

Best Organizational Governance Practices

**Effective Governance and Oversight Task Force
City Council and Staff
5pm and 9am, February 25 and March 4
Vaughan, Ontario**

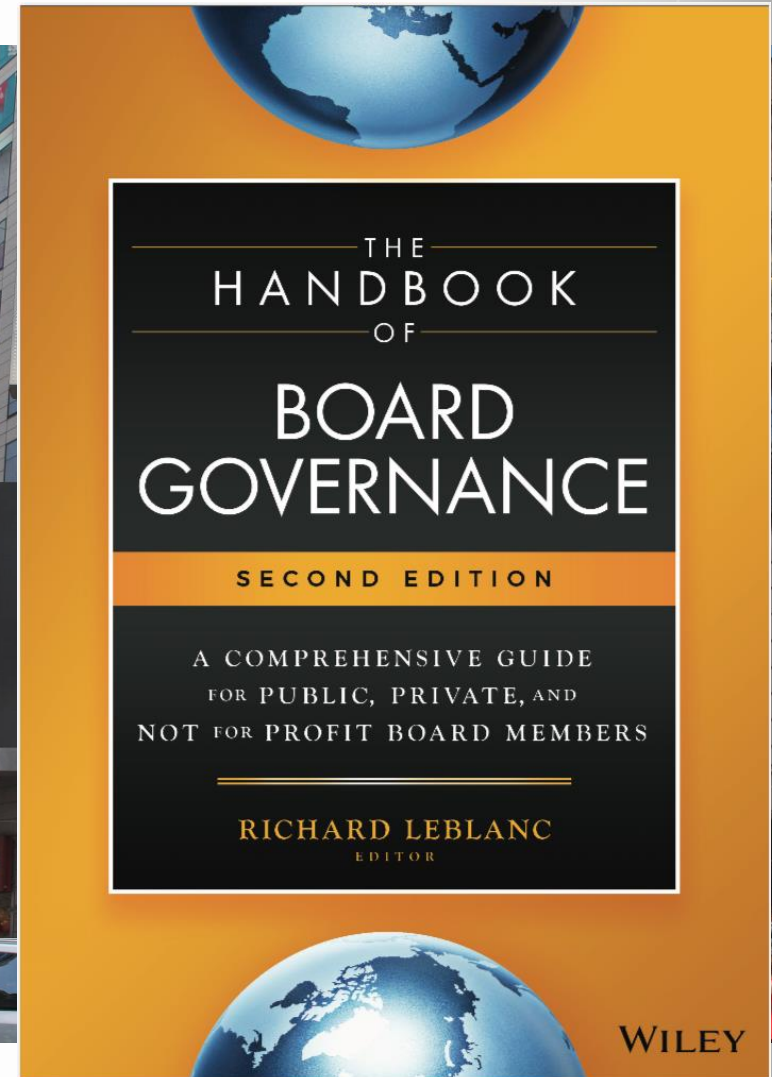
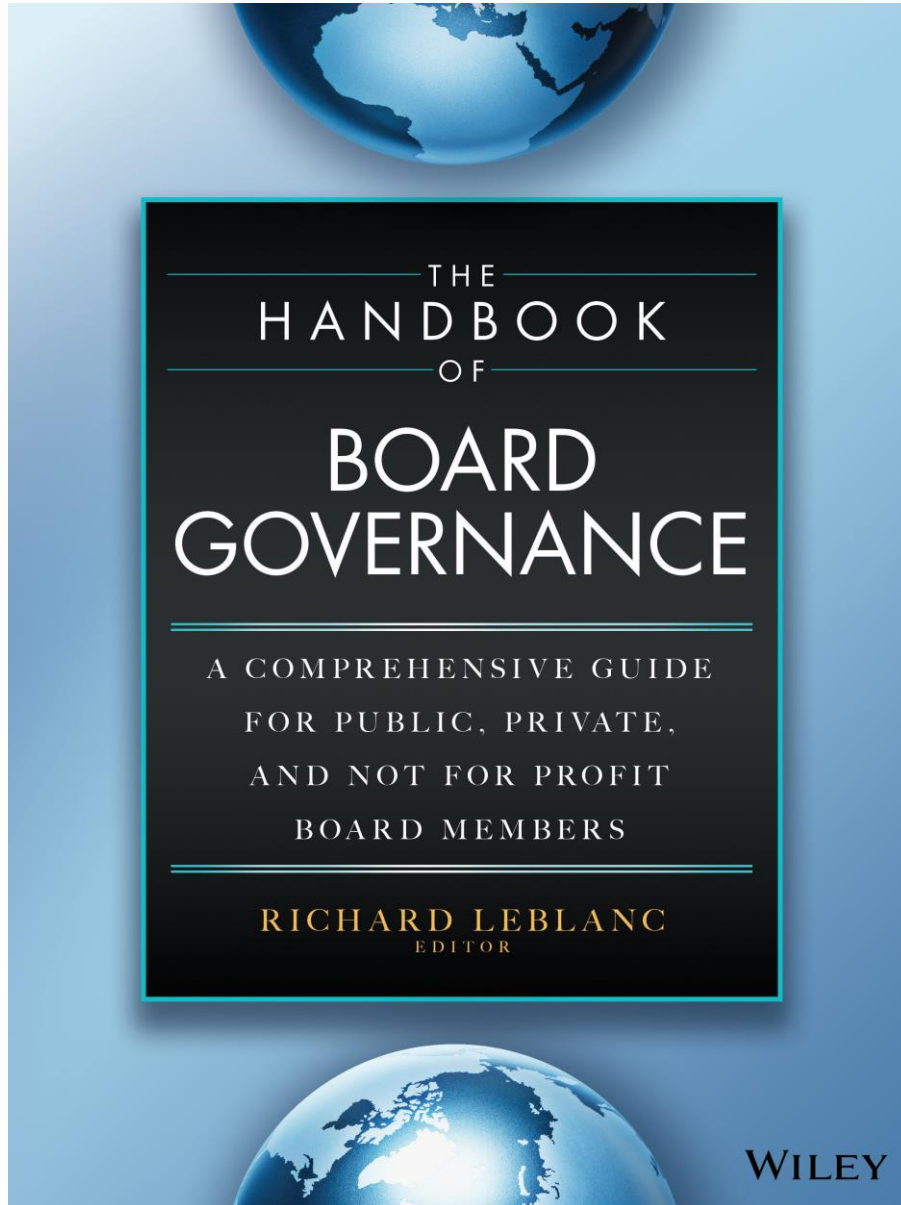
**Richard Leblanc, CMC, BSc, MBA, LLB, JD, LLM, PhD
Professor of Governance, Law & Ethics,
York University, and
Independent Advisor to Boards of Directors**

- Political leaders are often under-boarded;
- Government is not governance;
- Fiduciary duty is conflated with constituent advocacy;
- Self-serving behavior is conflated with public trust;
- Lack of training, controls and low barriers to entry;
- Staff knowledge, reliance, over-reach;
- Large concentration of power in lead executive role (Mayor, Premier, Prime Minister) absent controls;

- Reluctance to impose controls, limits on oneself;
- Resistance to codes, standards, transparency;
- Government is thought to be different;
- Denial, inertia, inaction, blame, political frustration;
- Limited triggers to correct: Impeachment, elections;
- Best governance practices often absent as a result;
- Best governance practices to come;

What I will address

- **1. Fiduciary duty, duty of care, and conflicts of interest;**
- **2. Tone throughout organization and whistle-blowing;**
- **3. Strategic role of the governing body;**
- **4. Composition of the governing body;**
- **5. Behavioural vetting of governors;**
- **6. Board dynamics and tone at the top;**
- **7. CEO (CAO) succession;**
- **8. Non-financial risk oversight by governing body;**
- **9. Cyber-security, BYOD and social media;**
- **10. Questions and Answers.**



There is not an excuse that I have not heard

- “It doesn’t apply to our sector or company.”;
- “It costs too much.”;
- “It is too difficult to implement.”;
- “We have never done it this way.”;
- “Regulators lack jurisdiction.”;
- “Our board is perfectly fine.”;
- “It is the law of unintended consequences”;
- “It is one sized fits all approach.”;

What does governance failure look like?

7



The New Governance Normal

8



What was my role and what happened?

9

- Called in by board, regulator, police, monitor, judge, law firm;
- Bribery and corruption within the company and board;
- Property destruction and death;
- Stock manipulation and fraudulent financial statements (several);
- Sexual misconduct;
- Improper expenses;
- Extensive lawsuits against directors: “I will [mess] up his life”;
- Significant fines and loss of reputation;
- Interviews of fraudsters (prison in three cases);



What have I learned from governance failure and success?



