Enterprise Risk Management: Prevent The Fires Before They Start The Kohl's Way

Steve Thomas, Chief Risk and Compliance Officer

Enterprise Risk Management – Background

"It is the Board's responsibility to ensure that management has instituted processes to identify major risks and has developed plans to deal with such risks."

Source: National Associate of Corporate Directors

"… a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Source: COSO Enterprise Risk Management – Integrated Framework.

Bottom line: RISK REDUCTION

Risk Reduction: Identification and Prioritization

- Risk Identification Process
  - Executives' insights and knowledge
  - Industry-specific risks
  - Regulatory environment
  - Macro considerations
  - Brand/Reputation considerations
- Prioritization Process – Tier 1 and Tier 2 Risks based on Regulatory and Operational/Financial Risk
  - Regulatory Risks – Those Risks with potential to erode value through lawsuits, negative publicity, financial risk and brand damage
  - Operational/Financial Risk – Those Risks that ultimately represent opportunity to improve profits through reduced costs and/or increase sales

Note: 20 Tier 1 Risks and 10 Tier 2 Risks

Risk Reduction/Mitigation – Process Overview

- Risk Reduction Committee
  - Cross Section of Kohl's key strategic Business Owners with C-Suite Representation
  - Quarterly Meetings
  - Review Tier 1 Risks
  - Active Quarterly Presentations by 3-4 Tier 1 Risk Owners
  - Quarterly Progress Reports by all Tier 1 Risk Owners
- Corporate Governance
  - Enterprise Risk Services department has direct ownership, e.g. Risk Identifier, Information Aggregation, Framework, Committee Facilitator
  - Executive Management, e.g. Risk Ownership and Accountability
  - CEO/C-Suite, e.g. Risk Oversight and Tone Setting
  - Board of Directors, e.g. Risk Governance on Risk Identification/Prioritization/Process

Risk Reduction Process Overview

- Quarterly Information Update Process
  - Risk owner(s) required to submit quarterly progress updates

Risk Rating	Owner(s)	Risk Topic	Planned Actions	Key Metrics	Secondary Metrics
Relative Rating	Executive(s) assigned as owner of risk	Brief summary of risk	Listing of future actions	1-2 key metrics or milestones that allows for progress measurements	1-2 secondary metrics or milestones that allows for progress measurements

Barriers / Obstacles	Recent Progress	**Overall Status**	
		Inherent Risk	Progress Vs. LY
Listing of potential barriers or obstacles that could inhibit progress	Key accomplishments during past 3-6 months	Increasing, Steady, or Declining	Significant, Moderate, or Minimal

Tier 1 Risks

1. Regulatory Risks

   - Wage Inflation/Minimum Wage
   - Pricing Compliance
   - Environmental Compliance

2. Operational/Finance Risk

   - Escalating Healthcare Costs
   - Ecommerce Holiday Readiness

Kohl's Risk Reduction Dashboard - Year End 2014

Non-Regulatory Risks	Y/E '13 Rank	Status: Inherent	Status: Progress
(1)	1		
(2)	2		
(3)	3		
(4)	1		
(5)	4		
(6)	n/a		
(7a)	6		
(7b)	6		
(8)	7		
(9)	8		
(10)	9		
(11)	10		

Status Legend

Inherent	Progress
Increasing	Limited
Steady	Moderate
Declining	Significant

Kohl's Risk Reduction Dashboard - Year End 2014

Regulatory / Reputation risks

	Y/E '13 Rank	Status: Inherent	Status: Progress
(1) _____	1		
(2) _____	2		
(3) _____	3		
(4) _____	4		
(5) _____	5		
(6) _____	6		
(7) _____	7		
(8) _____	8		
(9) _____	9		
(10) _____	10		

Status Legend

Inherent	Progress
Increasing	Limited
Steady	Moderate
Declining	Significant

Risk Profile – Cyber Security/Data Breach Planning

Preventing, Detecting and Responding to Cyber Threats
"Reasonable Security" Legal Standard

Background

- **Target** Breach - $252 Million; Home Depot Breach $43 Million
- **Costco, CVS,** and **Walmart Canada** Data breach related to photo processing operations
  - Outsourced function to third party – Disclosure of customer information
- **Sony** breach – Email Security
- **Anthem** announced a sophisticated cyber attack exposing personal data of 80 million individuals
- **Class Action Law Changes** – Erosion of Positive Precedent holding that consumers lack standing to assert claims based on data breach only if they can show actual damage – Target (Minnesota) and Neiman Marcus (7th circuit)

KOHL'S

Top 5 Causes of Data Breaches

1. Employee Negligence/Threat
2. External Theft of a Device
3. Employee Theft
4. Phishing
5. Malware

Source: Baker Hostetler
September 2015

Prevention

- Increase Firewall Protection
- Select and Install Advance Persistent Threat Detection Products (to detect advanced malware threats)
- Identify and Expand Network Segmentation
- Reduce/Eliminate Stored Data
  - Email/electronic share folder retention policies to reduce/eliminate customer, employee and business confidential data
- Conduct Third Party Assessment for Outsourced Functions
- Increase Company Wide Security Awareness/Training
  - Phishing Exercises/Password Education
- Insider Threat Assessment
  - Employee/Consultant review on who has administrative access to key systems and email

Detection

- Conduct Annual Forensics Review with different cutting edge IT Security providers
- Conduct Annual Penetration Testing
- Develop and Maintain Involvement with Industry Leaders to understand securities threats and counter measures
- Establish and Foster Relationships with local law enforcement, FBI and Homeland Security/Secret Service to secure “insider” cyber intelligence

Response Planning

- Establish Cyber Security Response Team
  - IT, Legal, Public Relations and Key Business Owners
  - Secure Outside Counsel, Forensic Experts that are available 24/7
- Establish Data Breach Plan

  NOTE: SEC Fined Equities firm on September 22, 2015 for failing "to adjust written policies and procedures reasonably designed to protect customer records and information"

  NOTE: 47 States have Breach Notification laws (only AL, NM and SD do not)
- Conduct Data Breach Simulations to test the plan to close gaps and evolve the Data Breach Plan
- Security Response Team Monthly/Quarterly Meetings to review Plan and Prevention Opportunities
- Secure Cyber Insurance

Questions?