THE DIGITIZATION OF THE RISK PROFILE:
Implications for Risk Leaders

YVETTE CONNOR
ALEXIE SIDORENKO
CHRIS MANDEL
Speakers

• Yvette Connor - Principal, National Practice Leader – Strategic Risk Advisory, Grant Thornton

• Alexie Sidorenko, Chief Risk Officer, Institute for Strategic Risk Analysis

• Chris Mandel, RIMS-CRMP - SVP, Strategic Solutions, Sedgwick & Director, Sedgwick Institute
THE EVOLUTION OF RISK MANAGEMENT CAPABILITY

Traditional Risk Management
- **Focus**: Insuring the bad things
- **Scope**: Risk Transfer/Insurance/Loss Prevention/Mitigation of Insurable Risks

Advanced Risk Management
- **Focus**: Short term success
- **Scope**: Mitigation of Controllable Risks/Manage Risk as an Expense
- **Advanced solutions**

Digital Risk Management
- **Focus**: Long term success
- **Scope**: Mission focused; Embedded Risk Mgmt Practices; Risk as Differentiator

Fundamentals Covered
- Enhanced & Broadened Capabilities
- Operational Success
- Emerging and Evolving Exposures
- Mission Accomplishment

Specific Business Needs;

Value

Time
What is a Risk Profile?

**IRMI Definition:** A measure of expected losses for a finite time period based on various items of historical data such as total losses, number of losses, average loss size, and payout patterns. The term is usually reserved to refer to a book of business, an individual account, or an individual policy with a sufficiently large exposure base to lend credibility to analysis of the data.

**Investopedia:** A risk profile is an evaluation of an individual’s willingness and ability to take risks. It can also refer to the threats to which an organization is exposed. A risk profile is important for determining a proper investment asset allocation for a portfolio.

**A Progressive View:** A depiction or summary of an organization’s threats and opportunities correlated to its short and long term objectives which identifies any gaps between its goals and the risks that can enable or prevent their accomplishment.

**A Digital Risk Profile:** A depiction or summary of an organization’s threats and opportunities from technology, the internet, the cloud and other aspects of digitally driven processes, that are correlated to its short and long term objectives and which identifies any gaps between its goals and the risks that can enable or prevent their accomplishment.
Important Aspects of Digital Risk

- Higher Speed of Impact
- Strategic Impact
- Operational Impact
- Governance Impact
- Digital “as” a Business
- Digital “in” the Business

Digital Risk
Issues in Digital Risk Management

- Focused on risk associated with digital business processes
- A business issue; not just a technology issue
- Must be owned by the C-suite/management; not just IT
- Heavy reliance on the valuation of the business impact
- Enables leaders to understand their digital risk profile of operations from a business perspective
- Should equip decision makers with knowledge and a balanced decision making framework (protect/operate)
More Digital Risk Issues

• Building digital resiliency where org systems & operations are designed to detect digital threats & respond to minimize disruption and financial losses

• Risk leaders will require a mix of business acumen with sufficient technical knowledge to assess and guide the organization in addressing digital exposures

• An emerging significant digital risk is created by business model disruption by competitors
  – Sufficiency of core business strategy?
  – Understanding the impact of non-traditional competitors

• Research shows shareholders place a higher multiple on firms that are more digitally enabled
More Digital Risk Issues

• Building digital resiliency where org systems & operations are designed to detect digital threats & respond to minimize disruption and financial losses
• Risk leaders will require a mix of business acumen with sufficient technical knowledge to assess and guide the organization in addressing digital exposures
• An emerging significant digital risk is created by business model disruption by competitors
• Sufficiency of core business strategy?
• Understanding the impact of non-traditional competitors
• Research shows shareholders place a higher multiple on firms that are more digitally enabled
Digitization Trends

