Buckley Sandler LLP

Legal Counsel to the Financial Services Industry

Cyber and Data Risk – What Keeps You Up at Night?

December 10, 2014

Introduction & Overview

Today's Discussion:

- Evolving nature of data and privacy risks
- Role of the board & senior management
- Privacy and security program development
- Cybersecurity, data protection, and data breach response
- Privacy and security gap assessments and reporting
- Managing change and developing risk aware cultures

Cybersecurity:
The process of protecting information by preventing, detecting and responding to attacks.*

* Framework for Improving Critical Infrastructure Cybersecurity

Data as a Strategic Asset

Asset in Hyper-growth Mode:

- "White noise" to "big data"
- Electronic transaction and paperless processes
- Online commerce → Regulatory
  Product personalization to KYC
  Personal profile & behavior analysis
- Data mining = market success
- Strategic/core to every business

Highly Vulnerable:

- Ubiquitous, portable
- Ephemeral, high velocity
- Rights & obligations – complex
- Immature management processes
- Lagging defense mechanisms
- Diverse "bad actors"/motivation
- Unpredictability of harm
- Competition for resources

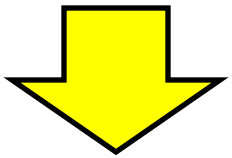
Result:

Produce more data, mine more data, acquire more data = High Value Target

Data Risk: Cybersecurity

Data Risk: Encompasses a variety of risks including:

Accuracy	Completeness	Consistency
Timeliness	Availability	Fitness for Use
Confidentiality		



Financial	Operational	Brand	Regulatory

Cybersecurity Risk:
Risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems.*

* The Institute of Risk Management

Cyber Risk Response Plan

Optimal

Enterprise Program: Mature Process

- Defined – risk-based, strategic
- Documented – life cycle
- Operationalized – roles, processes
- Evaluated – metrics, periodically
- Sustainable – adjust/change

Integrated:

- All levels of the organization
- Enterprise “eco-system”

Reality

“Siloed”: Immature Process

- Defined – tactically, operational
- Documented – incomplete
- Operationally – IT/Security focused
- Evaluated – incident focused
- Maintained – static, limited scope

Separated:

- Function focus and/or mid-level
- Reactively involve “eco-system”

Role of Board & Senior Management

- The role of the board and senior management in identifying, managing, and responding to cyber risk is under increasing scrutiny from shareholders, regulators, and the marketplace
- Deputy Secretary of the Treasury Raskin recently divided the subject into three categories with 10 questions:
  - Baseline protections
  - Information sharing
  - Response & recovery
- The following discussion will focus on baseline protections and response & recovery

Baseline Protection – 1

Is cyber risk part of our current risk management framework?

Deputy Secretary Raskin:

- Cyber risk management framework as part of enterprise risk framework
- Identify cyber threats presented by their specific businesses and operations
- Match threats to appropriate technology solutions
- CEOs and Boards should adopt policies, procedures, and other controls – like training and governance…address cyber threats that

Requires Board and senior management gain a reasonable understanding of:

- Cyber risk management
  - Threat landscape
  - Data risk and cyber risk applicable
  - Current capability and availability of response/control mechanisms generally
- Current cyber-response readiness state of enterprise and ecosystem
- Ability, time, and expense required to implement operational controls

Additional consideration:

- Required clear communication of residual risk
- Maturity of ERM programs varies widely by company and industry

Baseline Protection – 2

Do we follow the NIST Cybersecurity Framework?

Deputy Secretary Raskin:

- Risk-based approach…identify cyber risk posture…determine…risk profile and tolerance
- Not technical…focus is oversight and governance
- Organization communication plans for responding to attacks
- Provides common language and set of practices, standards, and guidelines
- Aligns with enterprise risk management
- Provides tools to evaluate third-party risk

Considerations for Board and senior management:

- Many companies base security in frameworks other than NIST
- NIST Cybersecurity Framework also offers mapping to other security focused frameworks – so takeaway is on adoption of an accepted authoritative framework
- Communication plans are key and should address the enterprise and its ecosystem (regulatory, stakeholders, partners, vendors)
- Adopting common terms, definitions, and language is essential to respond to and effectively manage cyber attack

Baseline Protection – 3

Do we know the cyber risks…third parties expose us to?

Deputy Secretary Raskin:

- Outsourced services for payment systems and/or back office processes mean non-employees may have access to enterprise networks, systems and data
- Imperative that enterprise understand what security safeguards vendors and third parties have in place:
  - Knowing all vendors and 3rd parties with access
  - Ensuring 3rd parties have appropriate protections in place to safeguard enterprise systems and data
  - Conducting on-going monitoring to ensure adherence to protections
  - Documenting protections and related obligations in contracts

Considerations for board and senior management:

- Complexity of third-party risk:
  - Identifying and defining 3rd parties/profiles
  - Imposing requirements/managing exceptions
  - Evaluation and enforcing
  - Sustaining the process
- Pre-, During, and Post- incident
  - Consider cyber risk impact in strategic decisions involving third parties
  - Include third party vendors and providers in cyber incident response planning
  - Communicate to the board third-party cyber risk classifications, profiles, requirements and discuss potential impact on cyber response capabilities

Response & Recovery

Deputy Secretary Raskin:

Increasingly focus efforts on making response and recover more efficient, effective, and predictable.

- Do we have a cyber-security incident playbook?
- What roles do senior leaders and the board play?
- When and how do we engage?

Considerations for board and senior management:

- Does a cyber-incident playbook exist? Has it been operationalized? Are adequately skilled resources identified and available?
- Is there an “owner”? Cyber response requires a leader with appropriate authority to manage the responsibility and meet the objectives.
- Clearly communicate roles and expectations to board and senior management before an incident occurs
- Leverage established communication channels to manage expectations during and post cyber incident
- Law enforcement engagement may enhance enterprise response effectiveness

Cyber Response: Complexities

Preparing the board and senior management for some of the complexities that can occur:

- Third party involvement - modularization of business and IT processes:
  - Cloud strategies
  - Serial outsourcing and complex third party ecosystems
- “Proving the negative”
  - Business risk decision
- Regulatory inquiries
  - Many regulators, all at once, with different concerns/focus
  - Managing consistency of response
- Media glare
  - Pre-breach messaging and spokesman
  - Train spokesmen and spokesmen on media tactics and appropriate responses

Cyber: Practical Steps

- Assess the current cyber risk process, program and playbook against the NIST Cybersecurity framework
- Provide training sessions focused on the role and expectations of the Board and Senior Management pre-, during, and post cyber incident
- Incorporate board participation in cyber-attack-response simulation(s) using real-world complex use cases
- Develop communication (external, internal, regulatory) plan to manage cyber incident/breach response
- Identify third party risk, create control profiles, evaluate current third parties, apply mitigating controls as needed
- Identify and solidify internal and external skill-sets that can respond immediately when cyber-incident occurs

Questions

Margo H. K. Tank
Partner, BuckleySandler LLP
202.349.8050
mtank@buckleysandler.com

Rena Mears
Managing Director – Privacy, Cyber Risk & Data Security Group, BuckleySandler LLP
202.349.7977
rmears@buckleysandler.com

Barbara Lawler
Chief Privacy Officer, Intuit
650.944.5136
Barbara_lawler@intuit.com

Buckley Sandler LLP