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?

<table>
<thead>
<tr>
<th>Very Prepared</th>
<th>Prepared</th>
<th>Somewhat Prepared</th>
<th>Not Prepared</th>
</tr>
</thead>
</table>

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 politician 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?

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


The Effects of Corporate Scandal

The New York Times
For Many Facebook Users, a ‘Last Straw’ That Led Them to Quit

The Wall Street Journal
Consumers Blast Equifax’s Hack Response
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

Innovation Requires Change

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
How to Implement Risk-Based Compliance

Risk-Based Approach
Risk-Based Compliance

- Governance
  - Requirements Repository
  - Applicability & Adherence Reviews
  - Risk Assessments

- Assessment
  - Controls
  - Procedures
  - Policies
  - Training
  - Testing
  - Audits
  - Reporting

- Mitigation
  - Legal and Compliance
  - Process Owner Subject Matter Experts (SMEs)
  - Legal and Compliance

- Monitoring
  - Requirement Repository
  - Applicability & Adherence Reviews
  - Risk Assessments

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

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 Reviews
- Policies & Controls
- Reporting
- Incident & Event Management

Information Security
- Application & Asset Inventories
- Vulnerability Analysis
- Controls
- Incident Response
- Security Braches

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

Compliance
- Requirement Repository = Governance
- Applicability & Reference Review = Assess
- Policies & Controls = Mitigate
- Reporting = Monitor
- Incidents of Non-Compliance = Events

Information Security
- Application & Asset Inventories = Governance
- Vulnerability Analysis = Assess
- Testing & Scans = Mitigate
- Security Breaches = Monitor

Vendor Management
- Vendor Inventory = Governance
- Vendor Due Diligence = Assess
- Contract Management = Mitigate
- Service Level Performance = Monitor
- Vendor Breaches = Events

Activity Part 1: Identify Risks

Identifying Root-Cause

Root Cause 1

Risk 1

Mitigation Activity 1

Risk 2

Mitigation Activity 1

Root Cause 2

Mitigation Activity 2

Root Cause 3
Adopt a Root-Cause Approach

**External**
Risk caused 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, unlawful noncompliance with policies, lack of necessary skills

**Process**
Risks arising from the organization's execution of business operations.
Examples: Inadequate budgeting, missing dependencies, 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 uniform numerical scale to objectively prioritize risks.

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

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

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

The Balanced Scorecard

Financial

Customer
Vision and Strategy

Internal Business Processes

Learning and Growth

Structure Reporting for Flexibility & Efficiency
Activity Part 3: Mitigate and Monitor

Risk-Based Compliance

- Governance
  - Requirement/Reposability
  - Applicability & Adherence Reviews
  - Risk Assessments

- Assessment
  - Testing
  - Metrics
  - Reporting
  - Regulatory Changes
  - Incidents of Non-Compliance
  - Audits
  - Regulatory Exams

- Mitigate
  - Applicability & Adherence Reviews
  - Risk Assessments
  - Requirement/Reposability

- Monitoring
  - Testing
  - Metrics
  - Reporting
  - Regulatory Changes
  - Incidents of Non-Compliance
  - Audits
  - Regulatory Exams

- Events
  - Applicability & Adherence Reviews
  - Risk Assessments
  - Requirement/Reposability

Manage Change over Time

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