Database Security for a Down Economy

Rich Mogull
Securosis, L.L.C.

Objectivity Disclaimer

This webcast is sponsored by Oracle, but all content is developed independently and represents our objective positions.

Today's presentation focuses specifically on Oracle security, but is not an endorsement of any database platform over another.

What We'll Cover

- The economics of database security
- Building business justifications
- Top 5 steps, with economic benefits.

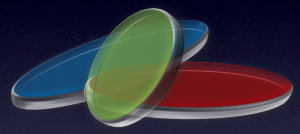
Mainframe

Jail

Internet I

Fortress

Internet II



Zone

Securosis

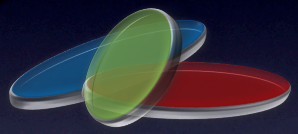
Mainframe

Jail

Internet I

Fortress

Internet II



Zone

NETWORK

Securosis

But what about the information?

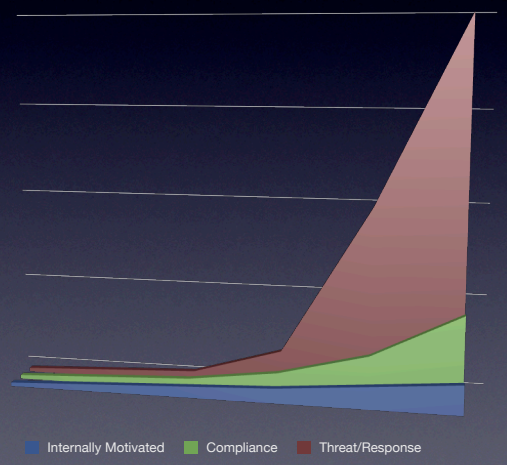
Threats

Quiet

Noisy

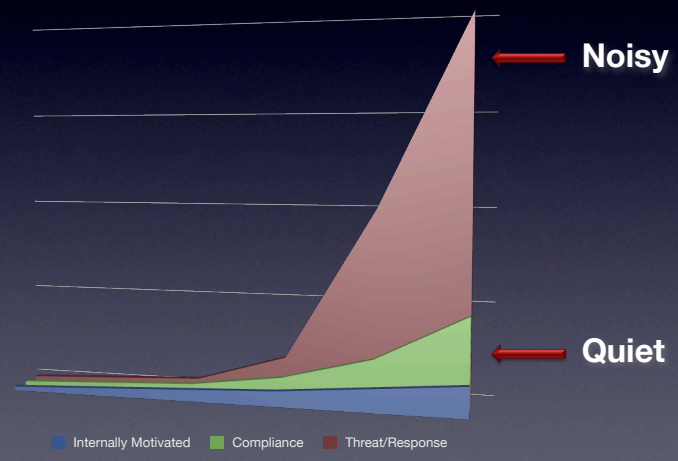
Securosis

Security Markets



securosis

Security Markets



securosis

Why We Under-Invest in Data Security

- "Old" threats never go away.
- Budget cycle momentum.
- Experience and training.
- Noisy vs. Quiet
- Lack of quantifiable results

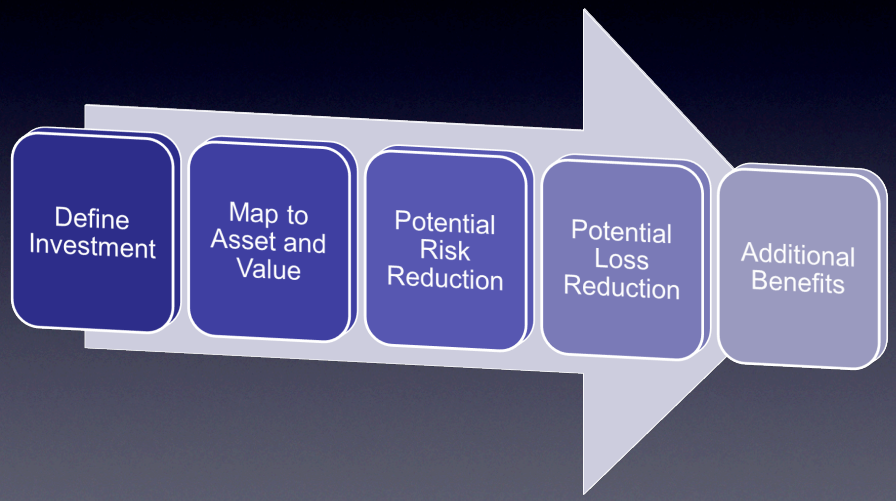
Securosis

The Business Justification for Data Security Model

http://securosis.com/research/publication/the-business-justification-for-data-security/