There are no bad companies, only bad boards. Look to the board, not the company.

**I am not here as a
municipal expert
but rather a
governance
expert.**

1. Legal Responsibilities: Fiduciary Duty

- The duty properly defined, understood and applied;
- There is no fiduciary duty to stakeholders, or even shareholders/members, in Canada;
- You cannot have a duty to more than one beneficiary;
- If you are there to represent your interests, or that of a stakeholder/shareholder, you are poison to your board;
- You are not there to represent any stakeholder, but rather the best interests of the organization as a whole;
- How to address inevitable conflicts of interest;

- COI Policy that is robust in its design and controls;
- The standard is objective, not subjective;
- Complete disclosure of related financial affairs, of yourself, your family and your affiliates, to Audit Committee;
- Declaring the conflict and not influencing, recusing from voting;
- Why the conflict / related party transaction?
- Whistle-blowing if conflict is not declared;

- Independent assurance of management of the conflict (Internal Audit, external);
- Creation of special committee of directors disinterested from (i) the conflict and (ii) conflicted director(s);
- This is all uncomfortable but the right thing to do;
- Code of conduct (robust) and sign off, and controls, and disclosure, by Directors, to a Committee, and to the BOD;
- Assume self interest by Directors: Are you white, grey or black? I have never seen grey become white;

- Reasonably prudent person would act under similar circumstances;
- You need to bring forth your skill set and you may be treated differently as a result;
- You can and will be scrutinized by a court or judge on the process you used for oversight and decisions;
- Use of committees to review and recommend;
- Business Judgment Rule insulates you ONLY with a proper process and exercise of that process;

- Lack of distraction (social media, text, email, shopping);
- Attendance, in person, and for full duration of meeting;
- Information is life blood of the board: quality, quantity, format, timeliness, relevance, source;
- Setting of Board and Committee agendas and time allocated commensurate with importance;
- Use of Competency Matrix;
- Asking questions;

Getting independent advice;

- You can be independent and captured;
- Objective, reasonable standard standard;
- Time limits: 9-10 years;
- Research tends to support limits, rotation;
- Research on social relatedness, origination;
- Gifts, vacations, perks, office, friendships, jobs for kids or friends: capture the director;
- Independent auditors and compensation consultants;

2. Tone Deep Inside the Organization

19

- Does bad news rise? How do you know?
- Anonymous, protected, remedied whistle-blowing?
- Employee surveys anonymous directly to board?
- Independent audit of culture?
- Risk takers inappropriately incented?
- Is your tone at the top unambiguous and consequential?
- Does the board report on culture?

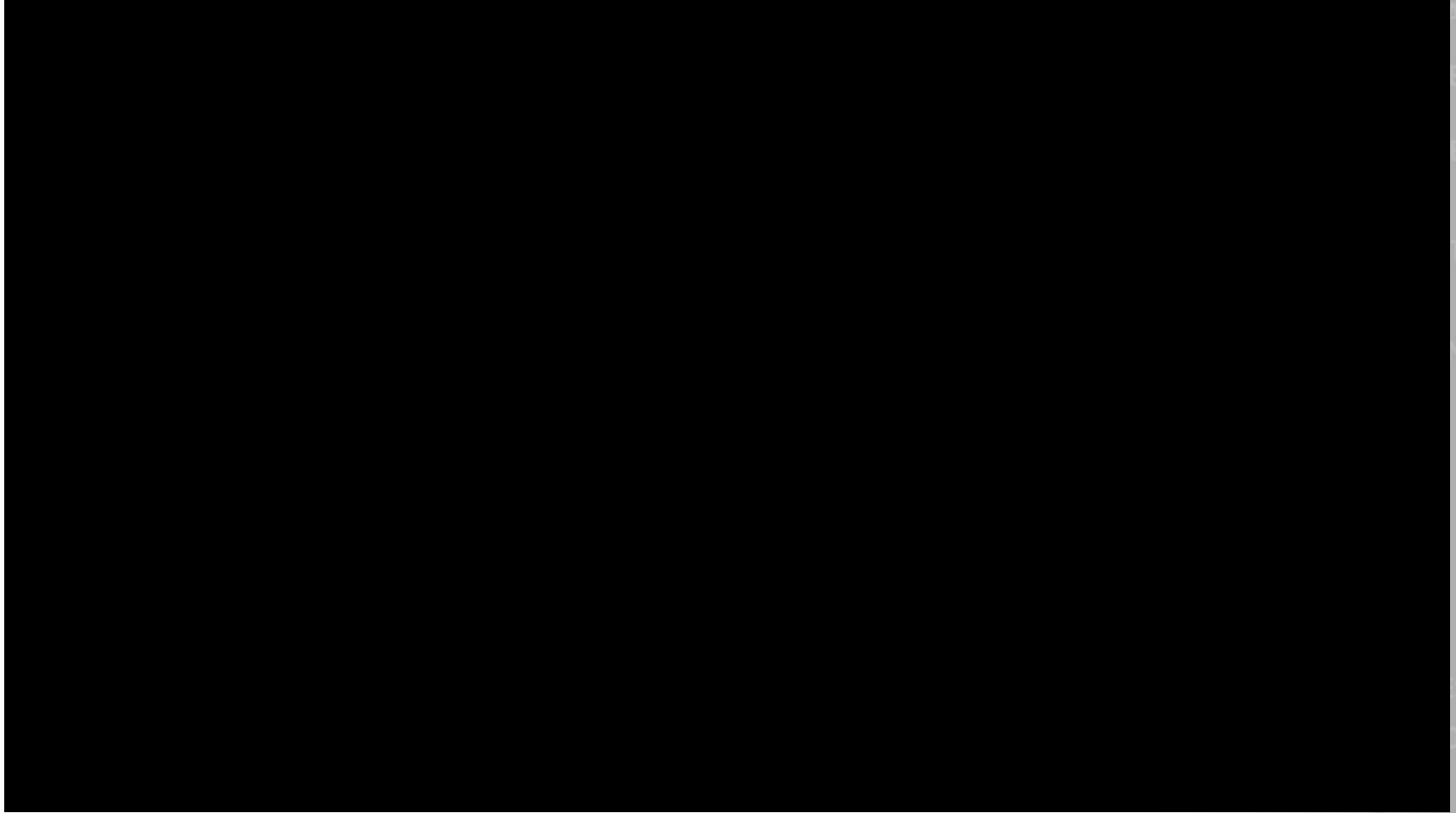
Tone at Top: A Good Example

20



Tone at Top: Another Good Example

21



Director Code of Conduct and Conflict of Interest Declaration

Table of Contents

1. Introduction and Purpose of this Code	1
2. Application of this Code	2
3. Compliance with Laws, Rules and Regulations, and Ethical Conduct	2
4. Duties and Responsibilities of the [REDACTED] Directors	2
5. Conflicts of Interest	2
6. Gifts, Hospitality and Honours	5
7. Expenses of Directors	5
8. Reporting of Illegal or Unethical Behaviour	5
9. Political and Outside Activities of Directors	5
10. Confidentiality of Information and Disclosure of Information	5
11. Relations with the [REDACTED] Staff	6
12. Expectations of Directors	6
13. Monitoring and Enforcement of the [REDACTED] Director Code of Conduct	7
14. Directorial Certificate of Compliance with the [REDACTED] Director Code of Conduct (Certificate)	8

14. Directorial Certificate of Compliance with the [REDACTED] Director Code of Conduct (Certificate)

Each Director shall sign this Certificate and Declaration annually.

To the best of my knowledge, information and belief:

1. I have read the [REDACTED] Board of Directors' Code of Conduct (Code).
2. I understand this Code, each of its fourteen Sections, and all of its Paragraphs.
3. I have sought clarification from the Audit Committee or the Board Secretary with respect to this Code's sections, meanings, interpretation, and application to my circumstances, as the case may be.
4. I have been, presently am, and agree to be prospectively, in compliance with the letter and spirit of each and all provisions within this Code.
5. If I come to acquire knowledge, information or belief that I am not, or may not be seen to be, in compliance with the letter and spirit of a provision within this Code, I shall promptly bring such knowledge, information or belief, as the case may be, to the attention of the Audit Committee in a prompt, full and true manner.
6. I know of no other Director, family member, affiliate, staff member of the [REDACTED], or any other person or entity that is not, or may not be seen to be, in compliance with the letter and spirit of each of the provisions within this Code.
7. If I come to acquire knowledge, information or belief that any of the foregoing persons or entities in Paragraph 6 are not, or may not be, in compliance with the letter and spirit of a provision within this Code, I shall promptly bring such knowledge, information or belief, as the case may be, to the attention of the Audit Committee in a prompt, full and true manner.
8. I understand that the Code is subject to change from time to time, and that I will be given adequate notice of such changes.

