Facebook and Equifax: Meeting Increased Customer Expectations, Not Just Regulatory Requirements

STEVEN MINSKY
CEO of LogicManager & Author of the RIMS Risk Maturity Model

Learning Objectives

At the end of this session, participants will be able to:

• Discuss the recent changes to the regulatory environment and other advancements fueled by social media and new technology.

• Explore the Facebook and Equifax scandals with an eye towards what these seemingly diverse cases have in common.

• Outline the tactical steps every company should take to avoid costly litigation and regulatory fines.
Agenda

1:00-2:00: The See-Through Economy

2:00-2:15: Break

2:15-3:30: How to Implement Risk-Based Compliance

3:30-4:00: Questions and Answers

How prepared is your organization to cope with the increasing levels of risk in today's interconnected world?

Very Prepared

Prepared

Somewhat Prepared

Not Prepared
Social media has created a see-through economy, and transformed the way companies must act.

Now, reputation is everything.

Equifax

September 2017 – Cyber breach compromises 143 million American Social Security numbers, driver’s license numbers, addresses, and birth dates.

Mid-September 2017 – Former CEO Richard Smith “retires.”

November 2017 – 50-state class action lawsuit filed against Equifax.

March 2018 – Number of Americans impacted increases to 148 million.

“Both the human deployment of the patch and the scanning deployment did not work.”

– Former CEO Richard Smith
   September 2017
Facebook

December 2015 – Cambridge Analytica uses Facebook users’ data to help a political candidate gain an advantage in the electoral race. Facebook asks Cambridge Analytica to delete the data, which the company confirms.

October 2017 – Trillium Asset Management calls on Facebook to establish a risk oversight committee.

January 2018 – Facebook claims they already have an audit committee that performs risk oversight.

March 2018 – Facebook learns that Cambridge Analytica harvested the private information of over 50 million Facebook users without their consent.

April 2018 – Zuckerberg announces that as many as 87 million people may have been impacted.

"We have a responsibility to protect your data, and if we can’t then we don’t deserve to serve you.”

– CEO Mark Zuckerberg

March 2018

What Do Equifax and Facebook Have in Common?
The Effects of Corporate Scandal

- Chipotle: **46%** decrease in stock value
- Equifax: **33%** decrease in stock value
- Facebook: **21%** decrease in stock value


Innovation Requires Change
Chipotle

2008 – Chipotle introduces its locally grown produce program.

2015 – E. coli outbreaks detected by public health officials.

December 2016 – Chipotle abandons dual-CEO structure.

July 2017 – Multiple customers in Sterling, Virginia complain of symptoms consistent with the norovirus.

November 2017 – Founder Steve Ells steps down as CEO.

August 2018 – More than 700 people become sick after eating Chipotle.

“We are all very confident that this E. coli outbreak would not happen again.”

– Former CEO Steve Ells

January 2016

The Challenge
Compliance Professional

**Goal:** Protect your organization's reputation and ensure compliance.

**Challenge:** Managing regulatory change in the see-through economy.
How Do You Manage Regulatory Change?

1. Identify the change

2. What’s the impact?

The Solution: A Perfect Sidekick

Compliance Professional

Risk-based Approach
<table>
<thead>
<tr>
<th>Which aspect(s) of integrating governance functions do you find most challenging?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing cross-functional information</td>
</tr>
<tr>
<td>Getting process owners &amp; front-line involvement</td>
</tr>
<tr>
<td>Standardizing your assessment scales &amp; criteria</td>
</tr>
<tr>
<td>Getting buy-in from other functional areas</td>
</tr>
</tbody>
</table>
Risk-Based Approach

- Governance
  - Requirement Repository
  - Applicability & Adherence Reviews
  - Risk Assessments
  - Controls
  - Policies
  - Training
  - Testing
  - Metrics
  - Reporting

- Assessment
  - Process Owner Subject Matter Experts (SMEs)
  - Legal and Compliance
  - All Employees

- Mitigation
  - Legal and Compliance
  - Process Owners
  - Audit

- Monitoring
  - Legal and Compliance
  - Process Owners
  - External Regulators
  - All Employees

- Events
  - Regulatory Changes
  - Incidents of Non-Compliance
  - Audits
  - Regulatory Exams

Engagement Process

- Controls
- Procedures
- Policies
- Training
How to Implement Risk-Based Compliance

1. Identify Risks Across the Organization
2. Connect Risks to Root Causes
3. Link Regulations & Requirements to Controls
4. Structure Reporting for Flexibility & Efficiency
5. Develop a Process for Managing Change Over Time

