Identifying and Managing Third Party Data Security Risk

Buckley Sandler LLP

Legal Counsel to the Financial Services Industry

Digital Commerce & Payments Series Webinar

April 29, 2015

Introduction & Overview

- Today's discussion:
  - What is third party risk?
  - Why should companies care?
  - How do companies assess it?
  - What are the criteria used to develop a framework to manage the risk?
  - How do you deal with residual risk?

Vendor Management: Popular with the Financial Regulators

- Since April 2012, the federal financial regulatory agencies have issued or taken:
  - At least 15 enforcement or similar actions based at least in part on third party oversight
  - At least 18 guidance documents addressing how financial institutions must manage third parties
  - At least six notable other public statements on the obligation to oversee third parties

Evolving Regulatory Expectations

- **OCC Bulletin 2013-29 (10/30/13)**
  - Updates and replaces OCC Bulletin 2001-47
  - Enhances and augments the previous Bulletin in many notable areas
  - Most detail of any regulatory guidance
  - Failure to have in place effective risk management process commensurate with risk and complexity of relationships "may be an unsafe and unsound banking practice"
- **FRB Supervisory Release 13-19 (12/5/2013)**
  - Addresses risks from "service providers"
  - Intended to build on the FFIEC Examination Handbook and be consistent with the OCC guidance

Securities and Exchange Commission

- Cybersecurity Examination Program in 2014
- Several questions on third party oversight in cybersecurity
- Results announced in February 2015
- Noted some findings relating to vendors

Some Primary Requirements in Privacy & Data Security

- The Gramm-Leach-Bliley Act
- HIPAA/HITECH
- State laws and regulations
  - Massachusetts
  - California
  - Nevada

Service Providers

- A defined term in the context of privacy and data security
- In reality often read to be much broader
- Service Provider – Vendor – Third Party
- Does the terminology matter?

OCC states:

A third party relationship is any business arrangement between a bank and another entity by contract or otherwise.

Buckley Sandler LLP

Security Breaches & Vendor Management

- Notice requirements under the breach requirements
- Contractual requirements
- Aftermath of an incident

New York State Department of Financial Services on Third Party Risk

- **May 2014** – Reported survey results of 150 banking organizations that highlighted the industry's reliance on third party service providers for critical banking functions as a continuing challenge
- **December 2014** – Announced new examination procedures focused on cybersecurity and included examination procedures and questions on:
  - Third party provider management
  - Third party service provider **vetting, selecting, monitoring & due diligence**
- **April 15, 2015 –** Published an update on Cybersecurity in the Banking Sector: Third Party Service Providers
  - 95% of banking organizations **conduct specific information security risk assessments** of at least their high-risk vendors
  - While nearly all have policies that require reviews of information security practices both during vendor selection and periodically, only **46% required pre-contract on-site assessments** and **only 35% required periodic on-site assessment** of at least high-risk third party vendors
  - While most institutions require vendors to represent they have established minimum security requirements, **only 36% require those security requirements** be extended to subcontractors
  - 68% of the surveyed institutions (78% of large institutions) **carry insurance** to cover cybersecurity incidents. However only **47%** reported having cyber insurance that explicitly **cover information security failures by a third-party vendors**.

Key Steps in Any Third Party Security Risk Process

- Understand the business and its environment
  - Industry
  - Legal & regulatory
  - Marketplace
  - Geography
- Identify the inherent data security risks (e.g. risk catalogue), the controls necessary to mitigate those risks, and the level of acceptable residual risk
- Evaluate the nature of the relationship with the third party
  - Business process, service performed, product provided
  - Data asset – access, use, share, cross-border transfer
  - Technology - level of integration, outsourcing
- Perform an assessment to determine:
  - The ability of the third party to comply with requirements (governance, controls, skill-sets)
  - Classification of risk the third party poses to the company (high, medium, low)
- Determine the risk level of the third party provider
- Identify additional controls necessary to reduce risk to an acceptable level or determine if an exception and risk acceptance process is applicable
- Incorporate controls and requirements in contracts and agreements (e.g. right to audit)
- Assess periodically to determine:
  - Compliance with contract and agreement
  - Any changes that would impact the risk profile

Third Party Risks: Types of Risks

When assessing third party security risks it is important to consider the impact on the financial, operational, regulatory, market and reputational risk of the business. Areas of potential risk in pre- and post contract security assessments include:

Governance	**HR/Skillsets**	Vulnerability – Incident Mgmt	Physical Security	BYOD
Board Involvement Sr. Management "Tone at the Top" Awareness /Leadership	Background checks Skill-Set Levels Appropriate Authority Access to Leadership CISO or CISO Equivalent	Intrusion Detection Patch Management Attack & Penetration Testing	Perimeter "Clean Desk" Policy Secure Disposal Techniques Credential/Access Monitoring	BYOD Initiatives Encryption Remote Wipe Data custodianship & Sharing
Enterprise Program	Breach Response	Outsourcing Risks	Logging and Monitoring	Resilience
Governance Structure Policies, Procedures Security Program Privacy Program Funding	Common definitions Established response plan Communication Protocols Response Tming	Availability Compliance & Enforcement Location Access & Data Sharing	Architecture Retention Aggregation Anomaly Recognition Periodic Review	Availability Disaster Recovery Business Continuity On-Going Assessing Change Management
Data Assets	Fourth-party Risks	Cloud / Virtual	Encryption	M&A / Spin-off
Classification/Sensitivity Sharing & Use Cross-border Transfer Onward Transfer Re-Identification	Sub-contractors - Serial Complexity Location Availability Communication	Cloud Architectures Cloud Providers Viability Control Responsibility Multi-Tenancy Environment Availability & Accessibility	Enterprise Strategy Key Management Storage & Transit	Data Ownership Custodianship Privacy Policy Co-Mingling

Assessments & Assurance

Initial security risk assessment:

- May involve the use of a questionnaire, and on-site review or both
- A scoring mechanism may be used to score individual questions or security and privacy control areas
- Scores may be aggregated and ranked in a scorecard indicating high, medium, or low risk

Security Assessment Response Scorecard

Categories prioritized by risk level identified by assessment scoring

Category ID	Security Area	Risk	Total Risk Score
7	Training and Awareness		5
3	Enterprise Privacy Program		5
1	Enterprise Risk Function		5
4	Enterprise Security Program		5
10	Perimeter – Boundary, Control		5
18	Threat & Vulnerability Management -		5
25	Cloud Architecture – Outsourced provider		5
23	Privacy Resources / Skill-sets		5
12	Security Resources / Skill-sets		5
28	Data in Transit-email		5
27	BYOD - Encryption / Protection		5
29	Laptop / Desktop Encryption		5
8	Data Asset Definition – Classification, Profiles		5
5	Privacy Policy Development		5
6	Security Policy Development		5
22	Third-party Management		5
34	Assess & Audit		5
20	Breach Response		5
15	Applications – SDLC		5
30	Server / Data Storage/ Back-up Encryption		5
14	Identity & Access Management – Credential Process		5
21	Privacy Operations: Notice, Choice, Redress		5

Periodic security risk assessments:

- May be correlated to "risk ranking" of the third party or the criticality of the business process or data asset involved
- High risk third parties may be required to obtain third party audits (e.g. SOC-2)
- Third parties with access to credit card data may be required to undergo PCI audited
- Medium or lower risk entities may be assessed through as part of the internal audit rotation or a self-assessment process
- The frequency of the audit/assessment process may also reflect the risk ranking

Risk Level	Assessment Type	Time Period
HIGH	Third Party Audits: PCI SSAE 16 - SOC-2, SOC-3	Annually
MEDIUM	Internal Audit + Self assessment	2-3 year rotation Annual
LOW	Self Assessment	Annual or bi-annual

Buckley Sandler LLP

Risk Factors

Some factors that may be considered in "risk ranking":

- Specific regulatory or industry requirements
- Critical infrastructure status
- Sensitivity or criticality of data assets
- Financial value of transaction or services
- Volume of data or transaction level
- Complexity of the business model of the third party
- Maturity of the program or control environment
- Geographical location, cross border data transfer
- History of breach
- Highly integrated architecture with broad access
- High degree of publicly facing websites/access
- Serial outsourcing (4th party) or ecosystem ("nth" party) environment

Cyber: Practical Steps

- Revise policies, procedures, and training materials
- Assess response plans in light of industry trends and recent incidents
- Planning and conducting of breach preparedness exercises
- Revising breach-related provisions in vendor agreements (including cloud services agreements)
- Have (and possibly employ) a right to audit
- Conducting an on-site Breach Day including one or more of the above items

Contact Information

Margo H.K. Tank
Partner
202.349.8050
mtank@buckleysandler.com

Rena Mears
Managing Director
202.349.7977
rmears@buckleysandler.com

James T. Shreve
Associate
202.461.2994
jshreve@buckleysandler.com

Buckley Sandler LLP