# Securing Data

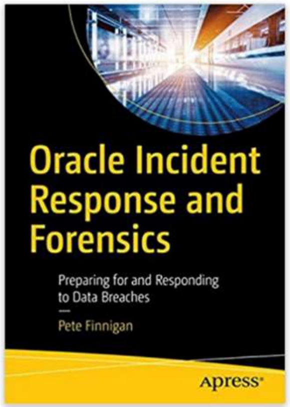
# Legal Notice

## Securing Data

Published by
PeteFinnigan.com Limited
Tower Court
3 Oakdale Road
York
England, YO30 4XL

**Limit of Liability / Disclaimer of warranty**. This information contained in this course and this material is distributed on an “as-is” basis without warranty. Whilst every precaution has been taken in the preparation of this material, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions or guidance contained within this course.

**TradeMarks.** Many of the designations used by manufacturers and resellers to distinguish their products are claimed as trademarks. Linux is a trademark of Linus Torvalds, Oracle is a trademark of Oracle Corporation. All other trademarks are the property of their respective owners. All other product names or services identified throughout the course material are used in an editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this course.


Oracle Incident Response and Forensics
Preparing for and Responding to Data Breaches
Pete Finnigan
apress

# Pete Finnigan – Background, Who Am I?

- Oracle Security specialist and researcher
- CEO and founder of PeteFinnigan.com Limited in February 2003
- Writer of the longest running Oracle security blog
- Author of the Oracle Security step-by-step guide and “Oracle Expert Practices”, “Oracle Incident Response and Forensics” books
- Oracle ACE for security
- Member of the OakTable
- Speaker at various conferences
  - UKOUG, PSOUG, BlackHat, more..
- Published many times, see
  - http://www.petefinnigan.com for links
- Influenced industry standards
  - And governments

# Agenda

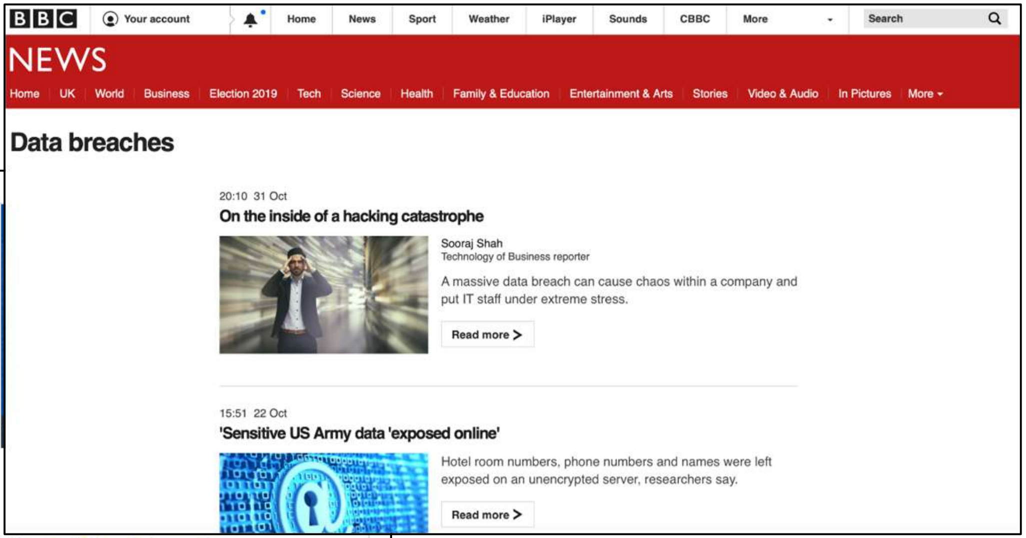
- Data Security landscape
- The focus on data security
- History of securing Oracle
- Current data and Oracle Security landscape
- Main threats to Oracle databases
- The focus in fixing database security
- **Secure your data or BUST**

# Data Security Landscape

# Hacking And Data Theft

I had a conversation with a taxi driver recently and he didn’t know what a data breach was BUT proceeded to tell me how he was scammed out of a loan payment. His identity was stolen and he paid a loan repayment but never got any money

- Data security is not a niche subject anymore
- The BBC even has a dedicated breach page
- Experts no longer wheeled in to discuss a breach
- **It is main stream**