Traditional, Silo’d Language

Compliance
- Requirement Repository
- Applicability & Adherence Review
- Policies & Controls
- Reporting
- Incidents of Non-Compliance

Information Security
- Application & Asset Inventories
- Vulnerability Analysis
- Controls
- Testing & Scans
- Security Breaches

Vendor Management
- Vendor Inventory
- Vendor Due Diligence
- Contract Management
- Service Level Performance
- Vendor Breaches
Risk-Based Translator

Activity Part 1: Identify Risks
Identifying Root-Cause

- **External**
  - Risk cause by outside people, environment, and other circumstances.
  - Examples: Fluctuations in economic markets, weather-related hazards or disasters, lack of public infrastructure

- **People**
  - Risks involving people who work for the organization.
  - Examples: Misuse of confidential information, willful noncompliance with policies, lack of necessary skillsets

- **Process**
  - Risks arising from the organization’s execution of business operations.
  - Examples: Inadequate budgeting, missing documentation, lack of policies or procedures

- **Relationships**
  - Risk caused by the organization’s connection with third-parties.
  - Examples: Contracts are not reviewed properly, inadequate security protocols on third-party relationships

- **Systems**
  - Risk associated with IT processes, security, data, or information assets
  - Examples: Data is inaccessible, failure to adopt new technology trends, inadequate system maintenance

---

Adopt a Root-Cause Approach
Standardize Assessment Scale & Criteria

Adopt a uniform numerical scale to objectively prioritize risks.

<table>
<thead>
<tr>
<th>1 - 2 Insignificant</th>
<th>3 - 4 Minor</th>
<th>5 - 6 Moderate</th>
<th>7 - 8 Serious</th>
<th>9 - 10 Major</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>Financial</td>
<td>Financial</td>
<td>Financial</td>
<td>Financial</td>
</tr>
<tr>
<td>Legal</td>
<td>Legal</td>
<td>Legal</td>
<td>Legal</td>
<td>Legal</td>
</tr>
<tr>
<td>Operational</td>
<td>Operational</td>
<td>Operational</td>
<td>Operational</td>
<td>Operational</td>
</tr>
<tr>
<td>Regulatory</td>
<td>Regulatory</td>
<td>Regulatory</td>
<td>Regulatory</td>
<td>Regulatory</td>
</tr>
<tr>
<td>Strategic</td>
<td>Strategic</td>
<td>Strategic</td>
<td>Strategic</td>
<td>Strategic</td>
</tr>
</tbody>
</table>

Activity Part 2: Identify Root-Causes
Link Controls to Regulations & Requirements

- Regulation A
- Associated Business Processes
- Process
- Controls
- Relationships
- Systems
- IS Training Program, e.g.

The Balanced Scorecard

- Financial
  - "To succeed financially, how should we appear to our shareholders?"

- Customer
  - "To achieve our vision, how should we appear to our customers?"

- Vision and Strategy
  - "To satisfy our customers and shareholders, what business processes must we excel at?"

- Learning and Growth
  - "To achieve our vision, how will we sustain our ability to change and improve?"

Structure Reporting for Flexibility & Efficiency

Activity Part 3: Mitigate and Monitor
Risk-Based Compliance

- Governance
  - Requirement Repository
- Assessment
  - Applicability & Adherence Reviews
  - Risk Assessments
- Mitigation
  - Controls
  - Procedures
  - Policies
  - Training
- Monitoring
  - Testing
  - Metrics
  - Reporting
- Events
  - Regulatory Changes
  - Incidents of Non-Compliance
  - Audits
  - Regulatory Exams

Engagement
- Legal and Compliance
- Process Owner Subject Matter Experts (SMEs)
- Legal and Compliance
- All Employees
- Legal and Compliance
- Process Owners
- Audit
- Legal and Compliance
- Process Owners
- External Regulators
- All Employees

Manage Change over Time

Organizational policy must change to match new line item(s)

Line items change

Regulation amended

©LogicManager

©LogicManager
## Which aspect of your risk management program do you consider to be most underserved?

- Cybersecurity
- Vendor Management/supply chain disruptions
- Regulatory management & compliance
- Incident Management
- Other

Questions & Answers

Steven Minsky is a recognized thought leader and writer in integrated risk management.

Steven is the CEO of LogicManager, Inc. and author of the popular RIMS Risk Maturity Model framework and assessment tool.

To follow Steven on his blog, visit: [www.logicmanager.com/blog/](http://www.logicmanager.com/blog/)