I, _____, hereby accept the terms described in the [REDACTED] Director Code of Conduct dated this ____ day of _____ (month), _____ (year).

3. Strategic Role of the Governing Body

24

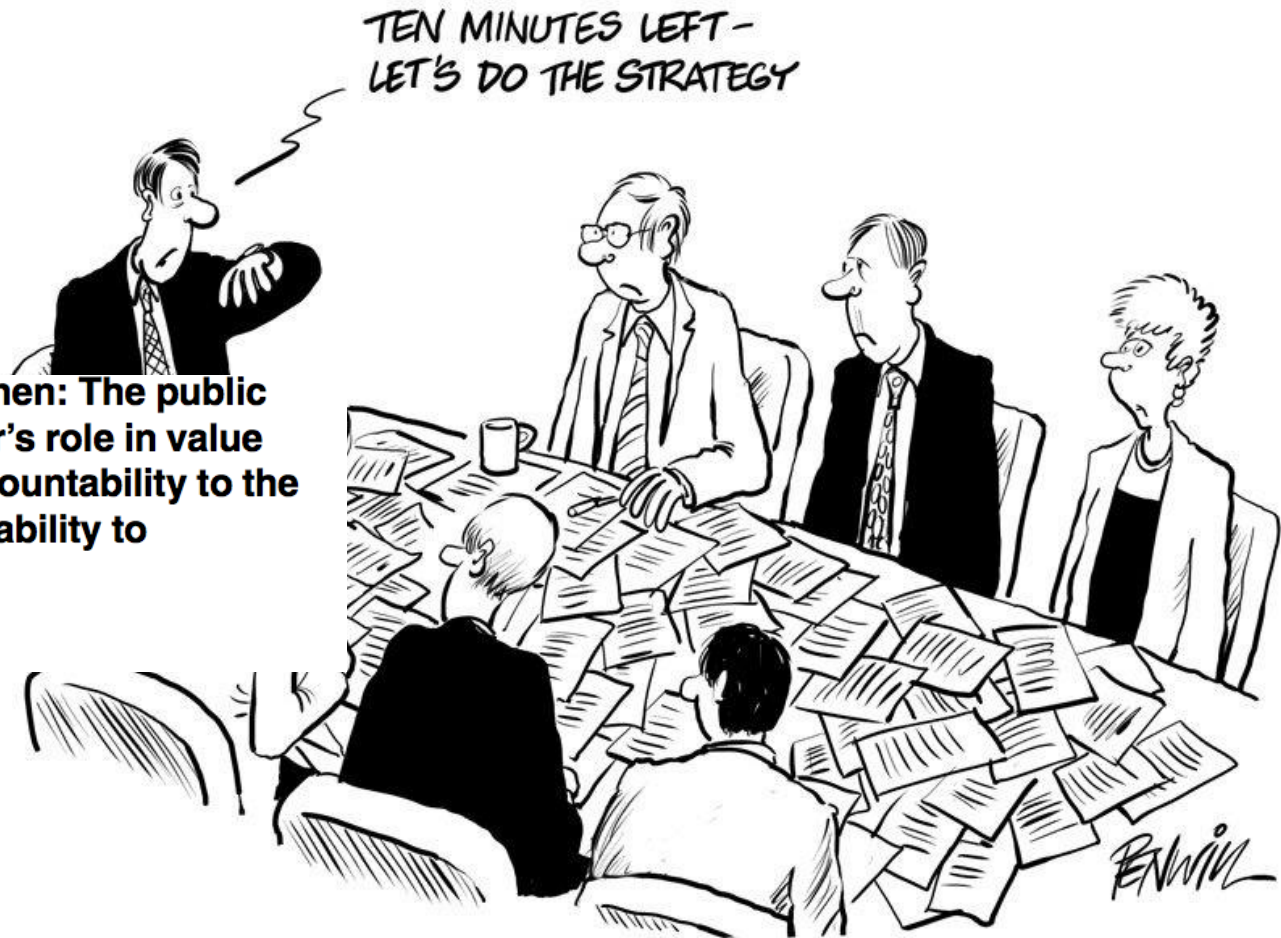
- Is each Director linked to your business model?
- Does your board spend 50% of its time on strategy?
- Do you fully understand the business model?
- Is 50% of your matrix linked to strategy?
- Whole board vs. a board committee;
- Do you conduct a 360 degree review including management?



Forty proposals to strengthen: The public company Board of Director's role in value creation; management accountability to the Board; and Board accountability to shareholders

Received (in revised form): 4th July 2013

Richard Leblanc



www.independentaudit.com

- Board encouraging during unpolished crystal ball:
Immature non-financial metrics: Ex, Cx, Px, Mx;
- 75% of the value of a Company is non-financial;
- Lagging vs. leading indicators: Lagging is too late;
- A Board cannot oversee a PowerPoint deck;
- How to ask a “strategic” question as a Director?
- This will not work if a Board does not have the
right Chair and the right Directors;

Strategic Plan – Value Drivers and KPIs

Organization

Draft Template of Value Drivers of Business Model

Name of the Value Driver (“Value Driver” or “Pillar”):

Definition of the Value Driver:

How Does Your Value Driver Contribute to the Mission of the Organization?:

Quantitative Measurement(s) of the Achievement of the Value Driver: (How is the Value Driver being measured? Please explain why these measurements are being used, and define any measurements or acronyms that are not in common parlance of a Director.)

Qualitative Description of the Achievement of the Value Driver: (Please explain clearly and simply how the achievement of the Value Driver is being measured.)

What is the Relative Weighting of the Value Driver in the Overall Business Model (e.g., what portion of 100%): What is the relative importance of the Value Driver in the overall Business Model of the Organization? What are some of the causal inputs and outputs for the Value Driver?

Key Performance Indicators to Measure the Achievement of the Value Driver (What specifically constitutes Low, Medium and High Levels of Performance?) In other words, what does Success look like? In a way that is SMART.:

6-7 page template for each VD to Board

Key Initiatives Needed in the Achievement of the Value Driver:

Resources Needed in the Achievement of the Value Driver:

What Can Impair the Achievement of the Value Driver (Risks), and How Has this Been Addressed?

Who is the Primary Senior Manager Responsible for the Achievement of the Value Driver?

Who Are Other Members of Management Responsible for the Achievement of the Value Driver?

What External, Competitive, or Third-Party Validation or Comparison has Been Undertaken in the Above?

