



# If your Oracle Database is Hacked

---

What Should you do?



# Legal Notice

---

## If your Oracle Database is Hacked, What should you do?

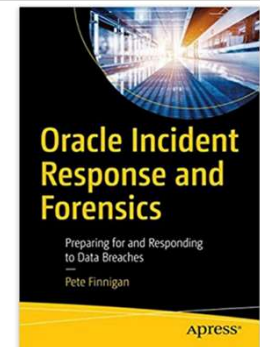
Published by  
PeteFinnigan.com Limited  
Tower Court  
3 Oakdale Road  
York  
England, YO30 4XL

Copyright © 2025 by PeteFinnigan.com Limited

No part of this publication may be stored in a retrieval system, reproduced or transmitted in any form by any means, electronic, mechanical, photocopying, scanning, recording, or otherwise except as permitted by local statutory law, without the prior written permission of the publisher. In particular this material may not be used to provide training of any type or method. This material may not be translated into any other language or used in any translated form to provide training. Requests for permission should be addressed to the above registered address of PeteFinnigan.com Limited in writing.

**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.



## 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, SYM 42
- Speaker at various conferences
  - UKOUG, PSOUG, BlackHat, more..
- Published many times, see
  - <http://www.petefinnigan.com> for links





## Agenda

---

- Background
- How do attacks happen
- Overall steps
- How to handle a breach
- Next steps



## Section

---

Background



## 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



## The Data Gold Rush - 2

- Companies produce inordinate amounts of data every day
- Companies main product may not be data (initially?)
- Lack of AI specialists out there to help this growth

data gold rush

About 67,000,000 results (0.43 seconds)

**Cultivated data is the next Gold Rush | TechCrunch**  
<https://techcrunch.com/2019/08/08/cultivated-data-is-the-next-gold-rush/>  
 8 Aug 2019 - Cultivated Data Gold Rush. Bernard MoonContributor. Bernard Moon is co-founder and partner at SparkLabs Group, a network of accelerators ...

**What is the Big Data Gold Rush All About? | Sagence**  
<https://sagenceconsulting.com/posts/big-data-gold-rush/>  
 An article by Consulting Magazine, "Big Data's Gold Rush," examines the massive potential opportunity for both consulting firms and clients related to Big Data.

**The Big Data Gold Rush - Forbes**  
<https://www.forbes.com/sites/bradpeters/2012/06/21/the-big-data-g...>  
 21 Jun 2012 - It is a tired cliché that Silicon Valley and high tech revolution resemble the 1849 California Gold Rush. But, at the dawn of the Big Data era, that ...

**Data: Gold rush of the digital age | Made in Germany | DW ...**  
<https://www.dw.com/data-gold-rush-of-the-digital-age/>  
 1 Jan 2019 - Made in Germany. Data: Gold rush of the digital age. Using the Internet means leaving behind a trail of data. From online shopping to social ...


**Data gold rush**

The amount of **data** spit out into the world each day is truly massive. ... It's creating a **data gold rush**, with companies globally expected to spend nearly \$190 billion this year on software and services to analyze any sort of information that could give them an edge over their competitors. 12 Jun 2019

Wall Street is chasing a data gold rush. Here's our deep dive ...  
<https://www.businessinsider.com/future-big-data-wall-street-finance-industr...>



## UK ICO – Second Biggest GDPR Fine



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.

[Home](#) [Your data matters](#) [For organisations](#) [Make a complaint](#) [Action we've taken](#) [About the ICO](#)

[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 Commissioner's Office (ICO) intends to fine it for breaches of data protection law.

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

The proposed fine relates to a cyber incident which was notified to the ICO by Marriott in November 2018. A variety of personal data contained in approximately 339 million 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





# Oracle Reference Customer - Promoted

The screenshot shows a web browser interface with a search bar containing the text "Ask 'How do I know my data is safe in Oracle Cloud?'". The page title is "Oracle Customer Success — Starwood Hotels & Resorts Worldwide, Inc.". The main headline reads "Starwood Hotels & Resorts Worldwide Delivers More Competitive Rates and Offerings by Accessing Reservation Data Updates 233x Faster". Below the headline is a "Share" button. The article text states: "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."