Data breaches

20:10 31 Oct

On the inside of a hacking catastrophe

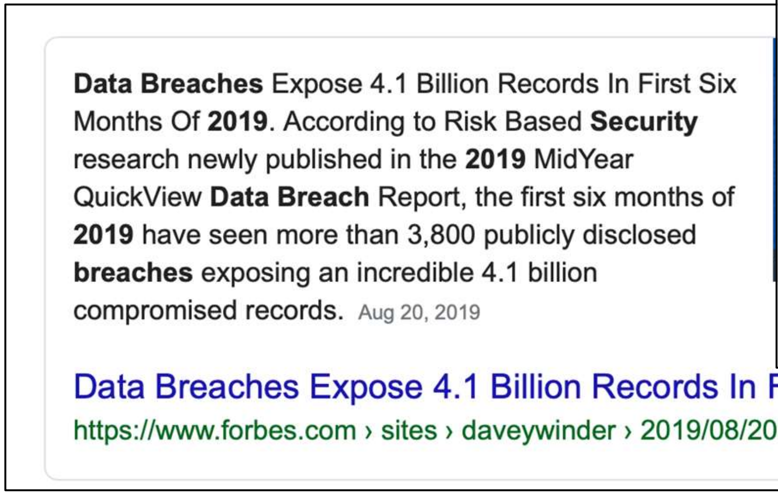
Sooraj Shah
Technology of Business reporter

A massive data breach can cause chaos within a company and put IT staff under extreme stress.

15:51 22 Oct

'Sensitive US Army data 'exposed online'

Hotel room numbers, phone numbers and names were left exposed on an unencrypted server, researchers say.



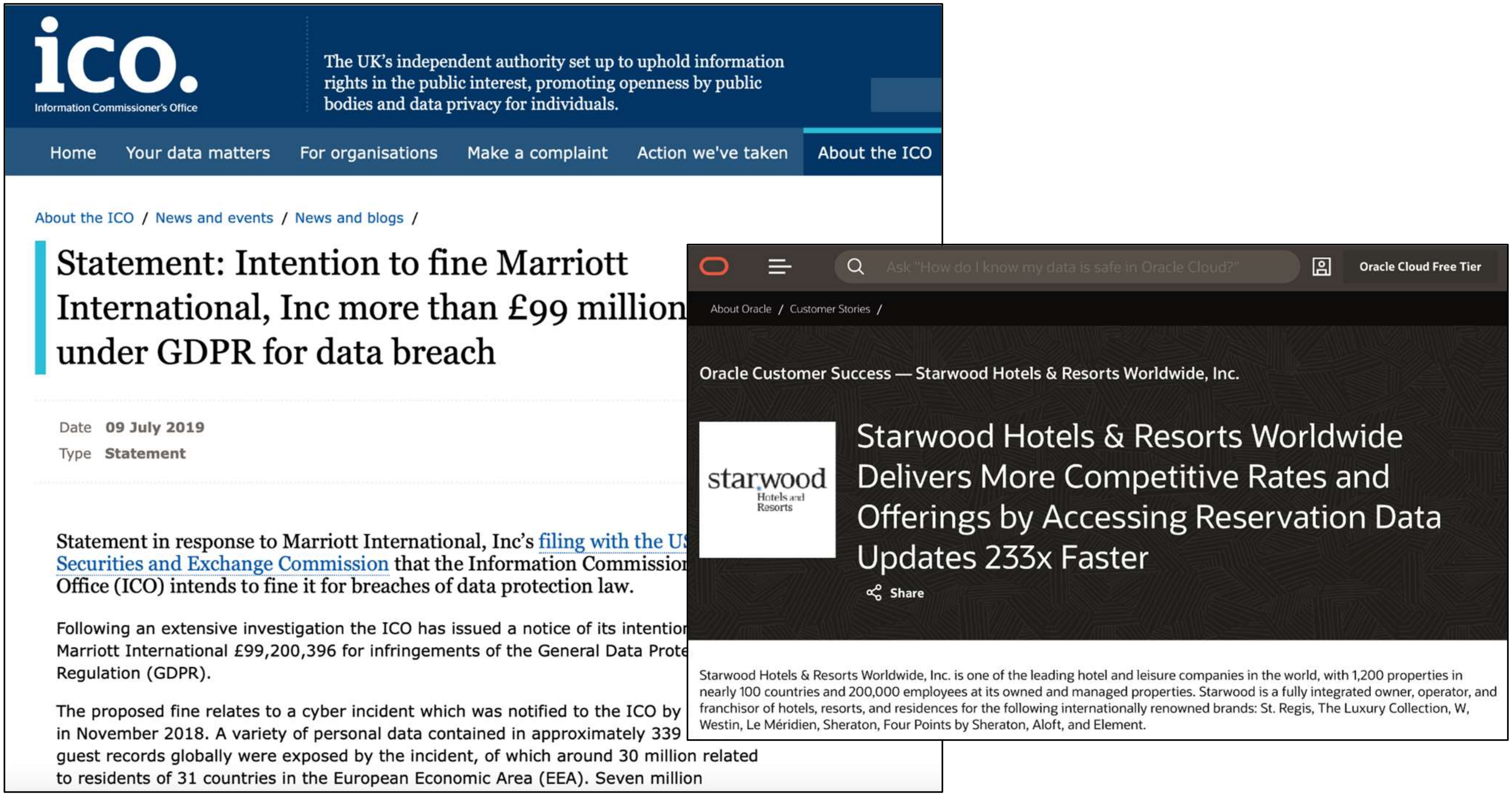
**Data Breaches** Expose 4.1 Billion Records In First Six Months Of **2019**. According to Risk Based **Security** research newly published in the **2019** MidYear QuickView **Data Breach** Report, the first six months of **2019** have seen more than 3,800 publicly disclosed **breaches** exposing an incredible 4.1 billion compromised records. Aug 20, 2019

