

Preparing for the Inevitable: the Anatomy of a Security Breach

Maximillian J. Bodoïn

*Holland & Knight LLP, Partner
Boston, Massachusetts*

Roadmap

- Introduction of new risks
- Obligations to protect against risks
- Proactive and reactive risk mitigation

Introduction of New Risks

- New sources and uses of data
- Significant added value
- Significant potential risk

Obligation to Protect Against Risks

- Statutory/regulatory framework
- Contractual obligations
- Reputational considerations

Obligation: Statutory Framework

- Various statutory obligations:
 - Security breach notification laws
 - Preventative InfoSec laws
 - Video Privacy Protection Act
 - Children's Online Privacy Protection Act
- No one ever steps in the same river twice.

Security Breach Notification Laws: Then and Now

Then	Now	
<p>Name plus:</p> <ul style="list-style-type: none"> • Social Security number • Driver's license number or State ID • Financial account number, credit or debit card number 	<p>Name plus:</p> <ul style="list-style-type: none"> • Social Security number • Driver's license number or state ID • Passport number • Checking account number • Savings account number • Credit card number • Debit card number • PIN • Digital signatures • Any other number that allows access to financial resources • Biometric data • Fingerprints 	<p>If access to financial account or resources:</p> <ul style="list-style-type: none"> • Email name or address • Internet account number • Internet ID name • Parent's legal surname • Passwords

Obligation: Contract

- Contractual obligations regarding data collection and usage
- Geolocation data – “greatest flashlight free”
 - Trending towards greater privacy protections.

Obligation: Reputational Harm

- Reputational harm can be as (or more) severe than statutory or contractual harm:
 - Undermine confidence
 - Impact adoption
 - Difficult to quantify

Mitigating Risk: Proactive Efforts

- Information security policies and procedures
- Internal risk assessments
- Independent third party information security audits
- Training
- Insurance

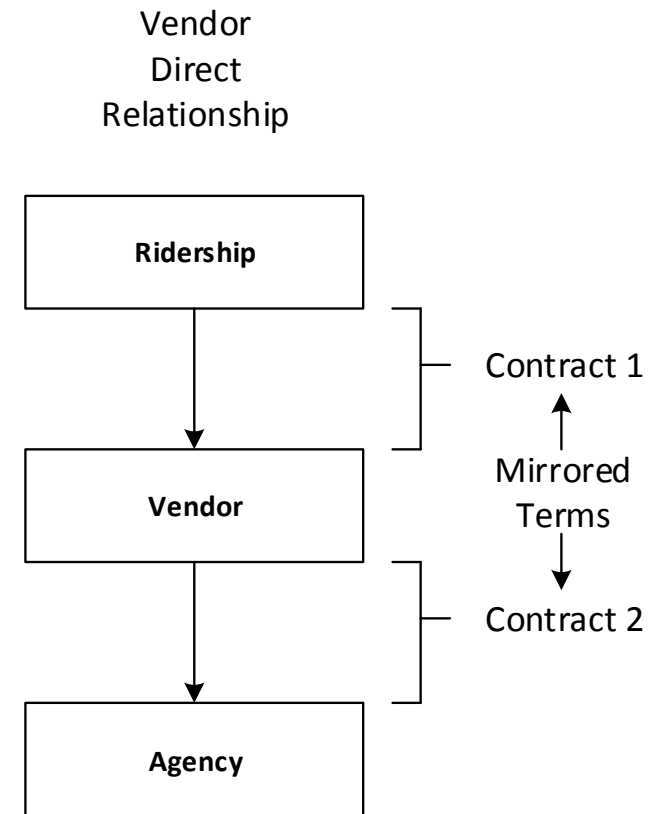
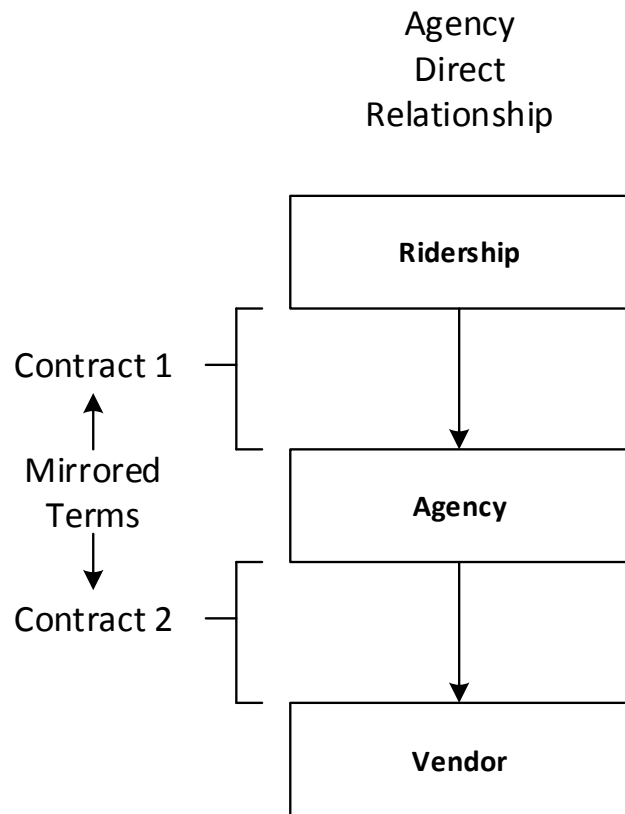
Mitigating Risk: Vendor Management

