A new approach to preventing attacks on your critical data

Andrew Muecke – ITSA, S.A Dept of Planning, Transport and Infrastructure

Pulse2012

Meet the Experts. Optimise your infrastructure.

May 31 – June1

Sheraton on the Park Hotel, Sydney

What is the S.A Department of Planning, Transport and Infrastructure (DPTI)?

- DPTI is a complex Department within the South Australian Government
- The Department in its most simple terms consists of:-

Public Transport (Trains, Trams and Buses)

Traffic Management (Traffic Lights, Tunnels, Bridges etc)

Registration and Licensing (e.g. Drivers Licenses)

Land Administration (Titles, Valuations, Conveyance)

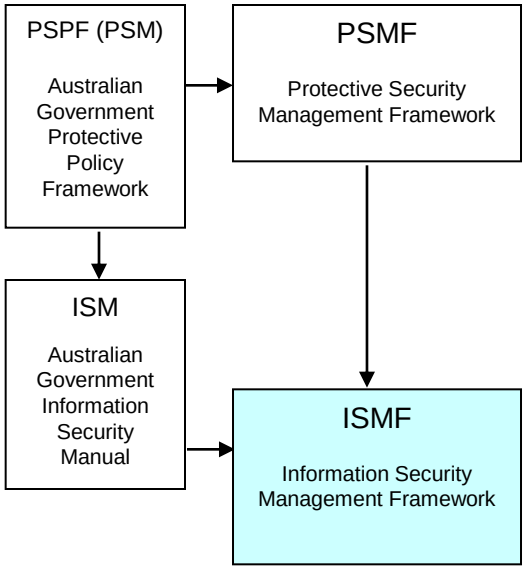
Parliamentary Network (incl. Electorate Offices)

Building Management (owned and leased)

Planning (Land Use, Road etc)

What is the information security context in the S.A Government?

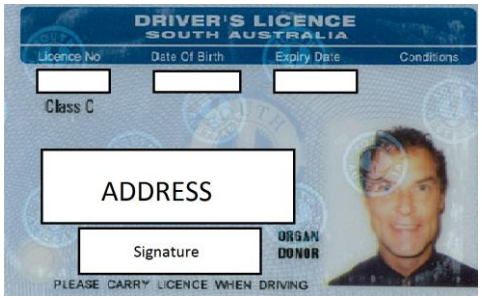
- The SA Government employs the Information Security Management Framework (ISMF)



- A risk based approach to security management
- Utilising AS/NZS ISO/IEC 27000 series
- Establish a security management system (ISMS) with an initial focus on critical assets and personal information

An exploration of the Department's Registration & Licensing (R&L) Environment

- This is an environment which contains a vast array of sensitive personal information
- Only a small amount of this information forms the Driver's License:-



PERSONAL INFORMATION

- Registration and Licensing also generates enormous amounts of money for the State

FINANCIAL INFORMATION

The R&L environment is a ‘critical system’ for the department and the State

- The ISMF states specific compliance requirements for critical systems
- A Governance structure was established for the operational registration and licensing environment that included ICT representation
- This structure allowed for a ‘business based’ risk management approach to be undertaken to determine compliance to the ISMF (i.e. acceptance of the level of compliance which may or may not be at ‘full compliance’)

An analysis of the R&L ICT operating environment in relation to the ISMF

- A number of traditional security measures were already in place:-
  - Firewalls
  - Intrusion Prevention
  - Switch Access Control Lists
  - Native Logging etc

- In business speak, we called this a multi-layered ‘onion skin’ model of security

- However, a gap was identified around ‘insider activity’ (otherwise known as monitoring ‘privileged users’)

On the search for Guardium

- The R&L Governance Committee supported the proposal to search for a Database Activity Monitoring system and to undertake a pilot

- The Governance Committee required milestone reporting of progress through selection and pilot

- It was understood however, that this was still very much a technically focused initiative and ICT would need to lead

What type of team was put together to do the discovery?

