fogler rubinoff

8th Annual Information Privacy and Data Protection Conference

December 1, 2016

The 7 Step Information Security Compliance Program

Ravi Shukla
Partner – Fogler, Rubinoff

1. Initial Data Mapping and Classification Stage

- Identification process should commence at the business unit level and be considered to have been fully completed only after an enterprise-wide assessment has been made.

- Organization should determine what its key assets are, where they are located, as well as their relative value.

- Where program is implemented iteratively, priority can be given to promptly enhancing the security parameters attached to the “crown jewels” (digital and non-digital formats).

2. Vulnerability Assessment

- Vulnerability assessments identify both the nature and scale of the internal risks which are present and should encompass both electronic format and traditional paper format assets.

- Such assessments are generally conducted simultaneously with a penetration test – which assess, as of a specific point in time, whether and how a third party could intrude into the organization's network.

- The insider element needs to form part of the security strategy along with an examination of external threats.

3. Incident Response Plan (IRP)

- Who has lead responsibility for different elements of the organization's response?
- How are critical personnel (or their back-up if required) to be contacted ?
- What data, networks, or services should be prioritized for the greatest protection?

Incident Response Plan (IRP) – cont'd

- How is data related to the incident to be preserved in a forensically sound manner?
- What criteria will be used to ascertain whether data owners, customers, or third party organizations should be notified?
- What are the procedures for notifying law enforcement?

4. Vendor Assessment

- Organizations need to account for data held by business partners, vendors and other third parties.

- Mandatory security requirements for vendors that may access, process, transmit and/or store the organization's information or have access to the organization's networks such as:

Vendor Assessment – cont'd

- deployment of an executive sponsored information security organisational function;
- limitations on permitted locations for data storage;
- deployment of a human resources security program;
- asset management requirements;

Vendor Assessment – cont'd

- access control requirements;
- restrictions on storing information on personally owned devices;
- use of minimum two-factor and/or multifactor authentication methods;
- operations security requirements;

Vendor Assessment – cont'd

- use of only documented change management procedures;
- cryptographic requirements;
- information security incident management requirements; and
- back-up requirements.

5. Insurance Coverage

- Gaps in the protection(s) provided by traditional coverage.
- For now, many insurance policies primarily cover the costs of business interruption, data destruction, and extortion in cases where "ransomware" was deployed.
- Insurers will generally charge higher deductibles than they would for other forms of corporate insurance.
- Is useful for organizations to go through the potential insurer’s vetting process.

6. Compliance Obligations

- Compliance requirements can arise from legislation, regulatory regimes (OSC, TSX), industry associations (PCI) and/or common law developments.

- PIPEDA is general Canadian federal legislation and its purpose is to establish rules that recognize both the right of privacy of individuals with respect to their personal information, as well as the needs of organizations engaged in commercial activities to collect, use and/or disclose PI for purposes that a reasonable person would consider appropriate in the circumstances.

Compliance Obligations – cont'd

- PIPEDA mandates the deployment of a customer facing Privacy Policy, an internal Privacy Policy, internal IT Security Standards and an internal Information Retention Policy as well as suitable training efforts in respect of the latter 3 policies.

- Provincial governments in Alberta, British Columbia and Quebec have enacted substantially similar comprehensive private sector privacy legislation.

Compliance Obligations – cont'd

- Ontario, New Brunswick, and Newfoundland and Labrador have privacy legislation, which applies to personal health information that has been declared substantially similar to PIPEDA with respect to health information custodians.

- Other provinces and territories have also passed their own health privacy laws. In some cases PIPEDA may still apply.

Compliance Obligations – cont'd

- The following three elements must be satisfied in order to establish the tort of intrusion upon seclusion:
  - the defendant's conduct must be intentional;
  - the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns; and
  - a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish.

Compliance Obligations – cont'd

- Intrusion upon seclusion is a common law cause of action for breach of privacy first recognized in 2012 in Ontario.

- Liability for tortious intrusion upon seclusion has fallen in the general range of $10,000 to $20,000. When multiplied by the number of individual plaintiffs who are often included in a class action, the overall potential monetary exposure may be very significant.

Compliance Obligations – cont'd

- Judicial support in Ontario for the proposition that a second common law cause of action for breach of privacy exists for which the elements are:
  - a person publicizes the private affairs of another;
  - the matter(s) publicized or the act of the publication would be highly offensive to a reasonable person; and
  - the private affairs are not of legitimate concern to the public.

Compliance Obligations – cont'd

- The plaintiff was awarded $100,000 in damages (the maximum available procedurally).

- A statute-based breach of privacy claim can potentially issue in British Columbia, Saskatchewan, Manitoba and Newfoundland (a similar provision is also included in the Quebec Civil Code). Key elements underlying any such statute-based claim are:

Compliance Obligations – cont'd

- no proof of damages necessary;
- the defendant's alleged actions must have been undertaken willfully and without a claim of right; and
- the defendant's alleged actions must have been undertaken with knowledge.

7. IS Risk Management

- Now be in a position to knowledgeably (meaning with the goals clearly defined) understand the organization's “full risk universe”.

- Seek alignment of the enterprise level information security risk management strategy and the overall business strategy.

IS Risk Management – cont'd

- After obtaining "buy-in" at the Board level, can allocate the resources (establish the IS budget and organizational structure) intended to ensure the proper management of those risks.

- Threat patterns are continuously evolving.

- Effective information security strategy depends on a "layered" approach that needs to be monitored continually and updated regularly.

fogler rubinoff

THANK YOU

Ravi Shukla
rshukla@foglers.com
416.864.7612