Securosis

The Process



securosis

Define Investment

Data Type	Value	Frequency	Audience

securosis

Map to Covered Data

Data Type	Value	Frequency	Audience

Data Type	Value	Frequency	Audience
Credit Card Data	5	4	2
Customer PII	3	4	4
Trade Secrets/Business Plans	3	2	1

Securosis

Potential Risk Reduction

			Impact								
Risk	Likelihood/ARO		C		I		A		Total		% Δ
	before	after	B	A	B	A	B	A	B	A	

Risk	Likelihood/ARO		Impact		%Change
	Before	After	Before	After	
Unencrypted data	4	1	4	4	62%
Portable storage	3	1	4	4	71%
Email leak (via CSRs)	5	1	4	4	71%

securosis

Risks

- Lost Media
  - Lost disks/backup tape
  - Lost/stolen laptop
  - Information leaked through decommissioned servers/ drives
  - Lost portable storage
  - Stolen servers/workstations
- Inadvertent Disclosure
  - Email leak
  - Unsecured repository
  - Unsecured connection
  - File sharing leak

See the whitepaper for more examples

securosis

Potential Loss Reduction

Loss	1	2	3	4	5	B	A

Loss	1	2	3	4	5	B	A
Notification Costs	$0-1000	$1001- 10,000	$10,001- 100,000	$100,000- 1M	>$1M	4	2
Reputation Damage	Positive public image	Single, local neg incident	Sustained neg local	Negative national	Sustained neg national		

securosis

Potential Loss Categories

- Quantified
  - Notification Costs
  - Compliance Costs
  - Investigation/Remediation
  - SLA Violation
- Qualified
  - Reputation Damages
  - Customer Loyalty
  - Loss of Sales
  - Competitive Advantage

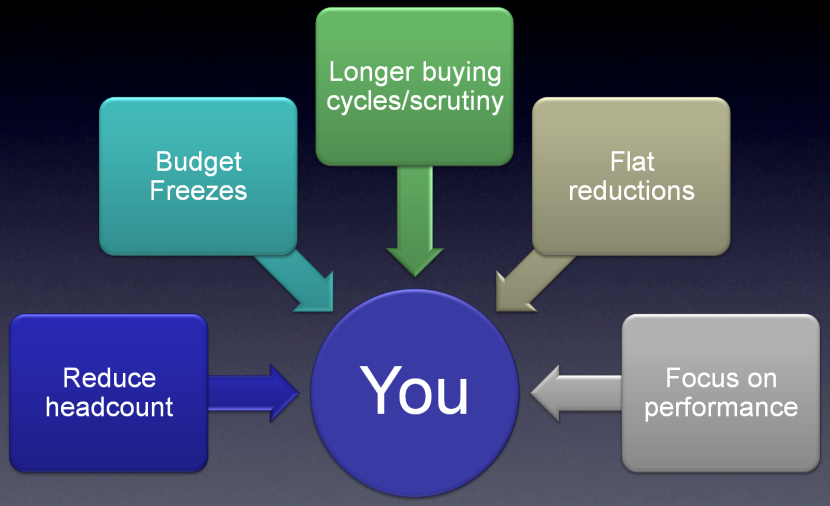
securosis

Additional Benefits

Benefit	Description	Est. Value ($)