- Vendor management begins before the procurement process:
 - Project due diligence
- Vendor management continues during the procurement process:
 - Privacy by design
 - Security by design
 - Procurement due diligence

Mitigating Risk: Vendor Contract Considerations

- Compliance with proactive efforts
- Data collection and handling practices
- Securing data rights and data ownership
- Data breach response obligations
- Allocation of financial risk
- Transition services
- Subcontracting

Mitigating Risk: Downstream Contract Compliance



Mitigating Risk: Incident Response Plan

- Preparation
 - Written incident response plan
 - Response team: key internal members, legal counsel, third party vendors
- Detection and Analysis
 - Investigation
- Contamination, Eradication, and Recovery
 - Mitigation, insurance, public relations, law enforcement
- Post-Incident Activity
 - Risk assessments and changes to business practices
- NIST Computer Security Incident Handling Guide (Special Publication 800-61 Revision 2)

Mitigating Risk: NIST Incident Response Lifecycle

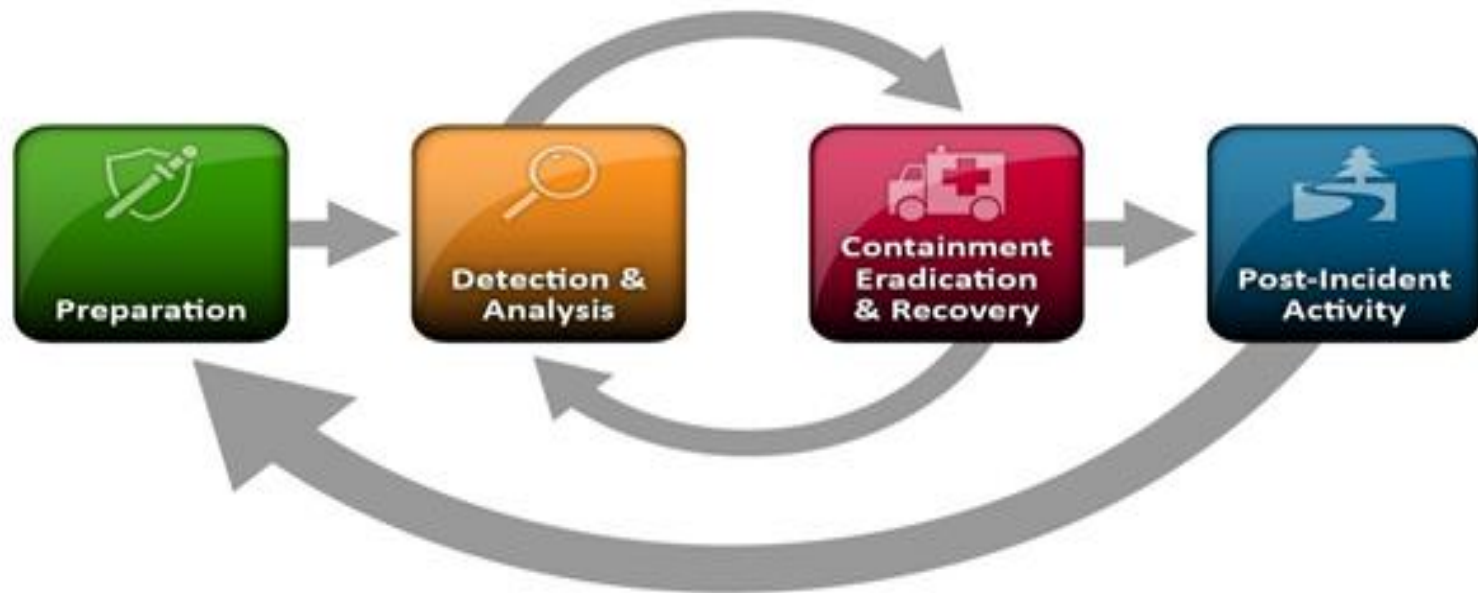


Figure 1 - Incident Response Lifecycle

Source: NIST
800-61 Revision 2

Questions

Maximillian Bodoïn | Holland & Knight

Max.Bodoïn@hklaw.com

617.573.5819