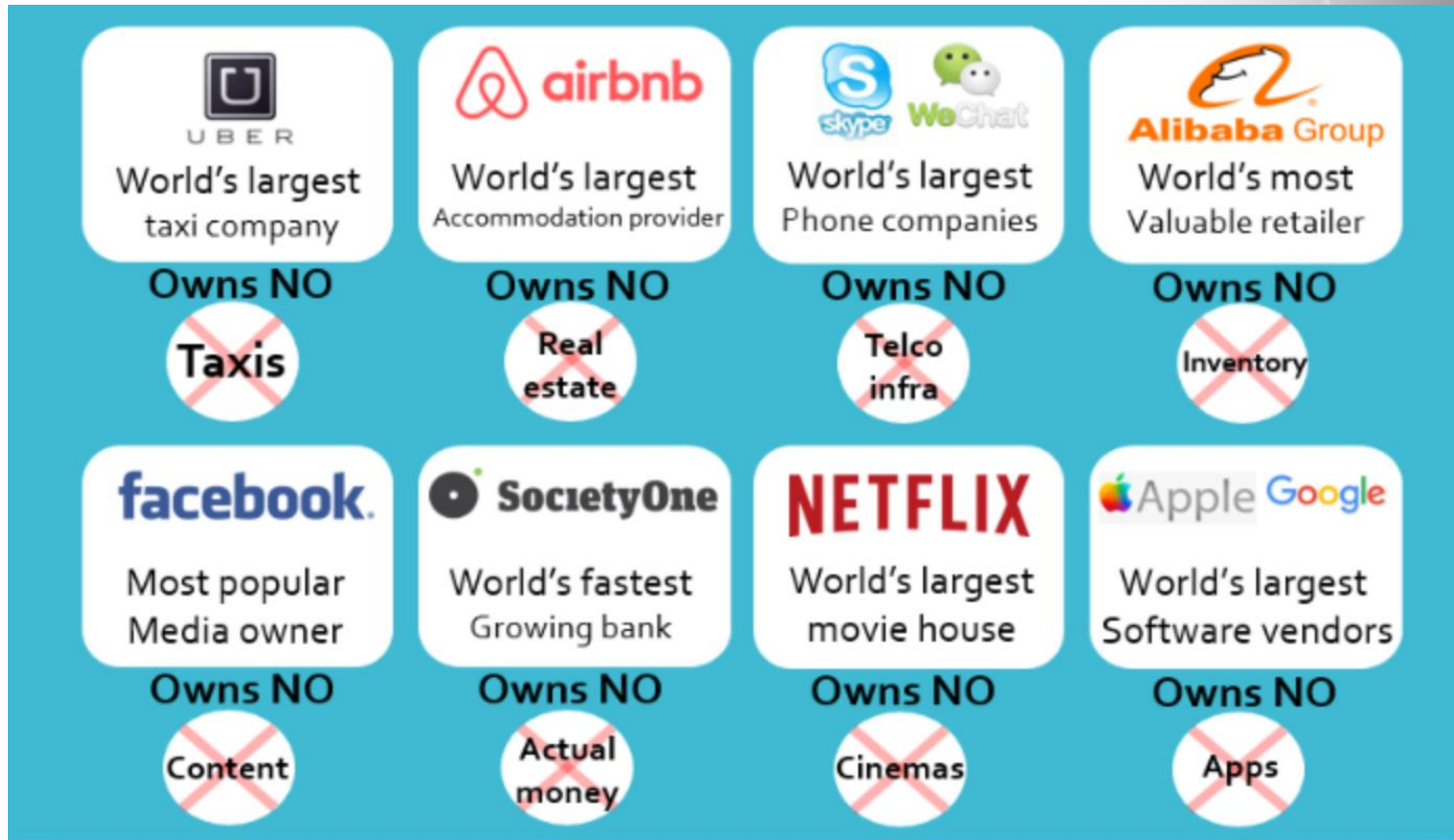
Conclusion: Please offer your concluding thoughts on the Achievement of the Value Driver.

Signature.....
Senior Manager Responsible for the Achievement of the Value Driver

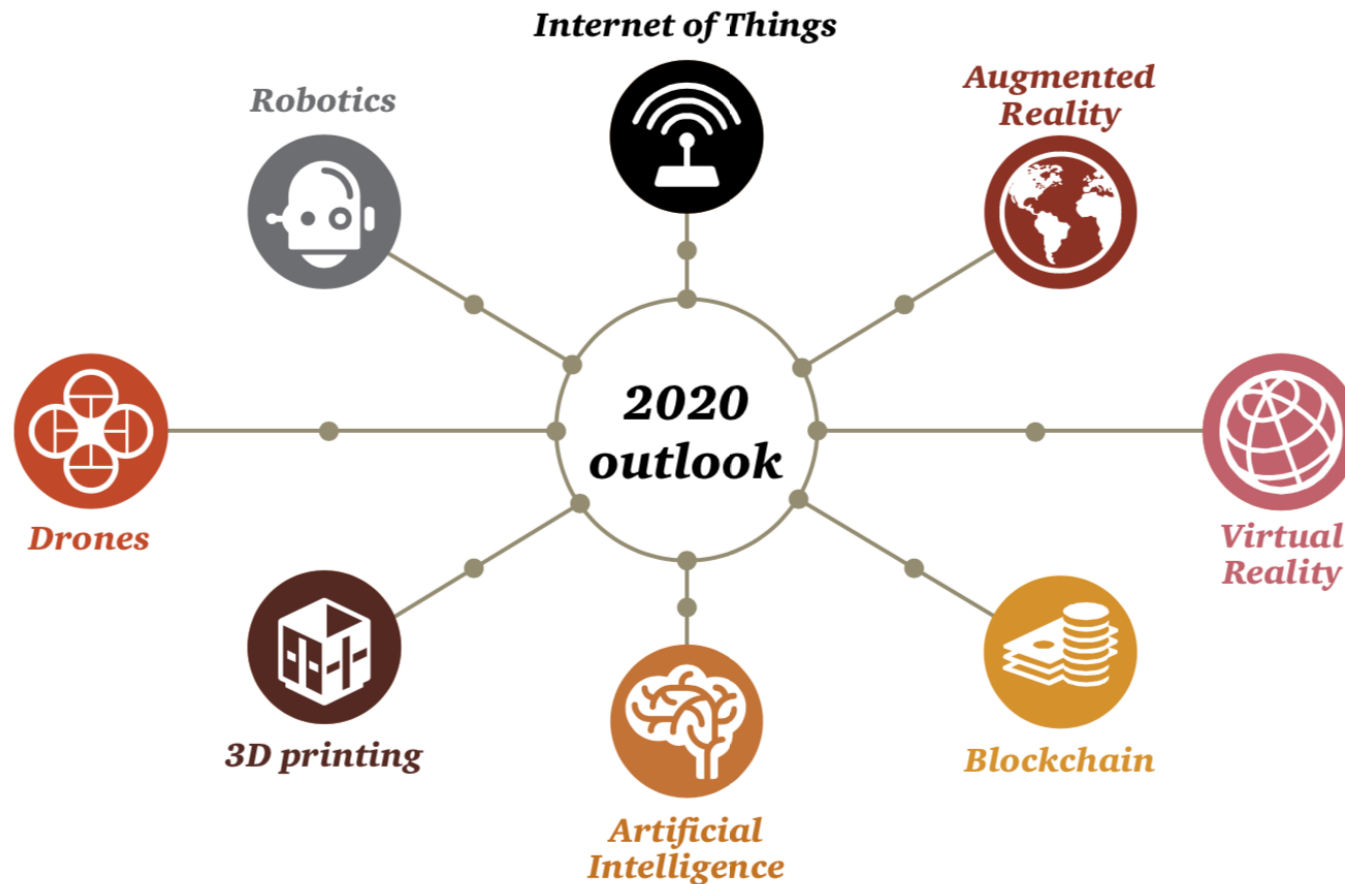
—

The digital disruption to business models

29



The disruption to traditional business models³⁰



How can boards tackle the Essential Eight and other emerging technologies?

Source: PwC Governance Insights Center, Technology Series

- Board, led by Chair, sets standards for vigorous value creation process, establishes ambitious value creation criteria, and leads management to develop optimal value creation plan;
- Deep dives and due diligence by directors into company, business model, industry and markets to understand value drivers, innovation opportunities and associated risks;
- Board approves plan and its milestones, monitors progress regularly, calling for prompt corrective action to ensure goals are met, including increased goals as new unplanned/unanticipated opportunities arise;

- Value maximization plan clearly and simply spells out key timelines, milestones, targets, and individuals accountable for each key plan component and specific results;
- Reporting format and information flow provides frequent, timely and accurate information to board on plan progress and any variances;
- Board addresses plan variances quickly and directly: management provides concrete responses on how shortfall will be corrected, by whom and when;
- Chair adopts a primary role in foregoing;

- Maintenance of 'day to day' management by CEO and rest of executive team;
- Highly engaged level of functioning by board and a shift in primary focus towards value creation;
- Robust debate and review of plan execution is primary board meeting agenda item; and at least one presentation each board meeting from key personnel below the senior level, on that particular individual's role in the value maximization plan and a full discussion of progress to date in that regard;

- Regular, robust communication between board and executive team, including open communication below the senior management level, in large part not focused on “oversight” but on engaging others in regard to their role in the company’s business and value maximization plan;
- Board links value creation plan execution to simple, straight-forward incentive performance metrics so direct link between management wealth creation and the performance and increase in equity value of company;
- Direct link to performance, value creation or the need to hit certain targets before any incentive compensation kicks in, below which management gets nothing.

4. Composition of the Governing Body

35

- Do you link board tenure to peer performance?
- Do you have 30-40% women on your Board?
- Do you conduct a skills review of Directors?
- Independence of mind? Grey directors?
- Do you disclose Director skills and education?
- Can investors remove and propose Directors?
- Do you meet with investors independent of Management to discuss Board composition?

