Third Party Contracts: How Well Are You Protecting Client Confidential Information in the Hands of Your Third Party Providers

Fraser Mann
Richard Austin

November 19, 2019

Agenda

I. Introduction

II. Research and Due Diligence

III. The Third-Party Contract
- Contractual Issues
- Negotiation Issues

IV. Self-Help

V. Vigilance

I. Introduction

- The level of protection of information under the third-party contract is determined in advance

- The adequacy of the protection of information is evaluated with 20 – 20 hindsight

- Approaches:
  - Research/due diligence
  - Contract issues
  - Self-help
  - Vigilance

Why bother to Protect Information?

- Legal requirements
  - Statutes
  - Cases/decisions
  - Guidance

  … discussed in depth in earlier presentations at this conference

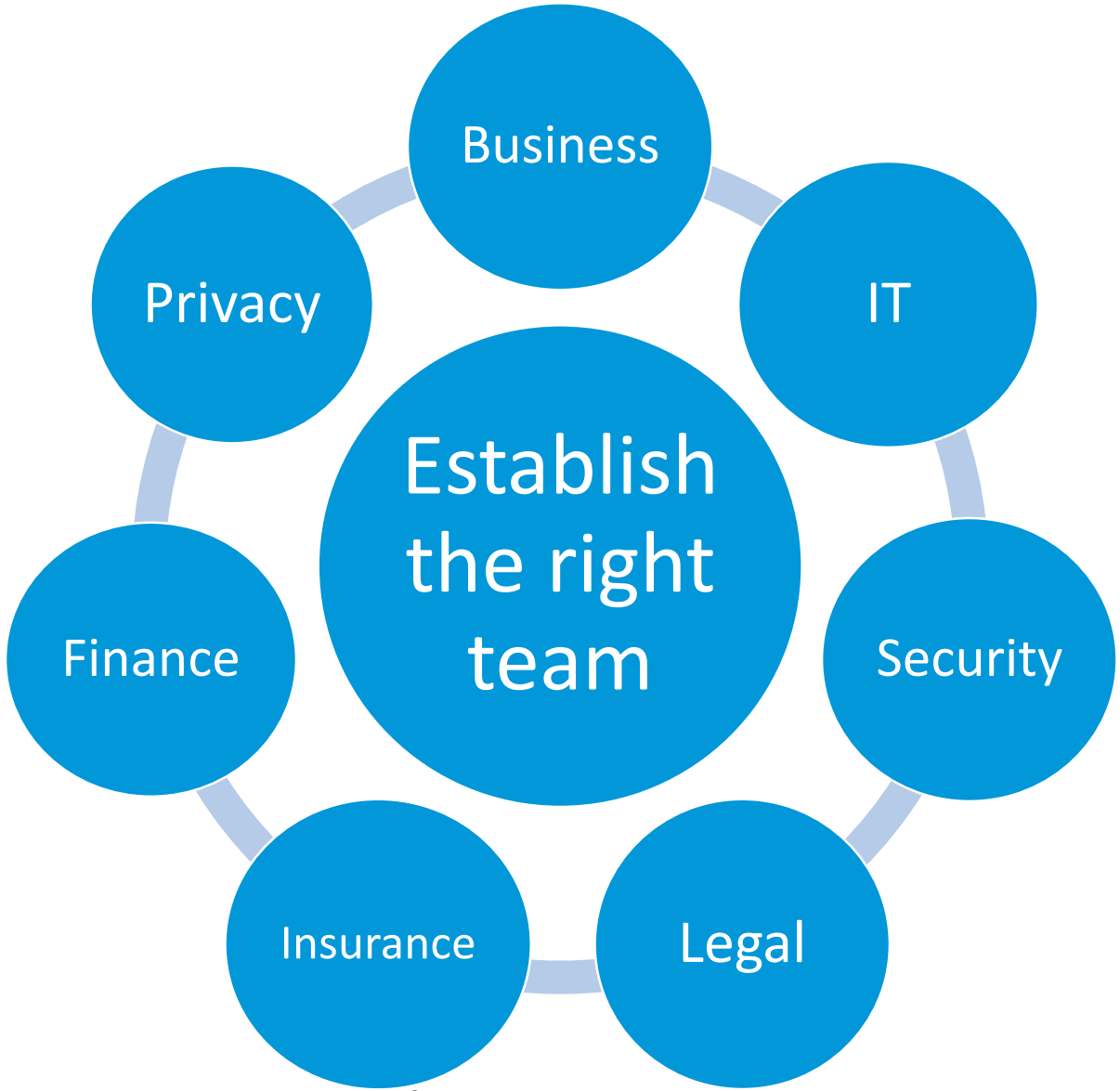
- Contractual commitments
  - To clients (*Terms of service, privacy policies, …*)
  - To suppliers (*Service agreements, license agreements, NDAs, …*)

- Other obligations

What is the Company Trying to Protect?

- Understand the information the Company is trying to protect
  - Now and in the future
- From what threats?
  - Now and in the future
- Under what regimes/in what jurisdictions?

Who Needs to be Involved?