➢ Increasing speed of data availability even in real time;
➢ Increasing breadth and depth of exposure data quality that when aligned with loss data enable a more complete view into risk profile;
➢ Declining cost of more robust tech tools that will make more risk leaders of all types able to be more effective and to contribute at higher more strategic levels, more effectively;
➢ Reduced regulatory burden flowing from the above as regulators get more comfortable with the way particularly large risk bearing entities manage risk;
➢ Increasing data privacy challenges as more potentially sensitive PI info is available to more stakeholders and as a result is more exposed to access by bad actors;
Digitization Trends (cont’d)

➢ Insurtech will evolve into “risktech” where risk solutions unrelated to insurance become an increasing focus of practitioners and hopefully the innovators;
➢ Eventual complete digitization of the risk profile forcing risk practitioners to broaden their skillset to areas outside their comfort zones (e.g. technology, IoT, AI etc);
➢ More investment in data collection and analysis tools tied to the above;
➢ Increasing transparency among risk stakeholders;
➢ Ultimately, declining cost of risk in more traditional exposure areas e.g. WC and increasing cost of risk in emerging exposure areas - unclear how that will net out;
➢ Increasing formation of alliances and coalitions among stakeholders with common interests wanting to leverage each other’s resources and knowledge for mutual benefit
Where Do Digital Risks Live?

Strategic
- Acquisitions
- Business Model
- Competition
- Demographic
- Brand
- Disruptive innovation
- Market.

Operations
- Customer service
- Infrastructure
- Processes
- System capabilities
- Talent
- Technology

Financial
- Capital
- Cash flow
- Credit
- Debt obligations
- Foreign exchange
- Liquidity
- Etc.

External
- Economy
- Environment
- Geopolitical
- Regulatory
- Tax policies
- Weather events
- Etc.
Top Risks of 2018

1. **The rapid speed of disruptive innovations and new technologies within the industry may outpace the organization’s ability to compete or manage risk appropriately.**

2. **Resistance to change could restrict** the organization from making necessary **adjustments to the business model and core operations.**

3. **The organization may not be sufficiently prepared to manage cyber threats** that could significantly disrupt core operations and damage its brand.

4. **Regulatory changes and scrutiny may heighten,** noticeably affecting the manner in which organizations’ products or services will be produced or delivered.

5. **The organization’s culture may not sufficiently encourage timely identification and escalation of significant risk issues** that could affect core operations and achievement of strategic objectives.
Top Risks of 2018

6. Succession challenges and the ability to attract and retain top talent may limit the ability to achieve operational targets.

7. Privacy, identity management, and information security risks may not be addressed with sufficient resources.

8. Economic conditions in markets the organization currently serves may significantly restrict growth opportunities.

9. Inability to utilize data analytics to achieve market intelligence and increase productivity and efficiency may significantly affect core operations and strategic plans.

10. Companies that were not “born digital” face significant operational challenges.

Source: NC State Univ and Protiviti Survey
A DIGITAL RISK WORLD is a VUCA WORLD

Volatile: nature, dynamics and speed of change

Uncertainty: Lack of predictability, subject to surprises

Complexity: Multiplex of forces, confounding issues, chaos and confusion

Ambiguity: Haziness of reality, mixed meanings, potential for misreads
YVETTE CONNOR, PRINCIPAL, STRATEGIC RISK ADVISORY, GRANT THORNTON
Board Governance + Cyber = ERM Opportunity

The opportunity:
- Boards are in the public spotlight
- Boards have a heightened level of “cyber” awareness
- Technology terminology is obscure
- “Good” results have not been clearly defined
Not All Risks Are Created Equal

A Board challenge is to figure out what to focus on, and when...

Risk Management is the allocation of finite resources to infinite risks

- Reputation Management
- Risk Financing, Insurance, Projects, And Initiatives
- Operational, Errors/Losses, Compliance, Administration
- Company Killers, Client Impact, Reputation
- Safety Net for P&L, Balance Sheet
- Cost

Typical Risk Focus

Organizational Impact
Risk Management Trends

- Fragile Global Supply Chain
- Talent Gap
- Data Security – Cyber Threats
- Big Data – Privacy
- Geo-political Instability
- Compliance Complexities

- New(er) Risk Shifts:
  - Frequency of Change
  - Materiality – order of magnitude
  - Velocity – speed to impact
  - Correlation - global interdependence

- Regulation & Litigation
- Climate Change Impacts?
- Reputational Damage

Source: Corporate Executive Board & World Economic Forum – 2018
Feeling The Digital Heat

What processes do we have in place?

