



Responding to Data Breaches

Sol Bermann
Chief Privacy Officer
State of Ohio - OIT
October 2, 2007



Basic Steps

1. Have a plan
2. Assemble & Organize
3. Conduct Initial Assessment
4. Contain Risk & Exposure
5. Reassess While Driving to Root Cause
6. Closing the Incident



Have a Plan

- ‘Nuff said!*

*Oh, and test it too



Assemble & Organize

- Cross-Functional Team (depending on scenario)
 - Privacy
 - Security
 - IT
 - Legal
 - Communication
 - Director-level representation
- Questions to Consider
 - How was the data compromised
 - Has the breach been contained
 - Type of information involved
 - Is notice necessary
 - Start the privacy/security incident response process?
- Assign an Incident Team Leader/Decision Maker
 - Initiate activity log (attorney-client privilege consideration)



Conduct Initial Assessment

- **ID what you need to know**
 - what data was breached (is it sensitive?)
 - whose data was affected
 - was the data protected (ex: encrypted, truncated)
 - is the breach ongoing
 - what system was compromised
 - does law enforcement need to be involved
 - are there business continuity implications
 - are there other legal implications
 - is notice necessary
 - individuals, credit bureaus, Fed govt., other entities
- **Work with legal to make sure appropriate privilege is maintained**



Contain Risk & Exposure

- Minimize risks/consequences of breach
 - Contain the breach
 - Develop plan for affected parties
 - Determine the response
- Develop 1-2 sentence summary of overarching response strategy
- Develop a communications plan (both internal and external)
 - Template holding statement on inquiries
- Provide notice
 - Review template letters
 - Check credit bureau process for notice
 - Set up call center
- Assign roles for each activity
 - Are their external stakeholders that need to be notified



Reassess While Driving to Root Cause

- **Does the team need to be expanded or modified**
- **Review & evaluate the cause of the incident**
- **Understand how stakeholders are affected**
 - Put yourself in shareholder shoes
 - Update stakeholder analysis
 - Call center updates, e-mail, media,
- **Mitigation Plan**
 - Ex: purchase credit monitoring



Closing the Incident

- **Develop a final reporting process**
 - Coordinate who will draft & review the final reports
 - Who prepares what report
 - Who receives each report
- **Specific actions resulting from incident**
 - HR review of employee actions
 - Legal/Policy review (is there a need to add or augment existing law/policy)
 - Business unit review (is there a need to review third-party contracts)
- **Document lessons learned**
 - What changes should be made
 - Assign for implementation
 - Assign team member to ensure recommended changes are followed, and to monitor any on-going activities related to the breach



Contact

Sol Bermann
Chief Privacy Officer, J.D., CIPP
State of Ohio - OIT

sol.bermann@oit.ohio.gov
614-644-9391