II. Research and Due Diligence – The Who

Due diligence of Suppliers requires learning:

- **What are the risks relating to the Supplier's business?**
  - Financially stable
  - Ownership
  - Likely to be acquired or to divest key businesses
  - Supplier reputation and impact of disclosure of Supplier selection

- **What are the risks relating to the Supplier's business model for providing the services?**
  - Locations
  - Potential for conflict of interest
  - Stable well-designed infrastructure being used to provide the services
  - Subcontractor issues (including due diligence on key subcontractors)

Due Diligence cont'd

- **Maturity of the Supplier in relation to information security:**
  - Privacy practices
  - Security practices
  - Business continuity / disaster recovery plans and practices
  - Track record
    - Past incidents and disclosures
    - Past discussions with regulatory authorities

- **Transparency:**
  - Does the Supplier provide a reasonably-detailed description of the services?
  - Is the Supplier willing to commit to providing services that are consistent with the description?
  - When changes are being made to the services, is the process reasonably fair to Supplier's clients?
  - Is the Contract a "rabbit hole"?

Due Diligence cont'd

- **Is the Supplier willing to accommodate the Company's needs?**
  - Does the Supplier's agreement disclose the Supplier's willingness to be reasonable or is it just an attempt to exclude every possible liability?
  - Is the Supplier willing to consider revisions to its standard forms or using the Company's form of agreement?

III. Contractual Issues

1. Clear definitions:

- Confidential information
- Personal information
- Relating to data
  - Input / submitted data
  - Information derived from / generated by the services
  - Operating data:
    - Transient data
    - System data, e.g. operating and system logs

Contractual Issues cont'd

2. Clear statements on rights to data:

- Ownership of data
- Licenses

3. Clear statements on securing data and safeguards to be used:

- Physical, administrative and logical safeguards
- Logging, monitoring and auditing rights
- Periodic vulnerability assessments / penetration testing
- Compliance with standards, e.g.:
  - ISO 27001, 27002:, 27005, 27018, etc.
  - Statements of Applicability
  - Compliance versus Certifications
- Availability of Audit Results
  - SOC 1 Type II, SOC 2 Type II
  - PCI DSS Compliance Audits
  - Other tests, audits and reviews by or of Supplier

DW Deeth Williams Wall

MANN SYMONS LLP

Contractual Issues cont'd

4. Ensuring access:

- Safeguards:
  - Authentication, roles-based authentication
  - Multi-homing
- Service Levels:
  - Availability
  - Incident response and resolution
- Backups
- Export tools that give the Company the ability to take copies of its data from time to time, mitigating risks relating to the return of data or outages
- Return:
  - Commitment to return (addressing technical realities)
  - Format
  - Verification
- Destruction:
  - Safeguards
  - Addressing technical realities

Contractual Issues cont'd

5. Clear statements on Supplier's rights to use the information:

- Limits on information collection, use and disclosure:
  - Provide services
  - Ability to use information to improve products or services
  - Addressing anonymization and aggregation rights and obligations
- Confidential treatment

6. Clear statements on locations used by Supplier

- Storage
- Processing
- Access

Contractual Issues cont'd

7. Personnel-related provisions:

- Background checks
- Employee-awareness and training
- Rights of approval/ to require removal

8. Subcontracts:

- Customer's approval rights
- Flow down obligations
- Right to require removal

9. Breach incident response, management and notification:

- Notice and cooperation
- Recordkeeping obligations

Contractual Issues cont'd

10. Insurance

11. Liability

12. Governing Law and Jurisdiction

13. Enforceable Remedies for Non-Compliance

III.B Negotiation Issues

- **Objective** is to negotiate contractual provisions to allow the Company to comply with obligations

- **Challenges**:
  - "We never make changes to our standard contractual terms."
  - "These are industry standard terms."
  - "What you are asking for is unreasonable. No one has ever asked for that before!"
  - "That level of protection is not included in the price."
  - "That's a die-on-the-hill issue for us!"

Negotiations Issues cont'd

- **Negotiations are like any other commercial negotiation:**
  - Power dynamics affect what can be obtained:
    - Value of the contract
    - Relative importance of the contract to each party
  - Technical issues affect what can be obtained:
    - Cannot commit to 256b encryption if part of the infrastructure still relies on 128b
    - Supplier's dependence on its subcontractors
  - Formal procurement processes can shape the negotiation
  - Company must understand its BATNA

Negotiations Issues cont'd

- **Develop a Negotiations Plan:**
  - Identify the changes necessary for legal compliance:
    - Requiring a change based on specific statutory requirements is compelling
  - Identify the changes that support legal compliance even if not legally required
  - Identify key changes unrelated to legal compliance and understand why they are important

- **Distinguish between Supplier needs and Supplier wants:**
  - Understand the Supplier's needs
  - Contract provisions in a Supplier's standard agreement relating to needs may be, often are, drafted more broadly than required

Negotiations Issues cont'd

- **Some things (of many) to be careful about:**
  - Disconnects between service descriptions and contract commitments
  - References to (non-static) websites and URLs
  - Unilateral change provisions including changes to Supplier's policies
  - Being asked to comply with hundreds of pages of documentation incorporated by reference