Are mitigation efforts working?

What else may we need to become more resilient?

What about Privacy?
INSTEAD OF RISKING ANYTHING NEW, LET'S PLAY IT SAFE BY CONTINUING OUR SLOW DECLINE INTO OBSOLESCENCE.

WELL NEED A RISK ANALYSIS ON THIS PROJECT BEFORE I CAN APPROVE IT.

RISK 1: INDECISIVENESS
RISK 2: OVERANALYSIS
RISK 3: CLUELESSNESS
RISK 4: MICROMANAGEMENT...

I DON'T UNDERSTAND THESE RISKS.
THAT'S NUMBER THIRTY-SIX.
Ability to Identify Emerging Risks and Disruptive Trends

Findings:

A Critical need for strengthening risk management and regulatory systems:

• All groups of technologies will put increasing pressure on current risk management and regulatory systems in new ways.

• The global nature of these technologies suggests it will be challenging to respond quickly and in collaboration with other countries.

Digital Ecosystem – Internal & External

www.digitalattackmap.com
Collaborative Dialogue
Mandatory “Silo Busting”

Enterprise Risk Management has an opportunity to strategically engage
Simplifying The Digital Discussion

Have you defined cyber risk terms and applied a cyber risk framework?

Does your insurance align with your risk profile?

What are your top FIVE possible loss scenarios, why?

Have you reviewed compliance results against new regulatory requirements?

Skillset and leadership in ERM?
Learn To Bridge The GAPS

Interactions between Risk Management, IT, and Compliance
(CRO, CIO, CISO, Risk Manager, Compliance)
Baseline Cyber Risk Education

Why Everyone (finally) Is Going To Be A Risk Manager

- Updating governance roles
- Building a culture of digital safety
- Applying cybersecurity framework
- Implementing digital terminology
- Solving for performance approach
  - Measurement & scoring
  - Modeling
  - Metrics
- Prioritizing risk investments
- Tracking mitigation and resiliency efforts

An Emerging Risk Framework

1. Scan current cyber risk environment and consider the future possibilities for how cyber risk will evolve
2. Develop scenarios based on cyber risk narratives and characteristic models
3. Generate risk management options and formulate strategy and recommendations
4. Implement Management/Board approved strategy(s)
5. Review risk development and decisions

Facilitate – Validate - Communicate

**Option 1**
Act on the factors contributing to the risk

**Option 2**
Develop precautionary measures

**Option 3**
Reduce vulnerability

**Option 4**
Modify risk appetite to align with new risk

**Option 5**
Use existing risk management measures

**Option 6**
Do nothing
A Cybersecurity (Risk) Framework

- **Framework Attributes:**
  - Industry accepted and tested
  - Regulator approved/supported
  - Robust and flexible
  - Supports updates and changes

- **Framework Governance:**
  - Singular framework usage; avoidance of multiple and/or partial frameworks
  - Universally deployed
  - Consistently used/referenced
    - Internal self-assessments
    - Internal audit
    - External assessments/audits

*National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), Version 1.1*
Frameworks, Definitions, Questions

**National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), Version 1.1**

| ID.RA-1: Asset vulnerabilities are identified and documented | “The risk that occurs from Asset vulnerabilities not identified and documented”... | 1. Has a risk management plan been developed?  
2. Are periodic, unannounced, in-depth monitoring, penetration testing, and red team exercises included as part of the security control assessments?  
3. Are potential security threats, vulnerabilities, and consequences identified, classified, prioritized, and analyzed using accepted methodologies?  
4. Are system flaws identified, reported and corrected?  
5. Does the organization update the information system vulnerabilities list when new vulnerabilities are identified and reported? |
|---|---|---|---|
Example: Taxonomy Visualization
Functional Risk Reporting

