Vendor Management Challenge
Doing More with Less

Megan Hertzler
Assistant General Counsel
Director of Data Privacy
Xcel Energy

Boris Segalis
Partner
InfoLawGroup LLP

Session ID: GRC-402
Session Classification: Intermediate

RSA CONFERENCE 2012

Why You Should Care: From the Trenches

- Let's talk "personal information"
- What are the real-world consequences of failure to address data privacy and security in the contracting process?
  - Time - Distractions for highly skilled human resources that could be spending time adding value to the business
  - Money - Overtime, consultants, counsel, breach notice costs; often unrecoverable
  - Embarrassment, Reputation, Morale, Investigations = Money!
- Real-world examples of failed process
  - No data protection due diligence at the outset
  - Agreement with vendor did not address data security terms beyond general obligation of confidentiality
  - Any guess what happened next?

Why You Should Care: Example A

Employee information stolen from vendor's unencrypted laptop

Vendor informs customer concurrently with sending notice of the breach to customer's employees

- Customer does not have time to:
  - Prepare internal call center FAQs
  - Draft employee communications
  - Ascertain responsibilities under the law
  - Ensure vendor communication to employees is compliant

Why You Should Care: Example B

- Upgrade results in exposure of SSNs
- Delay notifying customer for a month
- Short window between telling customer and providing notice to customer's employees
- Customer placed under time crunch and has no leverage in the notification process

Learning Objectives

- Enhance awareness of legal and business requirements
- Identify business challenges for front line negotiation team
- Develop vendor management tools for front line personnel
- Implement effective compliance oversight

Outsourcing Benefits & Challenges

Benefits	Challenges
▪ Reduced cost ▪ Better technology ▪ Competitive advantage	▪ Privacy and data security ▪ Negotiation team knowledge ▪ Delay ▪ Increased costs ▪ Costly surprises

Vendor Management Solution Roadmap

- Understand obligations and consequences of inaction
- Make privacy and security integral part of selection process
- Classify data based on risk
- Develop contracting tools and options for front-line personnel
- Provide training and awareness
- Share compliance burden

View From Space: What's Our Goal?

- Select vendors that take privacy and security seriously
- Engage and empower company resources to make informed judgment calls
- Be flexible in privacy and security requirements
- Help vendors avoid and mitigate privacy and information security issues by providing guidance

Legal Requirements

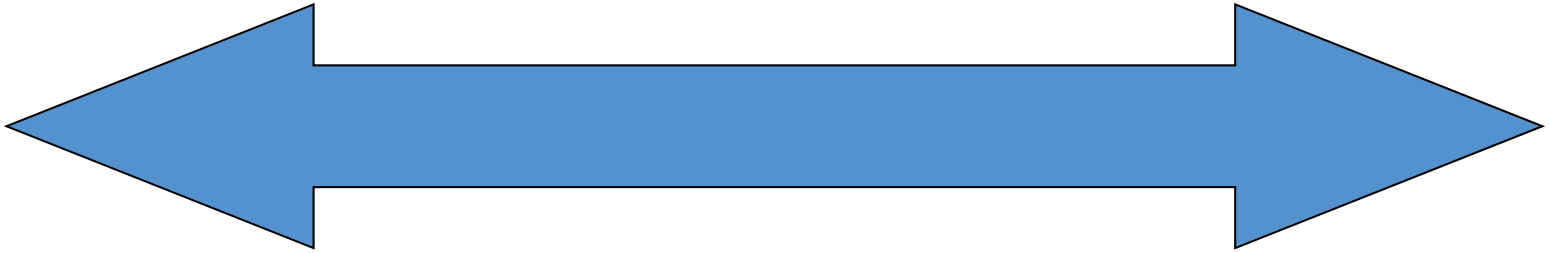
Vendor Oversight	Derivative Liability
▪ State information security laws ▪ Federal (GLB, FCRA Red Flags, HIPAA) ▪ Foreign (EU Directive and local laws)	▪ Pending federal legislation ▪ State breach laws ▪ HIPAA ▪ Foreign (EU Directive and local laws)

Contracting Lifecycle

- Integrate privacy and security into the process
  - Documented in a single resource: “Playbook”
- Program must address all stages of the lifecycle
  - Data Classification
  - Project Initiation
  - RFP
  - Negotiation
  - Oversight