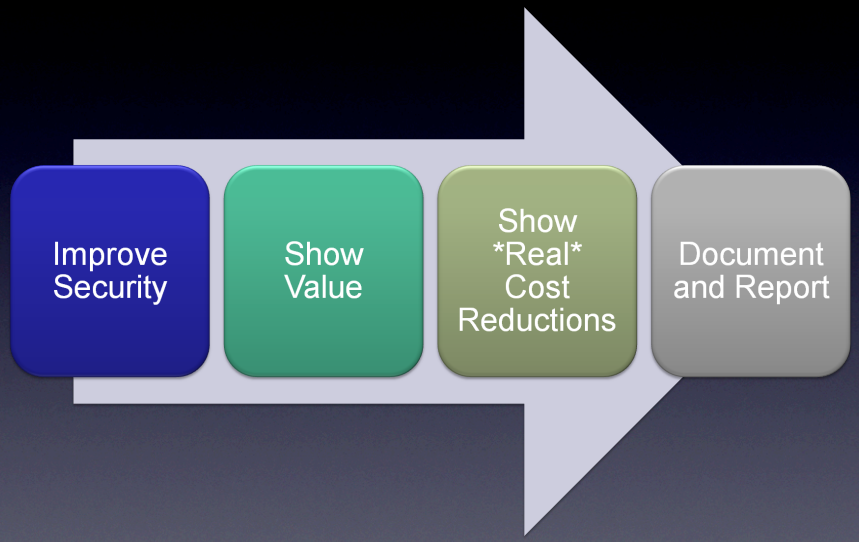
securosis

Economic Pressures



Securosis

4 Steps to Hero Status



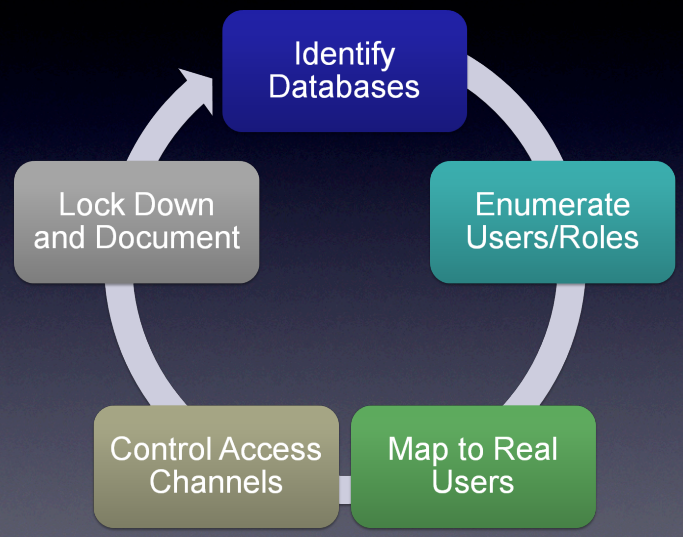
Securosis

Top DB Security and

- Access Control/Role Management
- Configuration Management
- Media Protection
- Auditing and Monitoring
- Internal Controls

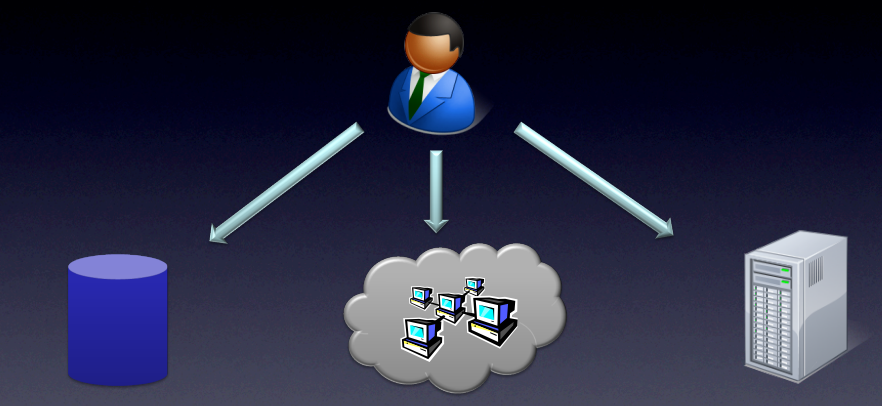
securosis

Database Access Control/Role Mgmt



securosis

Database Authentication



Database User

Network/Domain User

Local System User

Securosis

Securing Access

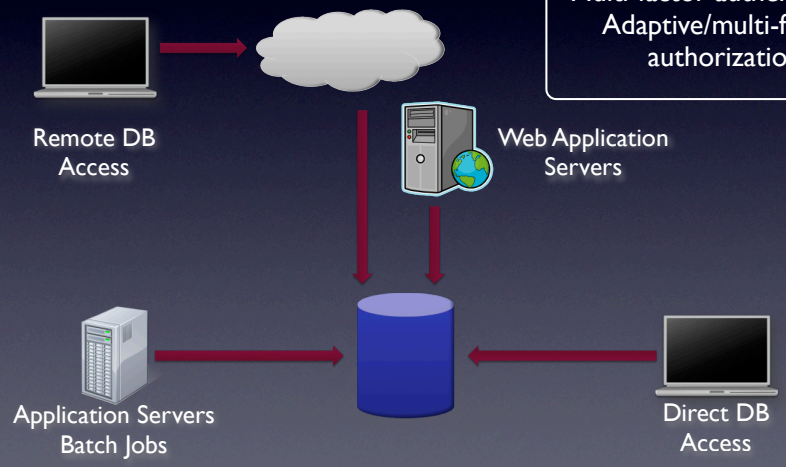
- Choose appropriate authentication methods.
- Link in with IAM (Identity and Access Management).
- Appropriately design, and fully document, authorization/ access control mappings.
  - Work with application owners/teams.
  - Especially for service accounts.
- Limit access channels
- Do not use generic administrator accounts.