Example of board diversity and competency

36

Women	Designated Group
Visible Minority	
Aboriginal Peoples	
Persons with Disabilities	

Broad strategic
role and
industry
knowledge

Market Knowledge									
Geography				Industry					

CEO/GM of Large Organization	Enterprise Leadership
CEO/GM of Small/Medium Organization	
Other Experience with Large Organization	
Other Experience with Small/Medium	
Experience "Under Fire"	
Active Professional	
Volunteer/Community Organization	

Functional Capabilities

Accounting/Tax
Financial Planning
"Financial Expert"
Sales and Marketing
Public Relations
Government Relations
Investor Relations

Strategic Planning
Human Resources Management
Information Technology Management
Legal/Regulatory
Compliance
Risk Management
Governance
Sustainability/Corporate Social Responsibility

Board Competencies

Sample Board Competency Matrix




Director	Director Competencies						
	1	2	3	4	5	6 Audit Committee Chair	7 Board Chair
Core Competencies							
Audit and Compliance	G	G	S	G	G	E	S
Board and CEO Performance	G	G	G	G	S	S	S
Credit Union Operations	G	G	G	G	G	S	S
Financial Literacy	G	G	G	G	G	E	S
Governance and Ethics	B	B	G	B	G	S	S
Leadership	B	B	G	G	G	S	E
Regulatory Environment	B	G	G	G	G	S	S
Risk Management	B	B	S	E	S	E	S
Strategic Planning	B	B	B	G	G	S	E
Overall Core Competency Level	B	B	B	G	G	S	S
Other Competencies							
Information Technology	B	G	B	B	G	S	G
Marketing	B	B	B	S	G	B	G
Legal	B	B	G	B	B	G	S
Entrepreneurship	E	G	B	B	G	G	S
Economics	B	G	S	G	G	B	S

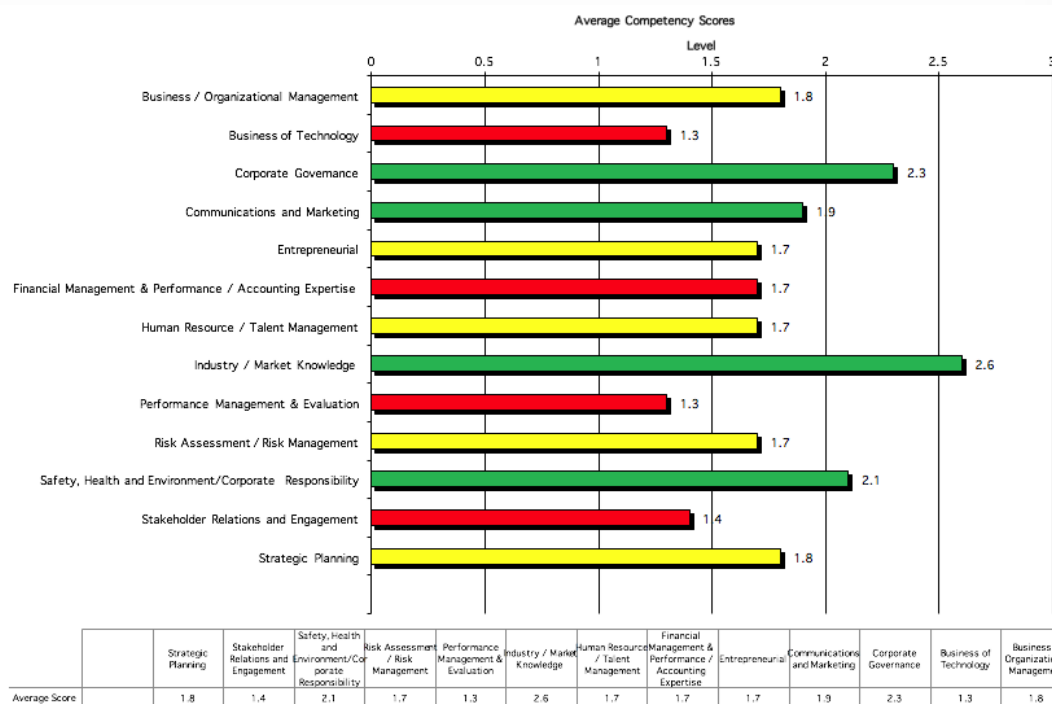


For a FRFI, relevant financial industry and risk management expertise are key competencies for the Board. There should be reasonable representation of these skills at the Board and Board Committee levels.

1. Risk Expertise on the Board?

Does the Board have risk expertise on it?

Risk Assessment / Risk Management Full understanding of enterprise risk management, including identifying, controlling, reporting and assuring material financial and non-financial risks, within an overall risk appetite framework.	1.0:  2.0:  3.0: 	1.7	Strong (see yellow to left): Six Directors Expert (see green highlight to left): One Director
---	--	-----	--



What are practices now? (49% no women)

39



CHALLENGE

CREATE

EVOLVE

TH

QUESTION

INNOVATE

TRANSF

PROVO

RESEARCH

STUDY

DECONSTRUCT

Homogeneity and group think

40

©Cartoonbank.com



"All those in favor say 'Aye.'"
"Aye."
"Aye."

"Aye."
"Aye."
"Aye."

Diverse groups
are tougher to
manage but may
make better
decisions.

Measuring Board Diversity

41

Board Diversity														Total
1.	Male		•	•			•	•	•	•	•	•	•	9
	Female				•	•						•		3
2.	Ethnic			•										1
3.	Age	30 - 39		•										1
		40 - 49					•	•			•			3
		50 - 59			•	•				•				3
		60 - 69	•				•			•		•		4
		70 - 72											•	1
4.	Urban		•	•	•	•	•	Small	•		•	•	•	10
	Rural								•			•		2

5. Behavioral Vetting of Directors

42

- Criminal, credit, social media checks?
- Background and thorough reference checks?
- Signed letters of resignation up front?
- Peer assessment of behavior?
- Ongoing integrity controls of Management and Directors?
- Internal controls over social media, reputation?
- Peer mentoring of behavior?

A. Strategic and Advisory Orientation

1. Knowledge
2. Judgment
3. Resources

B. Monitoring and Oversight Orientation

4. Conscientiousness
5. Capacity to Challenge
6. Willingness to Act

C. Analytical and Thinking Skills

7. Conceptual Thinking Skills
8. Financial Acumen
9. Decision-Taking Skills

D. Interpersonal and Social Style

10. Communication Skills
11. Teamwork Skills
12. Influence Skills

E. Integrity and Loyalty

13. Integrity
14. Independent Judgment
15. Organizational Loyalty

8. Please rate the board's performance in Addressing Director Under-Performance or Poor Behaviour.

Choice	Votes	Percentage
10 - Perfect - no improvement possible	5	2.39%
9 - Truly Outstanding	21	10.05%
8 - Excellent	26	12.44%
7 - Very Good	46	22.01%
6 - Good	43	20.57%
5 - Fair	37	17.70%
4 - Poor	21	10.05%
3 - Very Poor	5	2.39%
2 - Terrible	3	1.44%
1 - Not at all Effective	2	0.96%

More Director Behaviors That Should be Assessed, Recruited For

45

- Integrity and personal / professional ethics;
- Communication skills: listening, speaking, writing;
- Teamwork skills: group, consensus, social, self aware;
- Impact, influence, coaching and development;
- Leadership / chair skills: meeting, agenda, information;
- Intellectual curiosity, bias to learn, quick study;
- Capacity to challenge constructively: tone, words;
- Conscientiousness, diligence, duty of care, preparation;

Behaviors That Matter and Director Evaluation 46



Developmental Opportunities

#	Competency	Self Score	Peer Score	Peer - Self Gap	Board Avg	Peer - Board Gap
10.	Financial Acumen	7.00	6.38	-0.62	7.21	-0.83
7.	Willingness to Act	7.00	6.43	-0.57	7.22	-0.79
6.	Capacity to Challenge	6.00	6.50	0.50	7.23	-0.73
15.	Influence Skills	7.00	6.64	-0.36	7.03	-0.39
13.	Communication Skills	7.00	6.71	-0.29	7.33	-0.62



Self Score: the score you rated yourself for each competency.

Peer Score: the score your board colleagues rated you for each competency.