Vendor Management Tools – Data Classification

More Sensitive ⟷ **Less Sensitive**



- PHI
- NPI
- Payment card data

- Consumer report data
- Breach data
- EU sensitive data
- Other data business deems sensitive

- Everything else that identifies an individual or device

Vendor Management Tools – Project Initiation

- Project initiation survey answers threshold questions
- IT and Legal use judgment to evaluate responses and determine path forward
  - Is Personal Information involved?
  - Will vendors have access to the data? Is it an existing relationship?
  - Sensitivity of data, type of data subjects
  - Type of disclosure and its purpose
  - Volume of disclosure & associated risk
  - Initial assessment of risk – issue spotting
  - Cross-border data transfer issues

Vendor Management Tools – Project Initiation

Question	Response	Next Steps
Where are the individuals to whom the information pertains located?	Check all that apply: U.S. ☐ EU/EEA/Switz ☐ Others (List): ☐	▪ Determine whether Agent must establish a legal basis for cross-border transfer of Personal Information

Vendor Management Tools – Project Initiation

Question	Response	Next Steps
To how many individual records will service providers have access?	1-999 ☐ 1,000-9,999 ☐ 10,000-99,999 ☐ 100,000-499,999 ☐ 500,000 or more ☐	▪ Determine whether to require Agent to obtain information security incident insurance coverage

Vendor Management Tools – Project Initiation

Question	Response	Next Steps
Will third parties have access to Personal Information that has been anonymized or aggregated?	Yes ☐ No ☐ TBD ☐ If Yes, describe data:	▪ Because of re-identification concerns, access to anonymized or aggregated data still requires , Data Protection Assessment Questionnaire

Vendor Management Tools – Vendor Assessment

- IT and Legal are key stakeholders in building an assessment tool
- Focus on processing information, not just on gathering it
- Include with RFP (existing vendors complete for new projects)
- Ability to safeguard data becomes evaluation criteria
- For single-source, assessment is the basis of due diligence and follow-up
- IT leads evaluation with help from Legal
  - Judgment, not scoring

Vendor Management Tools – Vendor Assessment

Question	Response	CRI	CI	Evaluation
Will service provider access, collect, store, use, disclose or otherwise process Personal Data in aggregated or de-identified format?	Yes ☐ No ☐ If yes, describe aggregation method	▪ Verify information will not be used other than for the benefit of customer and that information cannot be re-identified.	▪ Same as CRI	Acceptable ☐ Not Acceptable ☐ Additional Due Diligence Required ☐

Vendor Management Tools – Vendor Assessment

Question	Response	CRI	CI	Evaluation
Does service provider regularly test and monitor key administrative, technical and physical controls, systems and procedures that safeguard Personal Data?	Yes ☐ No ☐ If yes, how often is testing performed?	▪ Required; evaluate the response in light of heightened risks associated with processing CRI	▪ Required; evaluate the response in light of lower risks associated with processing CI	Acceptable ☐ Not Acceptable ☐ Additional Due Diligence Required ☐

Vendor Management Tools – Vendor Assessment

- Assessment based on information gathered and business judgment
  - Security / privacy must be balanced against business interests
  - Zero-tolerance approach is insufficient and implacable
- After assessing, engagement is key
  - Work with vendors to meet requirements
  - Automate evaluation mechanics, not the thought process

Vendor Management Tools – Negotiation

- Key negotiation points
  - Sensitive data vs. less sensitive data
  - Information security incident definition
  - Scope of legal privacy/data security obligations
  - Sub-contractor oversight requirements
  - Information security incident reporting requirements
  - Record-keeping requirements

Vendor Management Tools – Negotiation

- FAQs empower front-line personnel respond to questions

Q: Are privacy and security concerns implicated when Service Provider has the ability to access or actually accesses Personal Data, but does not store it?

A: Yes. The privacy and security provisions of the Service Provider Personal Data Privacy, Confidentiality and Security Schedule apply to the Processing of Personal Data. Processing encompasses any operation or set of operations performed upon Personal Data, such as accessing, obtaining, storing, transmitting, using, maintaining, disclosing or disposing of the information. Once Service Provider has the ability to access Personal Data, there is a possibility that the information may be lost, stolen or otherwise mishandled, which in turn raises significant privacy and security concerns for Xcel Energy.