Material Risk Profile: Frequency - Severity - Volatility

Material Risk: Expected Impact to Weighted Avg

Inherent | Mitigation Effect | Residual
---|---|---
$977.6 | $850.6 | $177.0

Legend:
- Inherent Risk
- Residual Risk
- Volatility of Estimate
- Certain
- Neutral
- Uncertain

1 - Identify 2 - Proact3 - Detect4 - Respond5 - Recovery
Board-level Risk Reporting

### Risk Distribution By Business Process

- Vendor Management
- Accounts payable
- Revenue
- General Ledger
- P Cards
- Payroll
- Fixed Assets
- Treasury

### Risk Distribution By Country

Inherent Risk Score: 30%

### Risk Distribution By Office

<table>
<thead>
<tr>
<th>Office</th>
<th>Risk Range</th>
<th>Inherent Risk Score</th>
<th>Management Controls Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office 1</td>
<td>Critical</td>
<td>252.5</td>
<td>3.6</td>
</tr>
<tr>
<td>Office 2</td>
<td>Critical</td>
<td>131.2</td>
<td>3.6</td>
</tr>
<tr>
<td>Office 3</td>
<td>Critical</td>
<td>123.0</td>
<td>6.6</td>
</tr>
<tr>
<td>Office 4</td>
<td>Critical</td>
<td>111.6</td>
<td>6.4</td>
</tr>
<tr>
<td>Office 5</td>
<td>Critical</td>
<td>116.2</td>
<td>4.3</td>
</tr>
<tr>
<td>Office 6</td>
<td>Critical</td>
<td>135.6</td>
<td>4.2</td>
</tr>
<tr>
<td>Office 7</td>
<td>Critical</td>
<td>113.1</td>
<td>4.3</td>
</tr>
</tbody>
</table>

### Risk Drivers

- Operational
- Strategic
- Compliance
- Reporting
- Reputational

Risk Drivers:
- Minimal
- Low
- Moderate
- High
- Critical

### Management Control Score

60%
Summary

• Digital Risk Governance is a matter of future survival in an increasingly complex and interconnected world

• Implementation will vary company by company depending on culture, leadership support, internal and external risk profile and risk tolerance

• Getting started and making headway is more important than getting it perfect but tone from the top is critical

• Digitalization and technology won’t make all problems go away as the world is full of surprises…but a strong enterprise wide cyber risk framework will help you prepare and respond more effectively, and it will help every company take more intelligent risks.
ALEX SIDORENKO, CRO INSTITUTE OF STRATEGIC RISK ANALYSIS
Digital is the new normal. Are we about to make the same old mistakes?

Alex Sidorenko
14 years in corporate risk management taught me about 2 different risk managements

**Risk management for corporate governance (RM1)**
- ERM
- Risk appetite
- Risk management frameworks
- Risk reports
- KRIs

**Risk management for decision makers (RM2)**
- DQ
- Budget@Risk
- NPV@Risk
- KPI@Risk
- CF@Risk
Remember how we used to do interviews and workshops to capture information about risks?

Then we discovered...

- Neuroscience
- Behavioral economics
- Cognitive biases
- Poor remuneration
- Hidden agendas
- Corruption and fraud

Remember how we used heatmaps to assess and later communicate risks?

Then we discovered…

- Basic laws of probability
- Flaws in heatmap design:
  - Range compression
  - Centering bias
  - Ranking reversal
- Missing links to objectives
- Missing correlations
- Missing aggregate effects

Remember how we used to report risks separately from objectives and performance?

Then we discovered...
Remember how we created artificial and unnecessary risk management procedures that no one used instead of changing how business actually operates and makes decisions?

Then we discovered…

- ISO31000:2018 and how it talks about finding significant decisions, changing the way decisions are made by adding risk analysis and making risk management integral to decision making
- Changing how budgets are set based on risk analysis
- Changing how schedules and plans are approved based on risk analysis
Are we making the same mistakes with cyber?
THANK YOU
Speaker Contact Info.