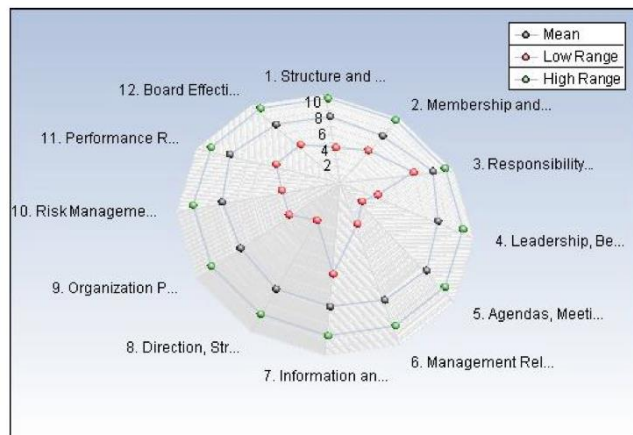
Peer-Self Gap: your Peer Score minus your Self Score. Red occurs when your Self is less than your peers did.

Board Average: the average score for this board (all directors) for each competency.

Peer-Board Gap: the Peer Score minus your Board Average. Red, in this case, occurs when your Peer Score is less than the Board Average.

N/A: either no rating was received or the N/A was selected and therefore no score was calculated.

BEAM™ Summary Profile



Category (In Descending Board Average Order)																Board Average
1. Integrity and Loyalty	8.36	8.07	7.93	7.90	7.76	7.90	7.81	7.64	7.69	7.62	7.52	7.64	7.69	7.47	7.57	7.77
2. Strategic and Advisory Orientation	8.31	8.00	7.90	7.66	7.52	7.35	7.12	7.00	6.98	6.84	7.26	6.90	6.87	6.50	6.68	7.27
3. Monitoring and Oversight Orientation	7.98	7.93	7.45	7.67	7.57	7.16	7.36	7.44	7.21	7.28	6.86	6.79	6.79	6.97	6.55	7.27
4. Analytical and Thinking Skills	8.07	8.07	7.38	7.43	7.07	6.97	7.38	7.38	7.28	7.63	6.78	7.13	6.80	6.73	6.43	7.24
5. Interpersonal and Social Style	8.24	7.86	7.55	7.50	7.36	7.28	6.83	7.03	7.12	6.67	7.07	6.98	6.76	7.05	6.71	7.20
Overall BEAM™ Score	8.19	7.99	7.64	7.63	7.46	7.34	7.30	7.30	7.26	7.21	7.10	7.09	6.99	6.95	6.79	7.35

Green Score: 8.0 or above

Red Score: 6.0 or below

6. Board Dynamics and Tone at Top

47

- Do you speak up? Always?
- Do you meet in executive sessions (good boards twice per meeting)?
- Is ego left at the door?
- Will you rid yourself of a problem director or CEO?
- Is any Chair captured or entrenched?
- Is your CEO dominant or entrenched (examples)?
- Diversity, term limits, retirement, renewal?

In Camera or Executive or Board Only Session⁴⁸

- Widely regarded as a best practice;
- No management or staff;
- No agenda;
- No notes;
- No decisions;
- No leaks;
- Debriefing with the CEO;
- Happening now at committee levels.

- A Director's behavior: tone, approach, frequency;
- A Director who does not support board decisions;
- A Director who acts out of self interest;
- A Director who says one thing, and does another;
- Talking over people (disagree vs disagreeable);
- Toxic emails vs. board meetings;
- A Chair who weighs in too early, or unduly influences the collective Board, or who is owned by the CEO;

- Committees review and recommend, do not approve or decide: Committee first, then the Board;
- Risk and oversight coverage: committees;
- Match competencies to committees;
- A word on independent oversight functions;
- Governance / Nominating Committee recommends board and committee membership and chairship;
- Proper committee charters, agendas and reporting;
- Committee chair leadership important;

- The Board has one employee;
- The Board and each Committee acts as a unit;
- Directors do not act as Directors (several examples);
- Rogue Directors should be stopped immediately by the Board Chair in their behaviours;
- Proper documentation so the Governance and Management lines are well known and enforced;
- Improper Stakeholder-Director communication;
- One Director and a weak Chair can wreck a Board;

7. CEO (CAO) Succession

52

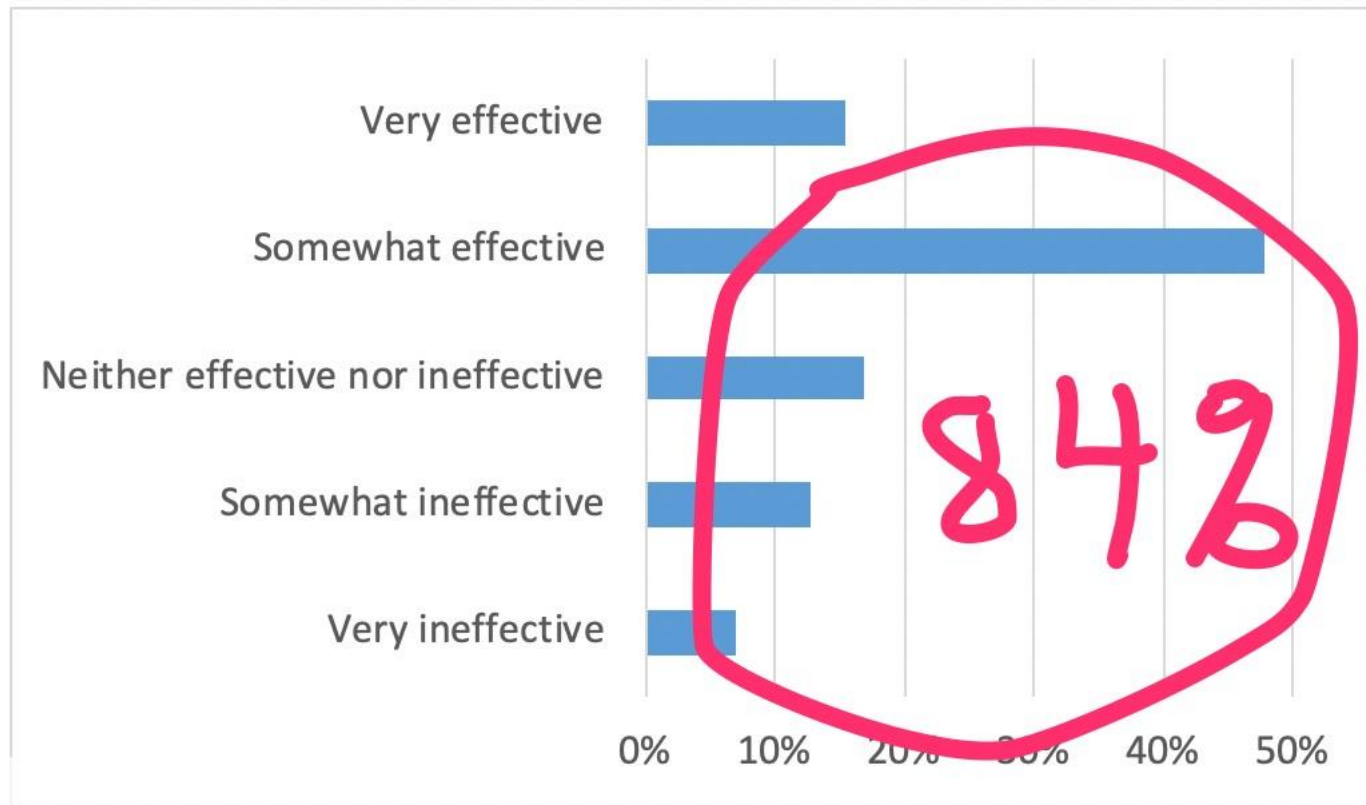
- Internal candidate who is CEO-ready (example)?
- Executive sessions twice each meeting?
- Full cooperation of incumbent CEO?
- Exposure to high potential talent (example)?
- Documented CEO succession plan?
- Full board involvement?
- Do you have the ability/courage to fire your CEO?

