SQL in the City Summit
Strategies for Solving Compliance Challenges

Steve Jones,
Redgate Software
SQLServerCentral
Steve Jones
Evangelist, Redgate Software
Editor, SQLServerCentral

28 years SQL Server data experience
DBA, developer, manager, writer, speaker in a variety of companies and industries

Founder, SQLServerCentral
Currently the editor in chief, with the goal of helping you learn to be a better data professional every day

11 year Microsoft Data Platform MVP
I have been honored to be recognized by Microsoft for the as a Data Platform MVP working with SQL Server

@way0utwest
/in/way0utwest
@way0utwest
sjones@sqlservercentral.com
www.voiceofthedba.com
Data Breaches are Headline News

Key takeaways from Singapore healthcare data breach

Adidas warns US customers about a possible data breach

JPMorgan Chase: 76 million homes, 7 million small biz thumped in cyber-heist

Macy's Customer Credit Data Hacked in Breach

eBay Breach: 145 Million Users Notified

Lessons from the Heartland Payment Systems data breach, redux

Financial Services Sector Breaches Triple in Five Years
MARKETING FIRM EXACTIS LEAKED A PERSONAL INFO DATABASE WITH 340 MILLION RECORDS

BMO and Simplii hackers demand ransom of $1m in XRP

30 May 2018

The hackers who claim to have stolen the personal information of thousands of BMO and Simplii Financial customers are demanding a $1 million ransom in the form of Ripple's XRP, according to CBC.
Where do these breaches come from?

92%  
External Attackers*  
for Finance and Insurance industries

56%  
Internal Users*  
Healthcare

48%  
Hacking attacks*  
In all cases

12%  
Privilege misuse*  
In all cases

*Study from 2018 Data Breach Investigations Report- Verizon
Number 1 asset involved in Breaches:

Databases
Why should we take action?

An Increasing tide of laws & legislation

- EU - GDPR
- AUS Privacy Act, Privacy Amendment
- US - HIPAA, DPA, SOX, CaCPA, S.H.I.E.L.D, NIST (draft, revision 5)...
- Everywhere - PCI DSS

Ongoing industry specific regulations & requirements

- Securities & Exchanges Commission (SEC) Federal Trade Commission, Commodity Futures Trading Commission (CFTC), The Financial Conduct Authority, NHS Digital...

Non-compliance results in fines or prison!
Data Compliance in Software Delivery

1. What do you process?
2. What needs protecting?
3. Who has access and for what purpose?
4. How can you demonstrate adequate protection?

Move from tell me to show me...

...consistent processes are key
Demo – Classifying sensitive data
“67% of organizations use a copy of the production database in development and testing.”

2018 State of Database DevOps Survey
65%
“67% of organizations use a copy of the production database in development and testing.”

2019
2018 State of Database DevOps Survey
Conflicts to solve

Developers

DBA
Conflicts to solve

Database Developers
- Evaluate software sooner
- Up-to-date, realistic data
- Production scale data
- Self-service access

DBAs
- Data must be protected
- All copies of data accounted for
- Sensitive data must be sanitized
DevOps as we know it is changing
DevOps as we know it is changing
Demo – Provisioning Databases
Stay Compliant AND use Production like Data
How does provisioning reduce your attack surface area?

<table>
<thead>
<tr>
<th></th>
<th>Production</th>
<th>Staging</th>
<th>Test/QA</th>
<th>Dev 1</th>
<th>Dev 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
</tr>
<tr>
<td>Staging</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
</tr>
<tr>
<td>Test/QA</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
</tr>
<tr>
<td>Dev 1</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
</tr>
<tr>
<td>Dev 2</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
<td>1TB</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>5TB</strong></td>
<td><strong>6TB</strong></td>
<td><strong>6TB</strong></td>
<td><strong>6TB</strong></td>
<td><strong>6TB</strong></td>
</tr>
</tbody>
</table>

PII is duplicated

<table>
<thead>
<tr>
<th></th>
<th>Production</th>
<th>Image</th>
<th>Staging</th>
<th>Test/QA</th>
<th>Dev 1</th>
<th>Dev 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production</td>
<td>1TB</td>
<td>1TB</td>
<td>50MB</td>
<td>50MB</td>
<td>50MB</td>
<td>50MB</td>
</tr>
<tr>
<td>Image</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staging</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test/QA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dev 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dev 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>1TB</strong></td>
<td><strong>1TB</strong></td>
<td><strong>50MB</strong></td>
<td><strong>50MB</strong></td>
<td><strong>50MB</strong></td>
<td><strong>50MB</strong></td>
</tr>
</tbody>
</table>

PII ONLY in PROD
My Ideal Data Sets

- Small curated data set
- Large, virtualized data set
Curated Sets of Data

Start with Production Data
• Additive Process – copying rows into a new database
• Subtractive – copy entire database, delete 90% of the data

Use Masking
• Use scripts or tools to de-identify/pseudonymize/anonymize
• Be careful

Inject Data
• Create known values for testing
• Brand new or based on existing masked data

Add Randomness
• Include new rows for edge cases
Compliant Database DevOps

- Standardize team-based development
- Protect and preserve data
- Automate database deployments
- Monitor performance & availability
Next Up: The Business Case – Set yourself up for success within three months

www.voiceofthedba.com
sjones@sqlservercentral.com
@way0utwest
/in/way0utwest