- Yvette Connor - Principal, National Practice Leader – Strategic Risk Advisory, Grant Thornton
  – Yvette.Connor@us.gt.com

- Alexie Sidorenko, Chief Risk Officer, Institute for Strategic Risk Analysis
  – alex.ausrisk@gmail.com

- Chris Mandel, RIMS-CRMP - SVP, Strategic Solutions, Sedgwick & Director, Sedgwick Institute
  – Chris.mandel@Sedgwick.com
Speaker Bio: Chris Mandel

Christopher E. Mandel is SVP, Strategic Solutions for Sedgwick and Director of the Sedgwick Institute, the world’s largest and leading claims and productivity management firm. He has held leadership positions in ERM, risk management, insurance, consulting and brokerage for large global corporates for over 30 years including with such firms as USAA Group, PepsiCo, Verizon, American National Red Cross, Liberty Mutual and Marsh. He designed, launched and managed USAA’s first ERM strategy and framework rated by S&P as “Excellent” and “Leading” from 2006-2010. He has been a long-term senior leader in RIMS including being elected President in 2002-03 and was named Risk Manager of the Year in 2004. In 2016 he was given the Goodell Award, RIMS’ highest honor for lifetime achievement and was appointed to Risk Who’s Who in 2007.

He holds and has held numerous board positions in the industry and also teaches for RIMS and the International Center for Captive Insurance Education (ICCIE), Florida State and George Mason Universities.

Mr. Mandel received his B.S. in Business Management from Virginia Polytechnic Institute and State University and an MBA in finance from George Mason University. He is certified in ISO31000 and holds the RIMS-CRMP, RIMS Fellow, CCSA, CPCU, ARM-E and AIC designations. and is a frequent industry speaker, teacher and writer. He writes the “Claim Management” column for IRMI, is a contributor to Risk and Insurance’s "Risk Insider" column and has had continuously running columns in the industry trade press since 1996.
Speaker Bio: Yvette Connor

Principal – Owner
Strategic Risk Practice Lead
Grant Thornton LLP

Focal Point Data Risk
Chief Risk Officer
Focal Point Data Risk

Alvarez & Marsal, LLC
Managing Director - Enterprise Risk Management Advisory
Alvarez & Marsal, LLC

Adjunct Faculty: University Colorado - Denver, School of Business, Cyber Risk Management.
Speaker Bio: Alex Sidorenko

Alex Sidorenko is an expert with over 14 years of strategic, innovation, risk and performance management experience across Australia, Russia, Poland and Kazakhstan. In 2014 Alex was named the Risk Manager of the Year by the Russian Risk Management Association. As a Board member of Institute for Strategic Risk Analysis in Decision Making Alex is responsible for risk management training and certification (including creating exams) across Russia and CIS, running numerous risk management classroom and e-learning training programs. Alex represented Russian risk management community at the ISO Technical Committee 262 responsible for the update of ISO31000:20XX and Guide 73 since 2015.

Alex is the co-author of the global PwC risk management methodology, the author of the risk management guidelines for SME (Russian standardization organization), risk management textbook (Russian Ministry of Finance), risk management guide (Australian Stock Exchange) and the award-winning training course on risk management (best risk education program 2013, 2014 and 2015). In 2012 Alex created Risk-academy www.risk-academy.ru a web portal dedicated to free risk management training for SME across Russia and CIS. Alex worked as a Head of Risk Management at RUSNANO, one of the largest private equity funds in Russia, specializing in technology investment. Alex won an award for best ERM implementation at RUSNANO in 2014. Prior to that Alex worked in senior risk roles at Skolkovo Foundation, Strategy Partners, PwC and Deloitte. Alex recently published his second risk management book called “Guide to effective Risk Management 3.0”. Alex also regularly presents at risk management conferences in Russia and Europe. In November 2012 Alex short a series of TV programs dedicated to risk management in start-ups. Alex teaches risk management at major Russian business schools including OpUS, Technopark Skolkovo, MIRBIS, MFUA, SKOLKOVO and USIB as well as corporate universities, like Gazprom. He has successfully completed his double Bachelor degree in Risk Management and Econometrics at Monash University, Australia, achieving the top risk management and statistics student award two years in a row.