- Essentially this was constrained to three key resources:
  - The Information Technology Security Advisor (ITSA)
  - The Technical Security Analysts (2 staff)

- We had the full backing of ICT management throughout the discovery ($ cost, of course, is always an important factor to keep them interested!)

Finding Guardium

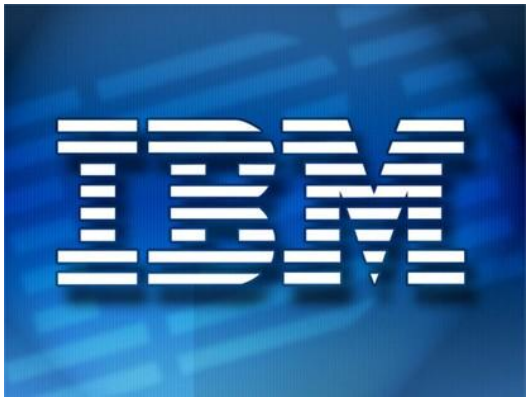
- Our research determined that Guardium was the market leader in the real-time enterprise database activity monitoring market
- Of its many benefits, two primary aspects that lead to its selection for a pilot were:-
  - Its independence from native database logging, the DBMS itself and the database server operating system (i.e. complete independence of the environment it is monitoring thereby permitting true ‘segregation of duties’)
  - Its ability to support all major DBMS (e.g. Oracle, MS-SQL etc) was perceived as a major ‘future’ benefit - the department has a mixed ICT environment and Guardium will be deployed as required to meet future business requirements

And Guardium delivers more

- There are many other strengths that differentiate Guardium from its competitors:-

  - Can analyse complex SQL traffic
  - Single read-only repository for all audit data
  - Data is immediately available
  - Etc, etc, etc…….

- Your IBM account manager can explain this in greater detail!



Moving to a ‘Guardium’ Pilot

- Contact was made with our IBM Account Manager and arrangements were made to connect a Guardium appliance into our ‘Lab’ and connect to our R&L Development environment

- IBM agreed to provide us with a Guardium appliance to install and test
- IBM produced specific documentation and test cases for the pilot

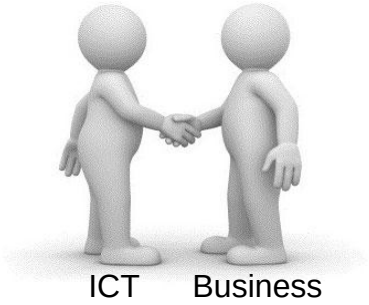
Informing the Governance Committee that its good to go!

- A minute was written to the R&L Governance Committee stating that the Guardium pilot was successful and that it was recommended that the product be purchased and installed in the production environment
- From this point onwards, the implementation (or project management) approach was going to employ a business-centric focus (not technology). Otherwise known as a ‘COMMON SENSE’ approach

We are bringing it back!

How do you market an initiative which is likely to be seen as intrusive?

- The deployment of Guardium was marketed as a positive move that was ***mutually beneficial*** to both the business and ICT:-
  - The business could be guaranteed that their databases were afforded the appropriate protection
  - ICT staff who support the R&L environment have proof that they are working for the benefit of the department



Who should be involved in the deployment, including training?

- Our decision was that we wanted it well known both in the business and the ICT support environment that Guardium would become a part of our operating environment
- When it came to a decision of who should attend Guardium training, we agreed on:
  - Our database administrators (i.e. privileged users)
  - The application/platform managers
  - ICT operational security

- There was no fear with including the staff who would be ‘monitored’ as Guardium allows true separation of duties. When deployed in the live environment, these staff would not be able to control what Guardium logs

Turning Guardium on in the Development Environment

- The deployment of Guardium is focused on the ‘computer based policy’ i.e. what data do you wish to collect
- One of the first parameters determined is that you cannot collect all data from a large system like the one supporting R&L as the disk space on the appliance would be quickly consumed
- With this in mind, a decision was made by the team that we would not monitor ‘trusted’ traffic as that would be an inefficient use of resources

This is the time that you use to refine your ‘policy’. As is always the case, a defined theoretical approach needs to be refined when it is brought into the real world . Remember , Guardium can log anything you want, but what do you really need?