Data Breaches Expose 4.1 Billion Records In First Six Months ...
https://www.forbes.com › sites › daveywinder › 2019/08/20 › data-breaches-...

# Major Fines

What about the other 27 EU States + the rest of the world who lost their data (339 Million records lost) – More fines?

# Large Fine by ICO - Marriot



ico.
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

About the ICO / News and events / News and blogs /

## Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach

Date 09 July 2019
Type Statement

Statement in response to Marriott International, Inc's filing with the US Securities and Exchange Commission that the Information Commissior Office (ICO) intends to fine it for breaches of data protection law.

Following an extensive investigation the ICO has issued a notice of its intentior Marriott International £99,200,396 for infringements of the General Data Prote Regulation (GDPR).

The proposed fine relates to a cyber incident which was notified to the ICO by in November 2018. A variety of personal data contained in approximately 339 guest records globally were exposed by the incident, of which around 30 million related to residents of 31 countries in the European Economic Area (EEA). Seven million

About Oracle / Customer Stories /

Oracle Customer Success — Starwood Hotels & Resorts Worldwide, Inc.

## Starwood Hotels & Resorts Worldwide Delivers More Competitive Rates and Offerings by Accessing Reservation Data Updates 233x Faster

Starwood Hotels & Resorts Worldwide, Inc. is one of the leading hotel and leisure companies in the world, with 1,200 properties in nearly 100 countries and 200,000 employees at its owned and managed properties. Starwood is a fully integrated owner, operator, and franchisor of hotels, resorts, and residences for the following internationally renowned brands: St. Regis, The Luxury Collection, W, Westin, Le Méridien, Sheraton, Four Points by Sheraton, Aloft, and Element.

# The Rise of Hacking

# In The Beginning We have Bragging Rights

- Phiber Optik – Mark Abene – Masters of Deception – Legion of Doom - https://en.wikipedia.org/wiki/Mark_Abene
- Erik Bloodaxe – Chris Goggans – Legion of Doom – editor of Phrack - https://en.wikipedia.org/wiki/Erik_Bloodaxe_(hacker)
- The great Hacker War – 1990/91 - https://en.wikipedia.org/wiki/Great_Hacker_War - Phiber Optik stated it was a fabrication by US Government
- 2600 Emanuel Goldstein - Ed, Captain Crunch, Hackerdom, Defcom…
- Kevin Mitnik – The Darkside, The Condor.. The most wanted man - https://en.wikipedia.org/wiki/Kevin_Mitnick - A judge thought he could start a nuclear war by whistling into a pay phone!
- Solo – Gary McKinnon – accused of the biggest military hack of all time - https://en.wikipedia.org/wiki/Gary_McKinnon - Free energy suppression and UFO cover-ups! – perl for blank/ default passwords