Number	Task
1	CSC Charter approved by BOD
2	CSC inaugural meeting, with project plan established by CSC and reviewed by BOD
3	Current vision, mission, strategy (summary) provided by incumbent CEO
4	Prioritized attributes for incoming CEO established + linked to strategy
5	Attributes for incoming CEO reviewed by BOD
6	Desired background, education, and experience required in the ideal candidate also set out
7	Retainer established for CSC Chair and Members and approved by BOD
8	Position description for incoming CEO (current PD to be reviewed by CSC and amend if need be, as drafted by RL for
9	Define key success factors, most important attributes for prospective CEO (must haves)
10	Drafting of CEO advertisement
11	Prepare package for prospective CEO candidates (overview of strategy, financials, organizational chart, brief backgr
12	Post advertisement, outreach to members, other stakeholders, the sector and broader community to reach and ge
13	CEO salary range (past, current and expected)
14	CEO incentive range (link strategy and key performance incentives to incentive pay for prospective CEO) (review of
15	CEO benefit package
16	Locations CEO may be based in, or other expectations
17	Board to approve pay package + benefits + employment contract for potential hire
18	Receive resumes, create long list, matching candidate background to attributes, identifying best 10-12 candidates
19	CSC telephonic meeting to discuss, create shorter list (top 5-7), and rank short list if possible
20	Create short list and share with BOD, with brief candidate profiles

21	Request telephone / video interviews with short-listed CEO candidates
22	Draft interview questions for short-listed CEO candidates
23	Due diligence on short-listed candidates (background, reference checks, etc.)
24	Interviews with short-listed candidates (video or phone)
25	CSC telephone meeting to discuss interviews, rank short listed candidates based on interviews
26	Further due diligence on top 2-3 finalists
27	Develop draft employment contract for BOD approval
28	Request for telephone interviews with finalists
29	Second interviews with top 2-3 finalists
30	CSC telephone meeting to discuss interviews
31	CSC to present report to BOD in August meeting on finalists and any recommendation
32	Preliminary negotiation (pay, contract) if CSC to recommend (a) hire of incumbent or (b) hire of another finalist to e
33	CSC to recommend / BOD to discuss (a) hire of incumbent; (b) hire of another finalist; or (c) expand search with hel
34	Board to approve hire (if (a) or (b))
35	Last round of due diligence and other checks
36	Finalize employment details with the successful candidate (if (a) or (b))
37	Conclude search (if (a) or (b)) or resume search if (c)
38	Board to approve key performance incentives
39	Review key performance incentives with CEO
40	CEO performance review after 3 and 6 months with updates to BOD
41	Continued onboarding of CEO

84% of CEO Evaluations are not effective

Effectiveness of CEO Performance Evaluation Process



Source: Stanford University and The Miles Group, in Richard Leblanc, Ed., The Handbook of Board Governance, forthcoming 2019, draft manuscript.

Chief Executive Officer Performance Evaluation

Introduction

The following Chief Executive Officer (CEO) Performance Evaluation (Evaluation) is an important part of XXX's continuing commitment to effective corporate governance. This Evaluation is designed to enable the Compensation and Human Resources Committee (Committee) and the Board of Directors (Board) to examine the CEO's effectiveness and establish goals for continuous improvement.

The CEO performance criteria, on which feedback from the CEO, XXX, is requested, reflect the expectations for this position as defined in the Chief Executive Officer Position Description (attached).

XXX should (i) respond to this Evaluation (i.e., a Self-Evaluation), and (ii) forward this Self-Evaluation to the Chair of Committee, XXX.

Results of this Self-Evaluation and Incentive Compensation of the CEO

The results of this Self-Evaluation, and the Employee Survey, will form the basis of:

- (i) A joint letter from the Chair of the Board and the Chair of the Committee to XXX, and
- (ii) A recommendation by the Committee, in the Committee's sole discretion, to the Board on the awarding of performance incentive compensation (i.e., a bonus) to XXX that shall not exceed XXX% of XXX's base compensation, which is \$X,XXX,000 for 201X. This bonus opportunity shall be weighted, in the discretion of the Committee, as follows:

1. Strategic Planning – 75 of 150 points;
2. XXX Relations – 35 of 150 points;
3. Board Relations – 20 of 150 points; and
4. XXX Relations – 20 of 150 points.

Total: 150 points

Model CEO CONTRACT

By: Dr. Richard Leblanc

BETWEEN:	2
AND:	3
WHEREAS:	3
NOW THEREFORE:	3
Position	3
Conditions	3
Roles and Responsibilities	3
Full-Time Employment and Restrictions on Outside Activities	3
Term of Employment	4
Reporting and Accountability to the Board of Directors	4
Performance Review	4
Strategic Plan and Goals and Objectives	4
Base Salary	4
Eligible Annual Incentive Compensation	5
Eligible Longer-Term Retention Incentive Compensation	5
Benefits	5
Pension Plan	5
Automobile Allowance	5
Vacation Entitlement	6
Travel and Subsistence Expenses	6
Compliance with the Company Board of Directors' Code of Conduct and Conflict of Interest Declaration	6
Confidentiality	6
Property of the Company	6
Non-Competition	6
Non-Disparagement	7
Non-Solicitation	7
Termination of Employment by the CEO	7
Termination of Employment of the CEO by the Board With Just Cause	7
Termination of Employment of the CEO by the Board Without Just Cause	7
Just Cause	8
Termination by Disability or Death	8
Contract, Amendment and Survival	8
Invalidity	8
Law Governing	8
Headings	9
Notice	9
Execution	9
APPENDIX A: CEO Position Description	9

8. Non-financial Risk Oversight by Governors⁵⁸

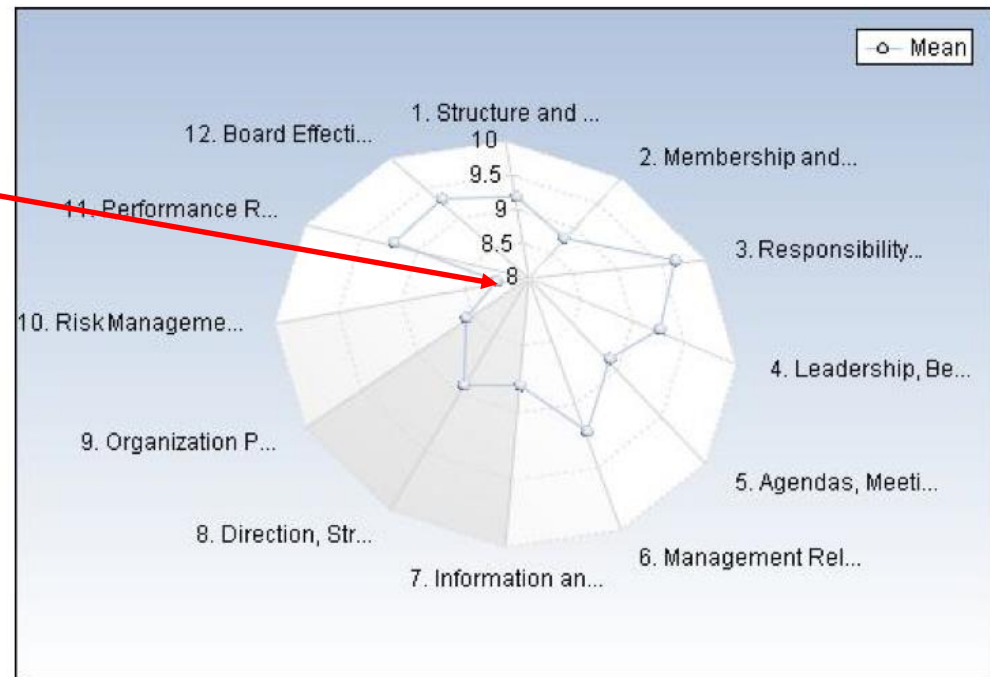
- 75% of your business model is non-financial;
- Written risk appetite framework?
- Risk-adjusted KPIs?
- Non-financial KPIs linked to pay?
- Emerging risks: Terrorism, active shooter, geopolitical, kidnap, populism, political violence, regulatory, trade, cyber, climate/natural disaster?
- Each non-financial risk in a committee?

Risk governance is often least effective by board

59

Shortly after
attempted terrorist attack

BEAM™ Summary Profile



1. Structure and Independence
2. Membership and Competencies
3. Responsibility, Ethics & Integrity
4. Leadership, Behaviours & Dynamics
5. Agendas, Meetings & Minutes
6. Management Relationships
7. Information and Internal Reporting
8. Direction, Strategy & Planning
9. Organization Performance and Executive Compensation
10. Risk Management Oversight and Assurance
11. Performance Reporting and Communication
12. Board Effectiveness, Improvement & Accountability

Oversight of Risk Management

60



Ex: “Top 15” ERM-related Risks, York University⁶¹

1. Government Policy Risk.
2. Competitor Risk.
3. Change Readiness Risk.
4. Capital Availability Risk.
5. Leadership Risk.
6. HR Non-Academic Risk.
7. Student Satisfaction Risk.
8. Communications Risk.
9. Organization Structure Risk.
10. Performance Measurement Risk.
11. HR Academic Risk.
12. Reputation Erosion Risk.
13. Strategic Labour Relations Risk.
14. Enrolment Targets Risk.
15. Resource Allocation Risk.