Vendor Management Tools – Negotiation

- Pre-determined negotiating positions provide negotiating flexibility

Default Provision	Objections	Response	Fallback Provision
1.4 Industry Standards means industry standards and best practices relating to the privacy, confidentiality or security of Personal Data…	▪ Definition is too broad and does not provide sufficient specific guidance	▪ Compliance with industry standards often is a potential minimum benchmark (regulatory compliance, common law negligence, reasonable)	**1.4** Industry Standards means [the ISO 27001/27002]

Vendor Management Tools – Negotiation (con't)

Default Provision	Objections	Response	Fallback Provision
2.6.1 Notify Company within 48 hours of any reasonably suspected Information Security Incident…	▪ We need more time to confirm whether an Incident actually occurred	▪ Must inform ASAP as soon as vendor reasonably suspects an incident has occured	**No fallback**

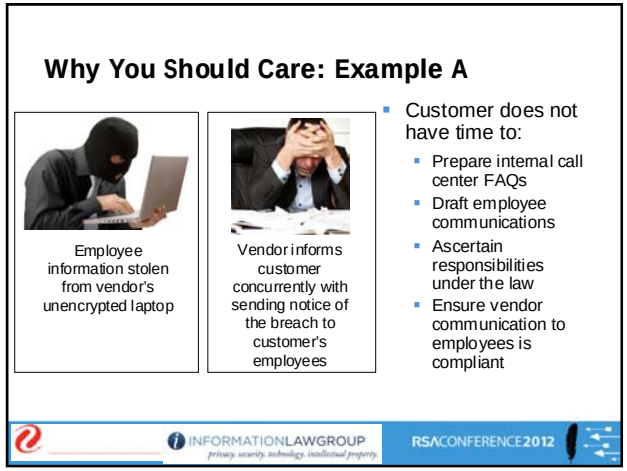
Vendor Management Tools – Oversight

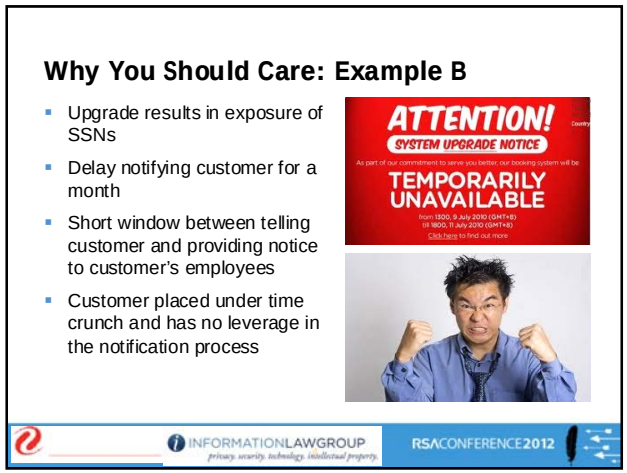
- Oversight is an integral part of a vendor management program
- Should be a collaborative process, designed to help vendors meet your requirements
  - Recommended privacy/security controls
- Focus on prevention
  - Risk assessment process
- Cooperate if something goes wrong
  - Incident investigation process
  - Breach notification process

From the Trenches: A Brighter Future

- Goal: data protection concerns are raised early in the contracting process
- Benefits of early action:
  - Vendor refuses contractual protections for SSNs; determined that vendor did not need access to SSNs and worked on replacing vendor for future projects
  - Customer avoids engaging vendor that was unable to identify/commit to countries where data would be processed, contrary to customer's data protection requirements

From the Trenches: What if?





- Different vendors
- Early notice for impacted individuals
- Customer would have been the decision maker
  - Response strategy
  - Notice
  - Legal obligations
- Indemnification for legal cost

Apply Program

- Within 3 months evaluate existing vendor management program
  - Identify vendors that have access to PI
  - Review contracts
  - Engage senior management
  - Follow up with vendors
- Within 6 months prepare key vendor management tools
  - Project assessment questionnaire
  - Vendor assessment/annual reporting questionnaire
  - Get assistance with contractual terms

Questions?

Megan J. Hertzler

Assistant General Counsel & Director of Data Privacy

Xcel Energy

Megan.hertzler@xcelenergy.com

612.215.4589

Boris Segalis

Partner

InfoLawGroup LLP

Bsegalis@infolawgroup.com

646.389.1289