- **Develop a negotiations plan and stick to it:**
  - Define the escalation path and conditions for escalation
  - Eliminate the "back channels" and attempts to undermine confidence in the negotiations team

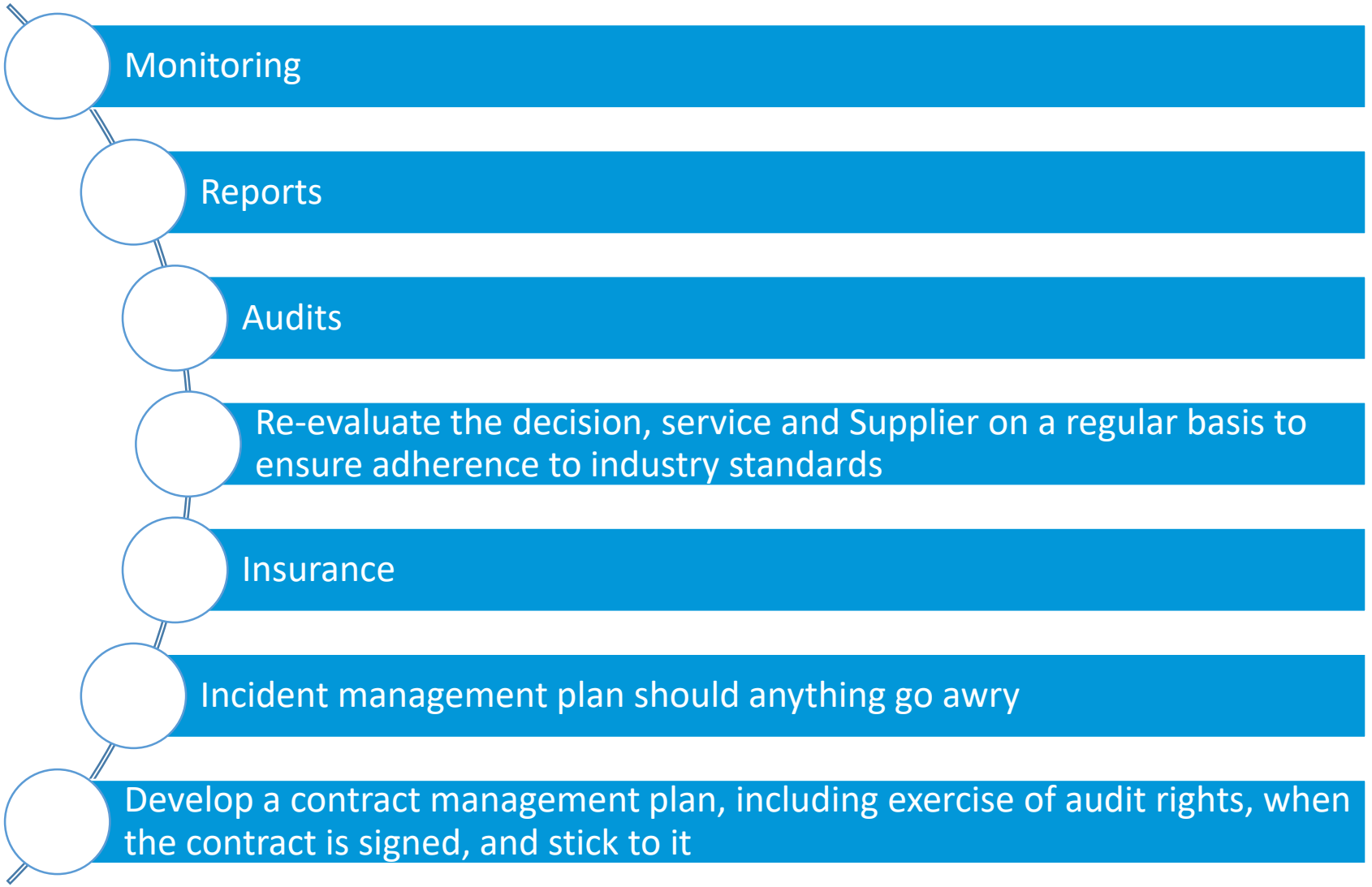
IV. Self-help

- Self-help is about what the Company can control and creativity

- No one-size fits all, e.g.:
  - Export functions to help with accessibility issues
  - Tokenization can help with weaker confidentiality provisions
  - Only permitting certain third-party solutions with specific classes of information
  - …

- Business, technical and legal staff and SMEs need to work together to develop instances of self-help on a case-by-case basis

V. Vigilance


Monitoring
Reports
Audits
Re-evaluate the decision, service and Supplier on a regular basis to ensure adherence to industry standards
Insurance
Incident management plan should anything go awry
Develop a contract management plan, including exercise of audit rights, when the contract is signed, and stick to it

Questions?

Richard Austin
Partner, Deeth Williams Wall LLP
(416) 941-8210

raustin@dww.com

Fraser Mann
Partner, Mann Symons LLP
(416) 274-2243

fraser@mannsymons.com

Deeth Williams Wall LLP
Lawyers, Patent & Trademark Agents

DWW.com

MANN SYMONS LLP

mannsymons.com