Impact: $172M and counting
  - Data stolen: credit card information
- Date: April 2011
- Source: Reuters
- Why Significant? SQL injection takes down a company.

Need to Justify the Cost of Security?

SQL Injection

Definition	• Attacker inserts an unauthorized SQL statement through a SQL data channel
Analysis	• Caused by non-validated input parameters
Consequence	• Access to unauthorized data • Unauthorized data manipulation • Denial of service • Privilege elevation

BEST PRACTICES

Checklist for Mitigating Database Breaches (1)

- Monitor access to the database
  - Find the data to focus on
    - Map the organization's databases
    - Drilldown and pinpoint those database tables which contain sensitive information
  - Set up policies to detect abusive or unauthorized access.
    - A combination of:
      - Black-listing (defining attack patterns, setting up corporate policies)
      - White-listing (all allowed behavior)
  - Setting up an audit trail policy
    - Static policies (i.e. recording all changes to the database structure, retrieval activities of sensitive data, access by users from the IT department)
    - Dynamic log policies (policies triggered by an unusual event)

Checklist for Mitigating Database Breaches (2)

- Ensure application and database security
  - Identify and block external attacks targeted at the application
  - Apply the latest patches
    - Use virtual patching to minimize the window of exposure
- Enforce segregation of duties
  - Make sure who's watching the watchdogs
  - Some parts of the monitoring solution must be implemented outside the control of a single database or system administrator

Checklist for Mitigating Database Breaches (3)

- Avoid careless distribution of sensitive data
  - Detection policies to depict the move of sensitive data to public-facing servers
  - Regularly schedule “clean-ups”
  - Periodically look for new databases that hold sensitive data
  - Perform data masking on production data before delivering it to QA or engineering
- Reduce the amount of stored sensitive data

Checklist for Mitigating Database Breaches (4)

- Periodically assess user and access management
  - Identify and remove excessive rights
    - For example, access privileges to sensitive objects granted to all users, administrative privileges granted to non-administrators
    - Correlate the access control information with the organizational role of individuals
  - Enforce proper authentication policies
    - Strong passwords across enterprise systems.
    - Two factor authentication
  - Clean up unused (dormant) accounts and privileges
    - Include: correlating between existing account and privileges and actual usage
- Encrypt backup data
  - Data taken directly from the database or data encrypted on the user's end-machine

QUESTIONS?

THANK YOU!