# Snowdon and NSA Tools – Government Hacking

- Edward Snowdon – copied and leaked CIA, NSA highest level data in 2013 - https://en.wikipedia.org/wiki/Edward_Snowden and ran to Hong Kong and then Russia.
  - Leaked details of government level hacking, global surveillance, cyber attacks, tools and much more
  - The key point for us is that he had "virtually unlimited access to data" and was able to exfiltrate 50,000 to 200,000 files / records
  - Created the NSA backup system!
- Julian Assange - in the Equador embassy from 2012 to 2019 – wiki leaks – but also hacker in 1987 hacking as Mendax - https://en.wikipedia.org/wiki/Julian_Assange - hacking US government and Pentagon
- NSA hacking tools hacked - http://thehackernews.com/2016/12/nsa-hack-shadow-brokers.html - can be downloaded for free

Hacking team purchased by InTheCyber in April 2019 to become Memento Labs

## Hacking Team – Hacking tools Hacked and for Sale

- Hacked in July 2015
- Phineas Fisher – pseudo name – hacked “Hacking Team” with over 100 hours of effort – **He was never found**
- 400gb of emails, documents, embarrassing information and most importantly the hacking toolkit **Remote Control System (RCS)** they sell to countries stolen
- Posted to Pastebin with details of how the hack happened - http://pastebin.com/raw/0SNSvyjJ - (removed)
- 0-Days used, found a Blackberry password and then accessed to a domain server allowed all other user passwords to be found in email. Then Fisher found a sysadmins email to get a github password for source code and bridge to the internal dev network

# The Data Gold Rush

# Data Gold Rush

- Data is the new gold – think 1896 to 1899 klondike in the Yukon
  - Usage patterns
  - User and customer behaviour
  - Company data
  - Tracking data – all GDPR
- Companies are starting to realise the importance of data
- Social media is massive
- Data driven advertising
  - Facebook, Google, Snowden and the NSA!
- Cultivated data is the way forwards
  - Not necessarily massive computing power and big data
  - Not always volume and velocity of data

# Pure Data Crime

# Criminals Steal Data – It is Easier Than Violence

- There is a major upsurge in data theft now
- It is safer for criminals to steal data than to walk into a bank with a sawn off shotgun
- It is not about bragging rights anymore
- Hard to know if Oracle is involved in each data theft case
- There is a ready market for stolen data on the dark web
- Breaches listed (some) at http://www.breachlevelindex.com
- ICO summary of data breaches - https://ico.org.uk/action-weve-taken/data-security-incident-trends/ - e.g. Bounty UK fined £400,000 – not extensive list
- **I personally have been involved in post breach investigations against quite a few Oracle based systems**

# The Rise of The Empire

- See https://gdpr-info.eu for details
- Also USA data breach notification laws (1386), Sox, GLB, Hippa
- £20M fine or 4% of Company GDP

# GDPR

- General Data Protection Regulation (GDPR) (Regulation EU  2016/679)
- Replaces the data protection derivative 95/46/EC in 1995
- Adopted by EU 27 April 2016
- Enforced from 25th May 2018
- Does not require national governments to pass any enabling legislation so was binding straight away in May 2018
- Each member state established a Supervising Authority (SA)
- Authority in the UK is the ICO (Information Commissioners Office)

# Section

## History of Locking Down

# Brief History Of Locking Down Oracle

- When I started to secure Oracle there were “no” or next to “no” books, papers, tools or security patches
- No one else was specializing in Oracle security in the database that I knew of
- Then in 2001 I was asked to write the SANS Oracle step-by-step guide
  - This also lead to the SANS S.C.O.R.E
  - SANS donated the book to CIS for the first Oracle benchmark

# Database Security 22 Years Ago

- Companies were interested in data security BUT
  - Lack of budgets for most companies (desktop/network)
- Legacy thinking
  - Functionality / SLA
  - Not security of Oracle or data in Oracle
- Tendency to think that its someone else's issue; OS, Network, Firewalls etc; **just not the Oracle database**
  - My experience from 1999 was an audit by KPMG / Delloite
  - Just file permissions of the Oracle software, no actual database settings, parameters, users etc
- **I decided to do better**