Securosis

Access Channels

Channels can be controlled/ locked.

Multi-factor authentication
Adaptive/multi-factor authorization



securosis

Economic Benefits

- No additional tools needed, although some may be extremely useful (and reduce costs).
- Locking down and maintaining ongoing documentation will reduce audit costs.
- Large security benefits.
- Often increases reliability- easier to track down issues.
- Excellent preparation for future projects.

Securosis

Secure Configuration

Secure the host

- Work with server/security team
- Do not run DBMS as local admin

Secure the DBMS

- Work with security to develop standards
- Follow secure configuration standards
- Keep updated/install CPUs

Secure communications

- Lock network services
- Lock database access
- Encrypt as needed

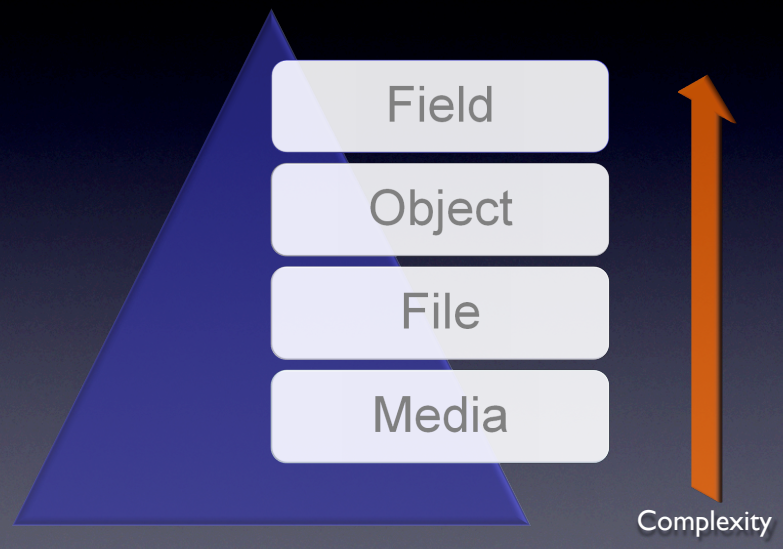
Securosis

Economic Benefits

- Large improvements in availability/reliability.
- Reduced audit costs.
- Lower ongoing systems maintenance and patching costs.
- Improves security by reducing vulnerabilities.