Preparations for Going Live (then adjusting the schedule!)

- Liaison with IBM Guardium support staff occurred throughout the project and was fundamental to the transition to going live

- Our timing was slightly delayed due to the proximity of a new version of Guardium being released. It was considered a safer option to upgrade in the Development environment and run the product for a 30 day period before going live (rather than go-live and perform the upgrade afterwards)

OK, lets get ready!

- A workshop, facilitated by IBM, was held prior to go-live which included the database administrators (privileged users), application/platform managers, internal audit and security staff
- At this point, the Department's Internal Auditors were included in the workshops so that they could gain an active understanding of Guardium and the function it would be performing
- The 'Policy' set deployed on the Development environment was revisited for a final time before it would be transitioned into Production

So, did the deployment to Production work well and were there any challenges?

- The deployment technically was very smooth – the lesson learnt above all others in this project was not about Guardium but about our own Change Management
- A mature Change Management practice, which is a great thing, will ensure your go-live approach will need to be ‘one step at a time’. Don’t forget, you are making changes to your critical system!
- So the lesson learnt is:-

Make your ‘Change Management’ team aware of what you will be doing as early as possible - introduce them to Guardium at the earliest opportunity!

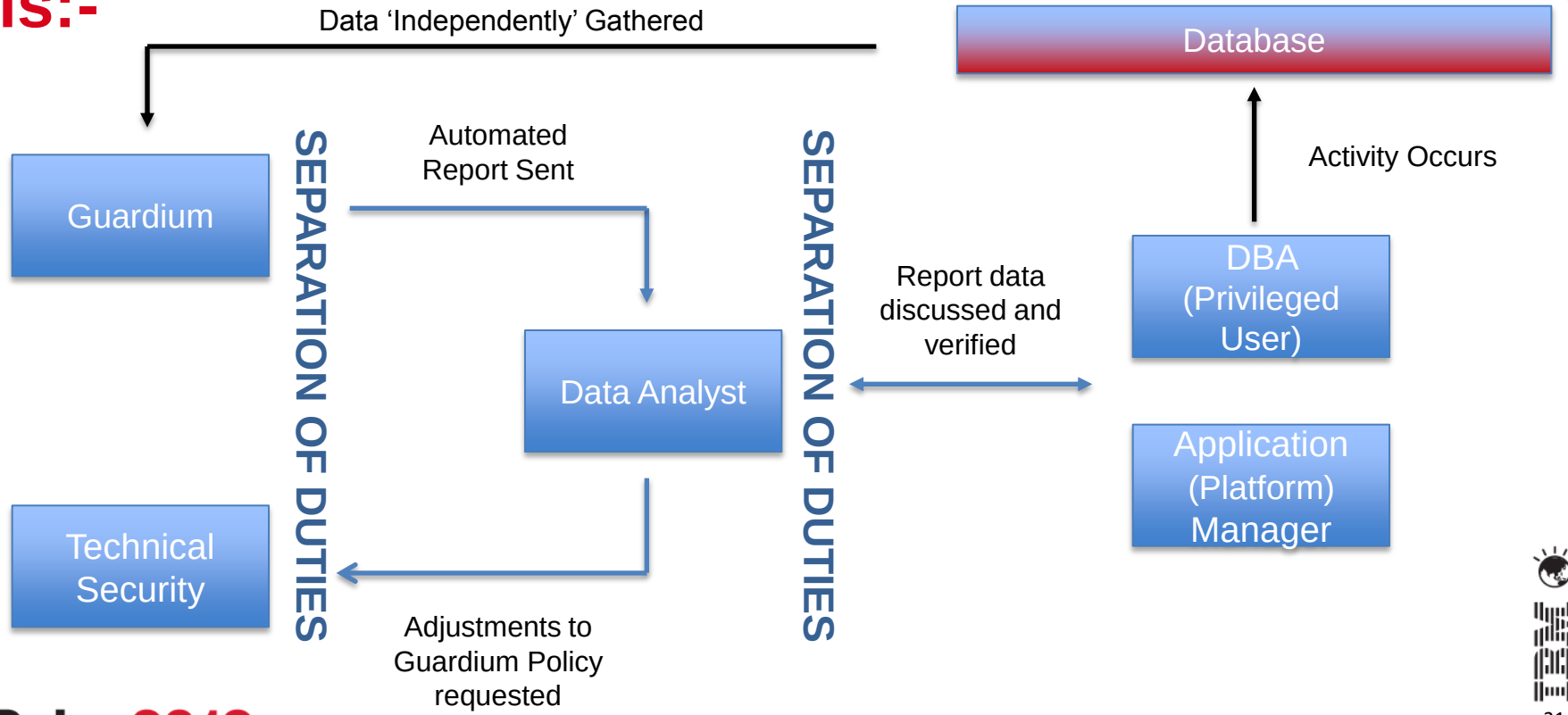
But what about the data Guardium is collecting?