# Section

## Oracle Security Options

# Security Options

- Oracle (the database) security features are immense:
  - Parameters and privileges on everything
  - Audit trails and lockdown profiles
  - User profiles and more
- Core security options must be done first (come back to that in a minute)
- SE, EE all include core security features
- Oracle sell security in cost options

Third party security solutions are also available (for a cost)

# Additional Security Cost Options - Usually Not Free

- Database Vault – primary tool to protect against privilege accounts and to put realms around data/function
- Oracle Label Security - Allows data to be accessed by row level labels and the users current label access level
- Data Redaction (ASO) – Redact some data from end users – black like through data!
- Transparent Sensitive Data Protection – create classes of sensitive data to allow more centralised way of protecting sensitive data – uses VPD and Data Redaction
- Transparent Database Encryption – allows data to be encrypted at rest – either at tablespace level or at the column level
- Oracle Data Masking – find data to mangle / obfuscate and specify rules to then change that data – keeping referential integrity
- Audit Vault and Database Firewall– centralised database for audit storage including certificate based confirmation of data

# Secure The Core Database

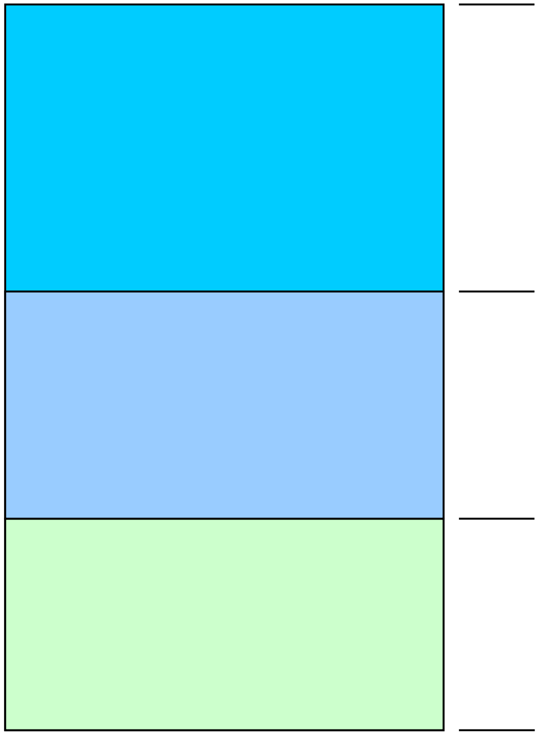
- Secure the core database first using std features
- **A security option from Oracle is just an application**
- The cost option (application)
  - Must be configured for your ideas / use. OOTB they usually do not do what you want
  - Security option must be secured as well
    - The interfaces, API, metadata, custom code
    - i.e. in VPD if you make the predicate function public anyone can run it or if a user has ALTER SYSTEM then can set events 10060 or 10730
- We can simulate cost options for free

PFCL
PETEFINNIGAN.COM LIMITED

# Current Data and Oracle Security Landscape

# My Current Security State of Oracle Databases

- My current experience of the state of Oracle database security can be summed up below.



