The Technology Agreement of Things: What are the challenges in dealing with Vendors?

Presentation to SPIAO May 27, 2018 by York Region

Zella Phillips - Senior Counsel, IT and Corporate Law

Marie Endicott – Supervisor Risk Analysis

York Region

What are we going to talk about

- Technology
- Exposure assessment

  (Security, Privacy, Risk Management, & Legal)
- Agreement key clauses
- Sub-contractors
- What success looks like

York Region

https://www.youtube.com/watch?v=nG36lKhy7ko

Technology Agreements

- Technology means
  - ✓ Hardware
  - ✓ Software
  - ✓ Professional Services
  - ✓ Maintenance
  - ✓ Licensing
  - ✓ Hosting

York Region

Where does the engagement of Others fit in?

- Information is an asset
- How to stop or control a breach

Exposure Assessment

- 4 Main Areas to Assess
  - ✓ Security
  - ✓ Privacy
  - ✓ Risk
  - ✓ Legal

Security

Cybersecurity Myths

WE CONDUCTED AN INTRUDER TEST

The test should cover the entire infrastructure so that the company can quickly eliminate all discovered vulnerabilities.

WE'VE NEVER BEEN ATTACKED SO OUR SECURITY SYSTEM MUST BE GOOD

Caution: threats continue to grow and become more complex.

WE'VE DESIGNED HIGH-END SECURITY TOOLS

Security tools are only effective when properly configured, integrated and controlled within all security operations.

WE COMPLY WITH INDUSTRY REGULATIONS AND BEST PRACTICES

Compliance requirements often only meet the minimum safety measurements and not all critical systems and information.

A THIRD PARTY PROVIDER RUNS OUR SECURITY

Regardless of the competence and capabilities of the provider, the question is whether complex threats in a company will be taken seriously enough for a third party to sufficiently protect it.

WE'VE INVESTED IN STRICT SECURITY CONTROLS

It is not enough to rely on standard IT security controls alone. Critical business elements should be above all protected.

OUR SECURITY IS MANAGED ADEQUATELY BY THE IT TEAM

A threat can take over an entire business. Therefore, management should work closely with IT.

WE ONLY NEED TO SECURE OUR INTERNET APPLICATIONS

One should also be equipped against internal threats and member / staff abuse.

WE'VE COMPLETED OUR SECURITY PROJECT

Security is an ongoing project that can never be completed.

WE AREN'T STATISTICALLY AT RISK

Every company is at risk for a data breach and should be prepared.

Cybersecurity Program

SECURITY GOVERNANCE AND MANAGEMENT	Policy & standards, strategy & operating model, risk management, training & awareness, third party security, physical security, business continuity, business engagement, metrics & reporting, asset management, human resources security
THREAT AND VULNERABILITY	Threat intelligence, vulnerability management, compliance monitoring, security incident management, penetration testing, event response and investigation
ACCESS AND IDENTITY MANAGEMENT	Provisioning & deprovisioning, user management, role based access control, multi factor authentication, access certification
APPLICATIONS	Secure system devices, code review, developer training, application protection, cloud protection
INFRASTRUCTURE	Security architecture, malware protection, web and email security, network protection, security hardening
DATA	Privacy, data classification, data protection, data back-up and availability, data discovery and monitoring, mobile device security

Security

- Vendor Security Questionnaire

Privacy

- Personal Information/Health Information
- Legislation (MFIPPA, PHIPA)

Privacy

- Privacy/Security Threshold Assessment (PSTA)
- Privacy Impact Assessment (PIA)

Risk Management

- Risk assessment tool for procurement
- Scope of work
- Type of vendor
- Information exposures
- Impact on the Region
- Impact on Residents or third parties
- Risk transfer requirements

Legal

- RFP and Agreement
- Agreement renewal
- Form of agreement
  - EULA (End User License Agreement)
  - SOW (Statement of Work)
  - MSA (Master Subscription Agreement)
  - SLA (Service Level Agreement)
  - Hosted Service Agreement
  - Terms & Conditions from Vendor website
  - Support & Maintenance Agreement

Agreement Specifics (no particular order!)

- Intellectual Property
- Retention of information
- Responsibilities in the event of a breach
- Privacy Legislation
- Ownership of data

Agreement Specifics

- Indemnification
- Limitation of Liability
- Insurance
- Payment Clauses
- Service Levels

Agreement Specifics

- Warranties
- Confidentiality
- Governing Law
- Termination Clause
- Ownership/Right to Use (Source Code / Object Code)

YR Agreement Specifics

- MISA wording
- Cloud Terms & Conditions
- Risk Transfer Clauses
- Direct and indirect damages
- First Party and Third Party
- Insurance Requirements

Sub Contractors

- Will the agreement app/y to subs?
- Do you know if your have subs?

MAKE SURE YOU ASK!

- YR example

What to look out for

- Non-direct damages
- Force Majeure
- Limitation of Liability
- Indemnification
- Data Ownership
- Data Retention & Deletion

What does success look like

- LOL to value of insurance
- Non-direct damages to cover network security information & privacy
- Indemnification from vendor
- In accordance with Ontario Law
- Payment milestones

Don’t forget about all of the other stuff – a good contract can only do so much to manage the risk

- Organization security
- Threat assessment & monitoring
- BCP’s
- Table top breach exercise

Questions