- A significant parallel process in your preparations for going-live is defining how you are going to manage the data – you know what you are collecting (as you have tweaked your computer based policy) but what are you doing with it?
- Our Department has used the parameters held within Guardium to self generate a weekly report on the previous week's activities that is received via email (containing a .csv file and a PDF file)
- We have appointed a senior staff member in our ICT Consultants area as the data analyst. They receive the weekly reports and are spending approximately an hour a week interrogating those report (for the first few reports time spent was between two to three hours)

A continuous process to get data collection just right!

- It is beneficial if the data analyst has some experience or exposure to ‘programming language’, but the key requirement is for them to be strong communicators
- As the data you are logging will be ‘SELECT’ statements and the like, the data analyst must have access to the database administrators and managers to build an understanding of what the data is telling them
- Not only does this focus efforts on that which is abnormal, the evidence gained allows for further tweaking of the computer based policy so that data gathering is at its most optimal

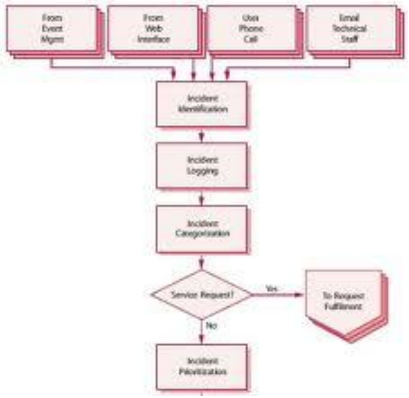
In diagrammatic terms, our Guardium setup is:-



Building Guardium into your ‘Security Incident Management Process’

- Now that you have a fully fledged operational process, you need to make sure that it is ‘attached’ to your Security Incident Management Process
- Although we all hope that our staff will do no wrong, the data analyst must have the support of the Department’s Security Incident Management Process if an anomaly is detected

Document ‘Guardium’ within your Security Incident Management Process!



What about data retention considerations?

- In our project, we left this particular component (backup, purge, archive and recovery) until after we went live. This was simply due to focusing our limited resources on the deployment
- Also, it was felt that the data in Guardium could follow the same blueprint as already used for the application data
- It is important to point out that a particular security measure within Guardium is that due to the encryption applied to data removed from the appliance only a Guardium appliance can read Guardium data. This means that you will need to restore that data to the appliance

~~Our Auditor-General is now very happy with us!~~

Our Auditor-General is placated!

- Guardium is now ensuring our R&L business and ICT environment that:-
  - Privileged user activity is being monitored
  - Changes to database schema or structural integrity is monitored
  - Data viewed by users and administrators (as defined by your policy) is monitored
  - Local activity on a (monitored server) is captured
  - Its ‘independence’ ensures ‘separation of duties’
  - As a result it is helping us to secure and harden the database environment
- And its ability to support all major DBMS will help us with future deployments in the Department

Any Questions?

Trademarks and disclaimers

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.