## What Do Attackers do?

---

- Examples of what attackers do
  - Read data (steal)
  - Update data (increase a payout for instance)
  - Delete Data (ruin a business)
  - Change the database settings and permissions
  - Change the application for later attacks



## How do Attackers Attack?

---

- At a high level
- You give data away (not intentionally)
- Attackers read data via web attacks or SQL Injection
- Attackers exploit flaws in the data model, the application, the hosting and more
- Your staff access the data and sell/give away
- DBA and super user staff can access any data
- Steal backups or other copies of the data



## Who Attacks?

---

- The public – external
- Internal employees with access to the application
- Internal employees no access to the application
  - Access to data left lying around – reports, paper, files...
  - Exploiting the application or database
- DBA staff with access to everything
- Third parties with system access



## Why?

---

- Application design and code flaws
- Application deployment flaws
- Application permissions
- Database security flaws
- Network flaws
- Copies of data
- External data



## Skilled or Unskilled

---

- An unskilled attack is like a thief walking down streets trying car doors or house doors and entering the house or car if its open
  - The database equivalent would be running tools such as SQL Map to locate “open doors”
  - In these cases the attacker probably doesn’t know Oracle
- A skilled attack is finessed and much harder to detect.
  - The skilled attacker would be an expert
  - Little to no noise; hard to detect
  - Straight to the point



## Section

---

# Overall Steps



## Scope

---

- I am not going into technical details of:
  - Data,
  - Redo and blocks,
  - Analysing changes in depth
  - Reviewing data
- I am going to focus on the process of managing the breach
- And how to deal with the breach





## What is Obvious Before We begin?

---

- As I will show in upcoming slides
  - If we secured the data, database and applications then the simplest way to avoid managing a breach is not to have a breach
  - Some elements will help breach response massively such as already having audit enabled
  - Having a plan before a breach means not randomly running around when there is a breach
  - Having a team in advance avoids mistakes
  - Being able to recognize a breach will reduce the impact of that breach



## What are the Main Steps?

---

- Be aware of a breach having taken place
- Confirm the breach
- Enter breach response mode
- Transfer control to the breach team
- Do not turn off / shut down
- Investigate that the attack is actually an attack
- Document the system
- Do live response



## Main Steps (2)

---

- Collect less volatile data
- Break the network connection
- Copy evidence
  - In the PC world this means copying disks
  - Not practical in Oracle because of license, size, continuity
- Checksum collected evidence
- Perform forensic analysis
- Build a timeline
- Document the attack
- Shutdown, restore, fix, lessons learned



## Section

---

# The Team and Reporting



## How and Who?

---

- Before we talk about how a breach is reported and to who (The incident response team!) we must talk about the team leader and then the team
- This must be in place before any breach
- The leader of the team should not be compromised by the attack (i.e. were they involved) and not swayed by the business (i.e. coerced to ignore and gloss over to keep the business running)
- They should have a management role only
- They should manage the steps and PR



## The Team

---

- The team leader should be a manager
  - Of the process, not necessarily a manager per-se
- The team leader must have a deputy; substitute as we do not know when the breach will happen
- The team should include
  - Security
  - Oracle – DBA
  - Business
  - Management
- All of these people need duplicates to reduce the risk of swaying the response if they are involved



## How to Report

---

- All reports of a breach must be to one central location
  - **This must be to the breach response team**
  - They do not need to have this as a full time role as it only kicks in if there is a breach
- The simplest approach is two fold
  - Training internally as to recognize what could be a potential breach
  - A simple email [breach@example.com](mailto:breach@example.com)
- Internal and external report to one location
- Think of this as a funnel



## Stop Random Investigations

---

- This can only be resolved by training and investigations
- For instance, if a DBA notices or is told of a broken process or corrupt data and this is sudden then they should not assume a bug
  - Was there a release?
  - Was there a data change?
- NO, then do not investigate and instead report to the breach team
- All potential breaches must not be randomly investigated all over the company





