Risk Management at the Speed of Digital Business

Jie Zhang
Gartner Inc.
Digital Business Creates New Risks, Not Just Bigger Risks
Everything will be connected, and every connection is a potential attack vector

465k patients told to visit doctor to patch critical pacemaker vulnerability

"We cannot solve a problem by using the same kind of thinking we used when we created them."

— Albert Einstein
Danger Lies Ahead

60%
Not prepared to manage cyberthreats with potential to significantly disrupt core operations

63%
Rapid speed of innovation and/or new technologies may outpace our ability to manage risk

Source: "Executive Perspectives on Top Risks for 2017," NC State University
By 2020, 60% of digital businesses will fail due to their inability to manage digital risks effectively.
Key Issues

1. What's wrong with the way risks are presented to the business?
2. Why is a change in thinking crucial to managing digital risk?
3. What steps are necessary to launch a digital risk management program?
Key Issues

1. What's wrong with the way risks are presented to the business?
2. Why is a change in thinking crucial to managing digital risk?
3. What steps are necessary to launch a digital risk management program?
Inherent Personality Conflict

Chief Executive Officer
"… the future is so bright!"

Versus

Chief Risk Officer
"… one more problem!"
How the CEO Views Risk in 2017: Macrotrends

- Macroeconomic growth/stability: 18%
- Regulations: 13%
- Political and social environment: 13%
- Consumer behavior and demand: 12%
- Changing business structure in specific industry: 11%
- Advances in technology – innovation disruption: 11%
- Industry competition: 10%
- Currency exchange rate: 8%
- General costs: 7%
- Trade conditions: 6%
- Digital change: 6%
- Environmental sustainability: 6%
- IT change (other than digital): 5%
- Emerging markets evolution: 5%
- Demographic changes: 5%
- Oil and other energy prices and sources: 5%
- Access to capital/investor confidence: 5%
- Workforce/Talent/Skills: 4%
- Interest rates and inflation/deflation: 4%
- Government spending and investment: 4%
- Geopolitical situation: 3%
- Globalization: 3%
- Taxation: 2%
- Organizational factor/not macroenvironmental: 2%
- Cybersecurity: 2%
- Healthcare: 1%
- Terrorism: 1%
- Other: 3%

“What are the two most important external macrotrends shaping your business strategy?” (Open-style responses)

n = 388 CEOs and senior business executives

Source: Gartner (April 2017)
Risk and Trust Culture Are Broken

- Non-IT executives have written off security and its associated risks as a technical problem, handled by technical people, buried in IT.
- Checkbox thinking is still the predominate mindset.
- There is no such thing as perfect protection and the organization cannot buy its way out of this problem.
- Executives do not understand the risks they sign-off and security people do not effectively link risk to business outcomes.
What separates successful CEOs from unsuccessful CEOs is the ability to take the right risks. Therefore, you must reframe the conversation from "high risks versus low risks" to "good risks versus bad risks."
Key Issues

1. What's wrong with the way risks are presented to the business?

2. Why is a change in thinking crucial to managing digital risk?

3. What steps are necessary to launch a digital risk management program?
Bimodal is the practice of managing two separate but coherent styles of work, one focused on predictability and the other on exploration.

**Mode 1** is predictable, improving and renovating in more well-understood areas. **Mode 2** is exploratory, experimenting to solve new problems.
Mode 1 Samurais and Mode 2 Ninjas

Samurai (Traditional)

- Prepared to manage the known
- Expected outcomes, stable context
- Decisions costly to reverse
- Established, proven standards
- Higher ceremony

Ninja (Experimental)

- Ready to respond to the unknown
- Projected outcomes, dynamic context
- Decisions inexpensive to reverse
- Emergent, experimental practices
- Lower ceremony
Digital Business Demands a Strategic Digital Risk Management Approach

Risk management practitioners must:

- Create an ecosystem perspective of risk
- Balance benefit and risk-based analysis
- Work with senior executives and security professionals to develop a risk strategy

Source: Gartner, "How to Get Your CEO to Embrace Digital Risk Management" (G00303007)
### Experimental Thinking Is Learning-Oriented

<table>
<thead>
<tr>
<th>Traditional Thinking</th>
<th>Experimental Thinking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flawless planning</td>
<td>Enlightened trial and error</td>
</tr>
<tr>
<td>Avoid failure</td>
<td>Fail fast</td>
</tr>
<tr>
<td>Rigorous analysis</td>
<td>Rigorous testing</td>
</tr>
<tr>
<td>Presentations</td>
<td>Lightweight experiments</td>
</tr>
<tr>
<td>Arm's-length customer research</td>
<td>Deep customer immersion</td>
</tr>
<tr>
<td>Periodic Thinking</td>
<td>Continuous Doing</td>
</tr>
<tr>
<td>Thinking</td>
<td></td>
</tr>
</tbody>
</table>
Digital Business Ecosystems Require a New Way of Thinking About Risk

Domain-Specific Risk Management

- Framework
- Metrics
- Systems
Leads to the ability to manage complex sets of risk
Through simplification, automation and *integration* of risk management processes and data
Digital Business Requires Integrated Risk Management
What Is Integrated Risk Management?