100% No one is at this state of security

60% Small Number are here

30% Most people are in this area

0% No one is here either

# Oracle Security in 2023

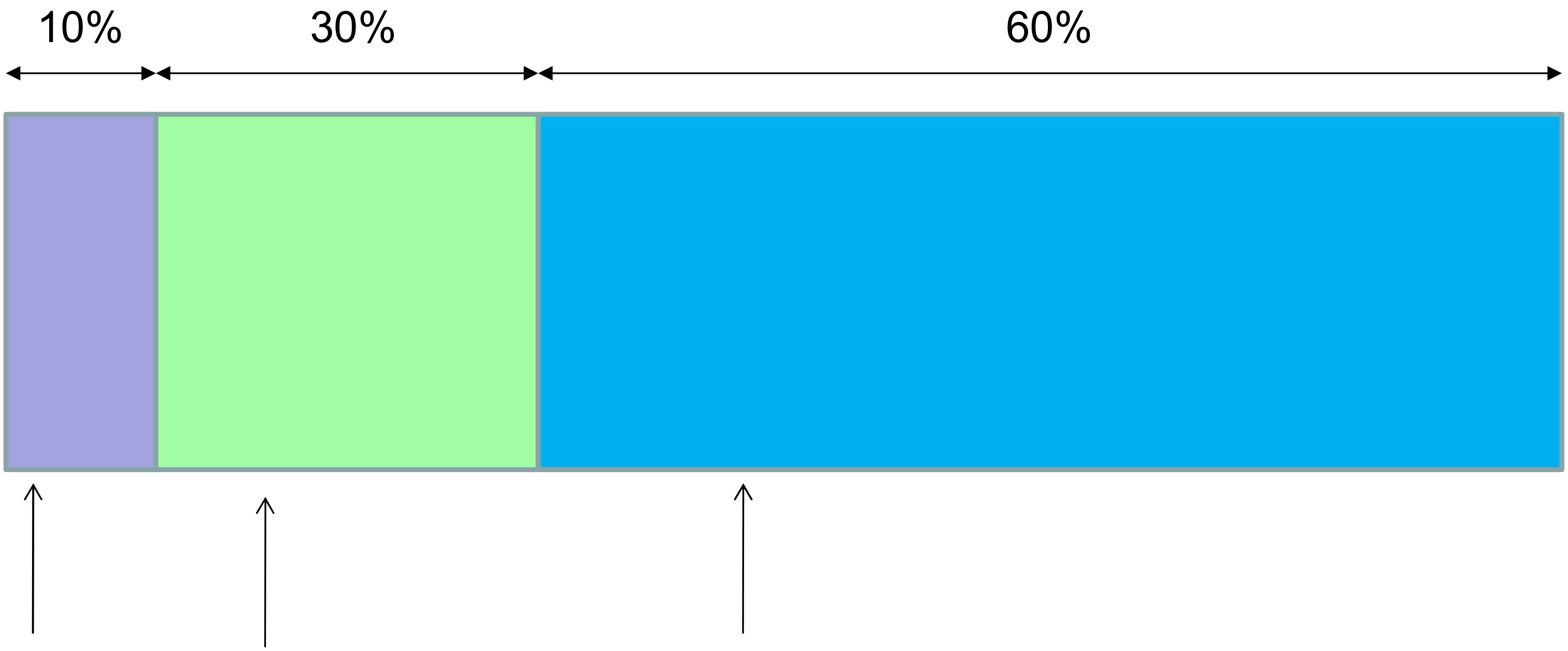
- I still see a reliance on traditional security ideas
  - Network security, firewalls, desktop, AD, anti-virus
  - I also see too big a focus on things like the CIS benchmark
    - This is focused on patch and harden
    - It is missing many things, 12c, 18c, 19c, CDB/PDB, ASM, newer…
    - It is a consensus but the consensus is too small
    - Its 10-15 years out of date
- I see a push to tick boxes
  - Buy TDE but don’t otherwise secure the data in motion
  - Buy Database Vault but still have one admin person with root, Oracle, SYSDBA and DV realm owner, DV admin etc

# Main Focus When Fixing Database Security

# What Is Oracle Security?

- It is not Oracle’s Security
- It is **our** security of **our** data

# Compartmentalise Data Security?



CPU’ s

General Hardening

Data Security: 1) access controls, 2) user security, 3) data security, 4) context based

# Lets Expand On the Sections

- Platform security
  - Security patching
  - Database Hardening
  - Database access controls
- Data security design
  - Access controls
  - User security (least rights)
  - Data security (access controls)
  - Context based security
  - Audit trails

# The Process To Secure Oracle

- Perform a detailed audit of a single production database
- Review existing security policy
- Develop and decide fixing strategy
  - For data security
  - For platform security
- Develop a database security policy
  - Develop a policy document
  - Create a lock down set of tools / steps
    - Initial lock down for all databases
    - Lockdown specific to data and application access
  - Develop policies for a scanner or scripts
- Lock down
  - New
  - Existing
- Check for compliance
- Update, Renew, Extend

# Access Controls

- The number 1 issue; stop people connecting to your database
- Remove users that are not needed
- Strong passwords, schema only, lock
- Limit SYSDBA to local on server only
- Limit network paths (firewall, valid node, listener)
- Use logon triggers to limit at the tool or source location level – use hashes not strings – add delays
- Use error triggers (logon only fires on success)

# Harden The Database

- Start with CIS **but go further**
- Remove default users and features
- Change security parameters
- Remove grants on PL/SQL, views, tables
- Lock down the listener
- Add password profiles
- Add a designed DBA role
- Default passwords
- Limit COMMON rights
- Use lockdown profiles