## A Breach comes in

---

- A potential breach comes in through the funnel
- Transfer control to the incident team leader
  - How: The incident team leader (or a sub-ordinate) manages this list / email
- The leader should assign someone to investigate based on the evidence so far
  - i.e. do we need a developer / DBA / Business Analyst or what?
  - Make a judgement on who could be involved – i.e. don't get a DBA to investigate something he/she did
- No changes at this point made to any system



## An Example

---

- I investigated a potential breach as requested by a customer
- They “thought” the breach had just happened and I travelled by car to the organisation in the North West of England
- I was able to determine that the breach was real quite quickly from the evidence they had already
- Further digging to find the start of the breach revealed it was likely hacked 3 years and 2 months before
- BUT, they were still right to get me there quickly



## How to Verify a Breach?

---

- This is difficult in the sense there is no simple “yes/no” way to do this
- Is it a real breach depends
- The simplest is that it comes to light that data was leaked
  - Its posted to Facebook, Twitter, Dropbox...
  - Check the data is not in the public domain already
  - Check the validity of the data – i.e. its real data
  - Identify if possible where it came from (65 records in prod but 52 leaked, 52 exist in test!)
- Remember the breach can be internal



## No Technical Details

---

- The focus of this talk is to discuss the process and how to deal with a breach
- We are not getting into the details of how to do live response and how to investigate forensically
- **Next time!!**
- Beware of time stamps
- Beware of correlation
- Beware that it is hard to find evidence of some changes
- Beware that read actions without audit trails are very hard to find



## Do Live Response and Forensic Analysis

---

- Collect the most transient data
- Collect less transient data
- Build a time line of evidence
- Check sum the evidence
- Correlate evidence together – i.e. an action in an apache log can be correlated to database records and also users used.
  - If the attack came via Apache then we know what database user was used to connect BUT the attacker could escalate via bugs in definer rights PL/SQL
- Work out when the attack started and ended and started



## Training and Awareness

---

- In advance of a breach staff should be trained
- The response team should be trained
  - On the process
  - On how to recognize a breach
  - On how to investigate a breach
- All staff should be trained
  - To recognize that something may be a breach
  - They should be aware of the process and breach team
  - They should be aware to submit to the breach funnel



## Public Relations

---

- Ensure a consistent and uniform response to the media and customers and interested parties
- I DO NOT MEAN LIE!!!
- Ensure that all news of the breach to customers, internal staff, managers, the press comes from one person / channel
- Ensure the message is vetted to provide accurate status or mechanicals of the investigation but no detail
- Ensure all staff know they cannot speak to anyone



## Detailed Report

---

- At the end of the whole process we can create a report detailing
  - When did the attack start and end
  - How did the attacker gain access
  - What did the attacker steal or change
  - What could the attacker have done with more skills
- The last one is interesting and I have seen many times. An attacker does something but didn't have Oracle skills or knowledge to go further BUT they could have done





## Fix or NOT and update Core security

---

- At this point we can decide to fix the database/data
- **OR**
- restore
  - Be very careful
  - If the attack happened months or even years ago restoring is not an option
    - The backups will also be corrupt
    - It is completely impractical to restore to a long time ago



## Fix the Security!

---

- Fix the flaws that allowed the hack to happen
  - In the database
  - In the applications
  - In the web servers
  - In the network
- Enable audit trails
- Enable / design database security
- Enable overall security
- Enable monitoring



## Inevitable Conclusion

---

- It should be obvious that there are things we must do now irrespective of a potential breach
  - Appoint and create an incident response team and leader and substitutes; this is not a full time job; think fire warden or first aider
  - Set up a breach / potential breach reporting system. This is a funnel – can be an email address
  - Train the team on how to respond and deal with a breach
  - Create a breach response process
  - Enable a good detailed audit trail to help with forensic analysis



## Conclusions

---

- Secure the database in advance
- Enable comprehensive audit trails
- Create a plan in advance
- Have the right teams trained in advance
- Have the right response tools in advance



## Questions

---

?

If Anyone has questions, please ask now or  
catch me during the event!!



# If your Oracle Database is Hacked

---

What Should you do?