Securosis

Encryption



Securosis

Data Masking

Production

ID	Name	SSN
1	Smith	111-22-3333
2	Jones	444-55-6666
3	Doe	777-88-9999

Development

ID	Name	SSN
1	Johns	123-45-6789
2	George	453-67-7356
3	Blike	245-12-7329

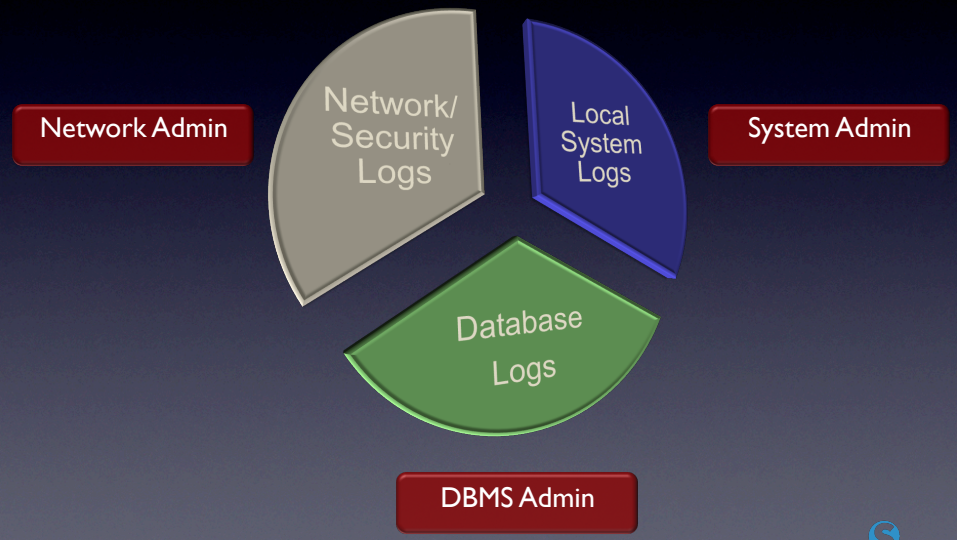
Securosis

Economic Benefits

- Reduces risks of unintentional data loss.
- May eliminate need for backup encryption.
- Works very well with auditing/monitoring.
- Reduced audit costs.
- Non-field encryption more cost effective than field level encryption, and (as a compensating control) may amortize mandated field encryption costs.

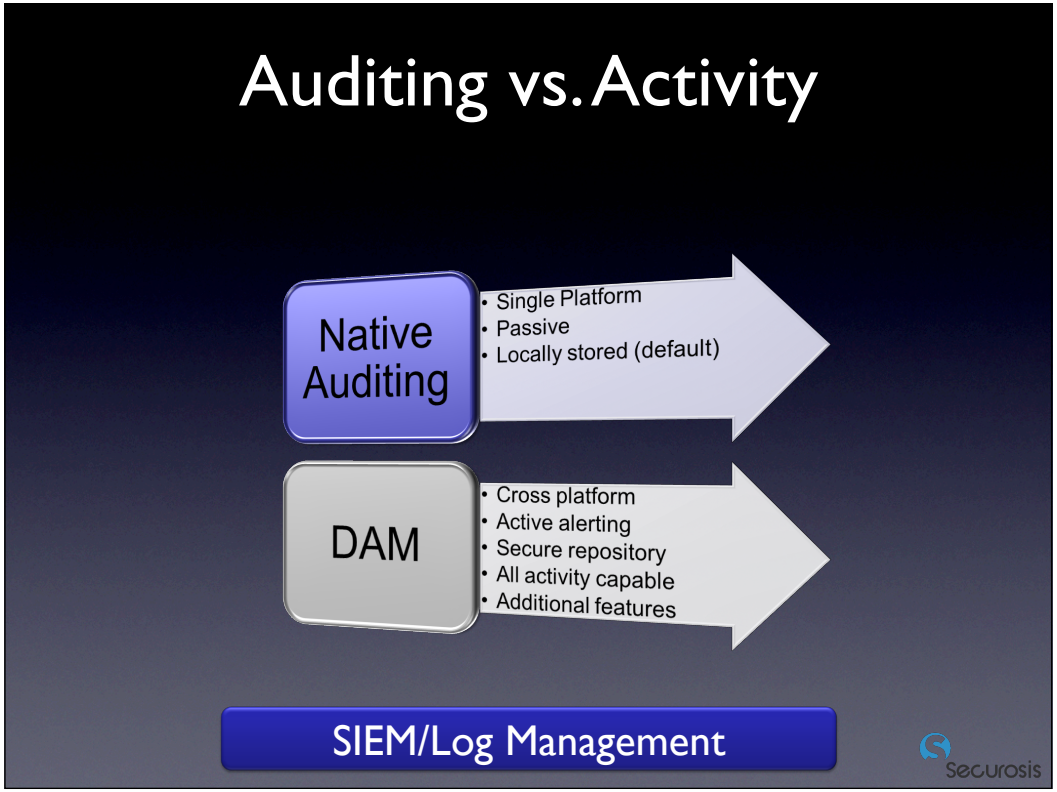
Securosis

Auditing



securosis

Auditing vs. Activity



Economic Benefits

- Dramatic audit cost reductions.
- An effective security control that only needs minimal external changes.
- Does not interfere with business processes.
- Can focus on sensitive areas to reduce management overhead.
- May provide performance management benefits.
- Many low/no cost options.

Securosis

Internal Controls

- Oracle Database Vault
- Encryption
- Structure
- Views
- Concept of least privilege
- Adaptive/multi-factor authorization

Securosis

Economic Benefits

- Low/no cost.
- Improved reliability.
- Ties in well with configuration management.
- Easy to maintain.
- Extremely effective from a security standpoint.

Securosis

Recommendations

- Understand the economics of your business.
- Start with higher value databases/applications.
- Take quick, practical hits over drawn-out programs.
  - Lock down fast and clean up slowly.
- Always document and build a business case.

Securosis

Database Security for a Down Economy

Rich Mogull
Securosis, L.L.C.
rmogull@securosis.com
http://securosis.com