# User Security

- Remove all duplicate users, not used users
- Remove excessive rights (system rights, Oracle roles, grants)
- Sod and CoI
- Remove duplicates and create separation
- Aim to least rights and only needed users
- Profiles
- DBA, support, third party and release

# Data Access Controls

- Data domains – allow privilege design
- Separate schemas
- Connection users (not the schema)
- Lock schemas
- Ensure data security is in the database (VPD, RAS, Home grown)
- Control resources and privilege use (API)
- Secure the application PL/SQL
- De-duplicate data

# Context Based Security

- Add identity – get/set, Oracle does not do this for you
- Add context based access to the database
- Context based DML
- Context based READ of data
- Context based code (API access)
- Implement Breakglass

# Audit Trails

- Implement a comprehensive audit trail for
    - The database engine
    - Data access
- Use Std, Unified, FGA or custom audit
- Design the audit
    - Don’t just list and enable random settings
    - **“What do I want to know?”**
    - Include everything
        - Management, sizing, policy, escalation, alerts, reports, users
        - Secure the audit trail

# Secure Databases In the Cloud

# The Move to Cloud

- Oracle and others have a big push to cloud?
- But data security must be first
- A database with data insecurities on premise is not magically secure in the cloud
- Cloud infrastructure may be more secure than yours
  - if remote already
  - If on premise data center then traffic is now remote
- There is nothing inherently wrong with cloud – if your servers are not in your building already then its just a remote server already;
  - A risk is producer / consumer responsibilities and who you are sharing with
  - It is the risk that data security is not adequately done in legacy already; adding TDE or DV does not correct inherent design issues and moving legacy bad data doesn't make security.

# Main Threats to Oracle Databases

# Oracle Database Security Threats

- I see and perform audits of a lot of Oracle databases and I see a similar level of lack of security across all verticals
- One of the biggest threats is that security is not the default in Oracle
- Oracle provide lots of security options BUT you have to configure them; so they are not usually implemented

# Often I See In Customer Databases

- Weak passwords – SYS, SYSTEM not changed for 14 years
- Lack of decent audit trails at the database level
- Applications and features installed that you don't need – APEX
- 44k – 39K PUBLIC rights in 12c/18c/19c/21c
- Lack of security of data
    - No schema separation
    - No grants
    - Applications have DBA, all grants, grants with GRANT…
    - Most applications that I see have MOST PRIVILEGES not LEAST PRIVILEGES
- Absolute lack of focus still on data security design

# Secure Data or Bust

# Secure Data Or Go Bust!!

- You must secure your data or go bust
- A legal contract does not stop someone stealing your data
- A pentest will not identify data security issues in your database
  - They maybe find 5 or 6 issues, I find 200
  - If you have 1000 databases that’s 200,000 fixes
- Build a realistic and achievable security for data

# Section

Gotchas

In general you cannot just turn something ON or OFF unless you think about every consequence first – this does not mean we should not do it

# Security Can be Complex

- There are many possible gotchas that need to be considered as part of securing data in Oracle
- Adding security can make access / work harder if not planned properly (password cannot be remembered if its no longer 3 characters!!)
- Security is also about people i.e.;
  - DBAs must not use SYSDBA therefore you must define a suitable set of privileges for daily use
  - Support or release must not use the schema passwd therefore lock the schema, use proxy and change release processes
- We will highlight an example in a little more detail next

# Revoking Grants

- The process:
  - Check objects are valid
  - Revoke the grant
  - Check for invalid objects
  - List the owners (schemas)
  - Grant the right back to the owner (schema)
  - Re-compile all objects
  - Check invalid again

- The re-compile is flakey and can lock up or need doing more that once
- A DBA who updates the database or runs catproc.sql can “undo” the security
- Must be scripted allow re-application as needed
- CDP/PDBs
  - Each container can be different
  - Do the PDBs first then CDB
  - Some PDBs not done?
- Jobs may have to be disabled
- **CIS doesn’t tell you the method**

# Conclusions

- Understand the big picture
- Build layered security
- Do not put all your eggs in the hardening only basket – such as following CIS
- Build hardening and patching before data security
- Build data security before context based security or cost options
- Cost options also must be secured
- Don’t try and fix 200 issues per database

PFCL
PETEFINNIGAN.COM LIMITED

# Questions / Discussion

?

# Securing Data