- **Framework —**
  - **Strategy:** Enablement and implementation of a framework, including performance improvement through effective governance and risk ownership;
  - **Assessment:** Identification, evaluation and prioritization of risks;
  - **Response:** Identification and implementation of mechanisms to mitigate risk

- **Metrics —**
  - **Communication and reporting:** Provisioning of the best or most appropriate means to track and inform stakeholders of an enterprise’s risk response

- **Systems —**
  - **Monitoring:** Identification and implementation of processes that methodically track governance objectives, risk ownership/accountability, compliance with policies and decisions that are set through the governance process, risks to those objectives, and the effectiveness of risk mitigation and controls;
  - **Technology:** Design and implementation of an IRM solution architecture
Key Issues

1. What's wrong with the way risks are presented to the business?
2. Why is a change in thinking crucial to managing digital risk?
3. What steps are necessary to launch a digital risk management program?
ITScore for Risk Management

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>Developing</td>
<td>Defined</td>
<td>Managed</td>
<td>Optimizing</td>
</tr>
</tbody>
</table>

- **Level 1 (Initial)**
  - No visibility into critical risks; very compliance-focused and reactive
  - Little executive support to assess risk
  - No risk policy

- **Level 2 (Developing)**
  - Responsibility for risk management has been assigned
  - Ad hoc risk assessments executed in silos
  - Risk register created

- **Level 3 (Defined)**
  - Formal strategic planning for risk management
  - Risk assessments proactively executed
  - Control gaps closed
  - Governance committees formed

- **Level 4 (Managed)**
  - Executive-level reporting
  - KRIs are mapped into KPIs
  - Formal residual risk sign-off
  - Integrated risk management guides program development

- **Level 5 (Optimizing)**
  - Continuous assessment
  - Enterprise-wide risk-aware culture
  - Risk fully integrated with strategic decision making
  - Governance driven by executive management
  - Board-level visibility and oversight fully demonstrated
Gartner Client Maturity by Industry

- Financial Services: 6.0% Level 5, 15.1% Level 4, 40.8% Level 3, 27.2% Level 2, 26.0% Level 1
- Communication/Media: 13.1% Level 5, 21.3% Level 4, 50.6% Level 3, 19.2% Level 2, 9.6% Level 1
- Government: 9.6% Level 5, 22.6% Level 4, 48.6% Level 3, 19.2% Level 2, 15.0% Level 1
- Manufacturing & Natural Resources: 16.3% Level 5, 24.4% Level 4, 50.6% Level 3, 16.3% Level 2, 7.5% Level 1
- Other: 16.1% Level 5, 22.9% Level 4, 53.5% Level 3, 22.9% Level 2, 7.5% Level 1

n = 1315 end users
Gartner Client Maturity by Company Size

- **$3B+**: 16.7% (Level 5), 30.5% (Level 4), 45.8% (Level 3), 7.0% (Level 2), 9.8% (Level 1)
- **$500M to <$3B**: 11.2% (Level 5), 28.5% (Level 4), 46.4% (Level 3), 13.9% (Level 2), 23.1% (Level 1)
- **< $500M**: 9.8% (Level 5), 23.1% (Level 4), 44.0% (Level 3), 11.2% (Level 2), 23.1% (Level 1)

n = 1042 end users

© 2017 Gartner, Inc. and/or its affiliates. All rights reserved.
10 Critical Success Factors for IRM Programs

Framework
- Appetite
- Assessment
- Aggregation

Systems
- Analytics
- Applications
- Architecture
- Assurance

Metrics
- Accountability
- Action
- Achievement
The CISO Is the Key to IRM Success

61% of companies have their board of directors meet directly with the CISO on a regular basis

20% of companies have dedicated board-level committees dedicated to "cyber/IoT" risk

Source: "What Directors Think 2017," NYSE Governance Services, 1Q17

Are you prepared to help your company succeed?
What Is Appropriate Risk?

There is no such thing as "perfect protection"

Less complex business, less of a target
Growing business, more customers and complexity
Larger, more complex business, more of a target

Business Model

Bad Risk
Lower Cost
Lower Maturity

As our business grows, we have to continually reassess how much risk is appropriate.

Good Risk
Higher Cost
Higher Maturity

Our goal is to build a sustainable program that balances the need to protect against the needs to run our business.
Risk landscape becomes more complex and interconnected

Hype Cycle for Risk Management, 2017

- **Innovation Trigger**
- **Peak of Inflated Expectations**
- **Trough of Disillusionment**
- **Slope of Enlightenment**
- **Plateau of Productivity**

- **Years to mainstream adoption:**
  - less than 2 years
  - 2 to 5 years
  - 5 to 10 years
  - more than 10 years
  - obsolete before plateau
Build a Collaborative Cross-Functional Team
The Future of Integrated Risk Management

Responding to: All Enterprise Risks
Standards: COSO, ISO 31000
Client: CRO

Responding to: Cybersecurity/IT Risk
Standards: NIST CSF, ISO 2700x
Client: CISO, CIO

Operational Risk Management
Integrated Risk Management

Risk Strategy
Performance Risk
Regulatory Risk

Digital Risk Management

Third Party
Social Media
Mobile
Big Data
IoT
Cloud
Recommendations

✓ Identify the areas in your business model where there is a need to innovate and where these methods can be applied
✓ Engage your stakeholders and get buy-in to build a collaborative team and use a design-thinking-based approach
✓ Design the process and governance, but don't overdo it
✓ Start small and grow — innovate, and learn how to innovate as you go
✓ Experiment with these approaches, to get it right for your organization