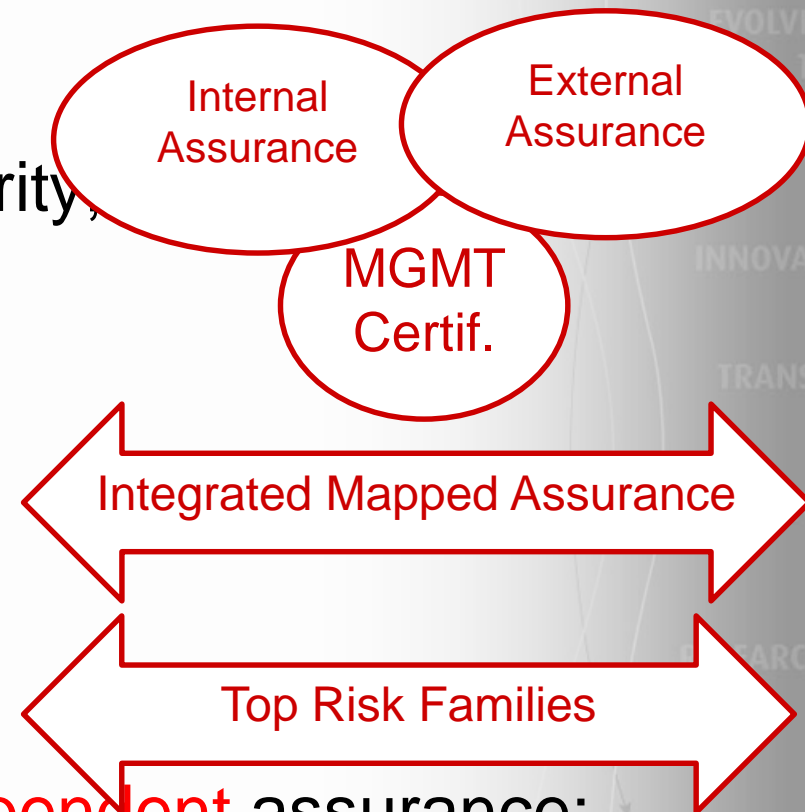
- Segregation of duties
 - Restricted areas
 - Approvals
 - Reconciliations
 - Record retention
- Safeguarding and asset accountability
 - Management override
 - Manual controls
 - Data Security
 - IT, inventory and other controls;
- Areas of vulnerability and fraud schemes;

ERM Risk Register Template

University Strategic Direction	Risk	Inherent Risk Before Response		Overall I.R. Rating Before Response	Risk Management Strategy & Points of Reliance	Residual Risk After Response		Overall R. R. Rating After Response	Accountability & Action Required
		Probability	Impact			Probability	Impact		
University Strategic Directions	IT Infrastructure will not support University initiatives (p. 9)	4 - Likely	5 - Major		Reduce ICT Foundational Document ITS Unit Plan Data Use Policy Etc.	3 - Possible	4 - Major		Complete plan Develop & implement college & admin unit plans including contingency & recovery •Etc.

	High	<i>Critical importance to the success of the University in meetings its financial and non-financial goals</i>
	Moderate	<i>Important but not critical to the success of the University in meetings its financial and non-financial goals</i>
	Low	<i>Risk does not have a material bearing to the success of the University in meetings its financial and non-financial goals</i>

- “Risk takers” & compensation;
- Non-financial risks and ICNFR: operations, technology, reputation, health, safety, security;
- Management knows the risks;
- Board:
 - Protect Internal Assurance;
 - **Complete, coordinated, independent** assurance;



- Formal documented risk appetite framework, with tolerances, registers and accountabilities;
- ERM that is integrated, dynamic and culturally embedded;
- Oversight functions compensation determined independently from business units, based on achievement of objectives of functions; no undue influence / conflicts;
- Risk function has input into performance metrics and compensation decisions of senior management;
- Third party reviews of risk, oversight functions;
- Crisis, contingency, scenario planning to Board;

Crisis Management: A Good Example

66



CHALLENGE
CREATE
EVOLVE
TH
QUESTION
INNOVATE
TRANSF
PROVO
RESEARCH
STUDY
DECONSTRUCT

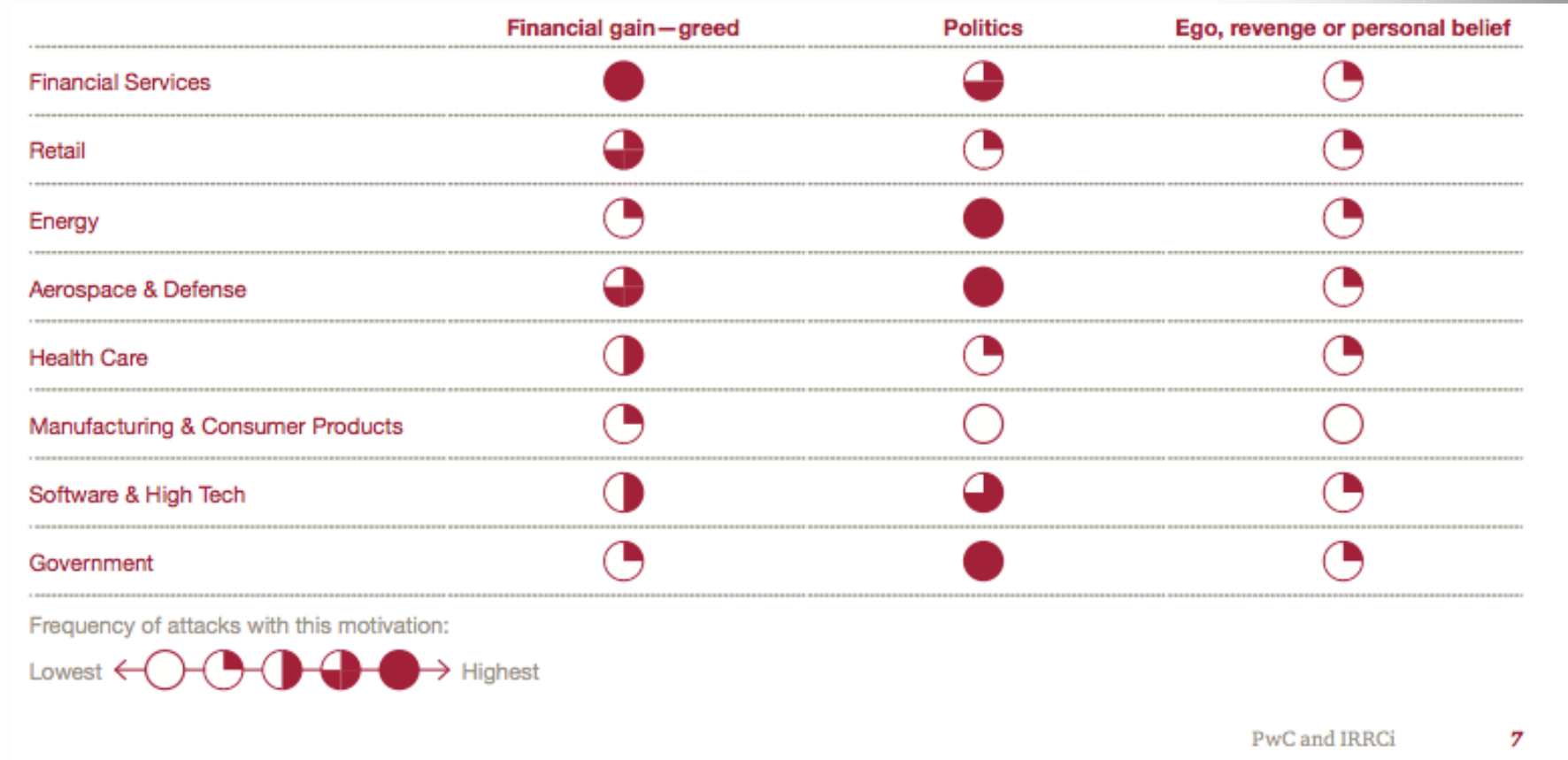
- Board-approved internal controls and policies?
- Information technology on your Board?
- Each Director cyber-literate?
- Cyber-standards adopted and implemented?
- Do you understand terms being used?
- Third party experts retained by Board?
- Crisis response plan?

Social Media, IT Governance Trends (cont'd) ⁶⁸

- Cybercrime: ~ \$9-21 trillion possibly at risk (NACD report);
- Cybercrime constitutes “greatest transfer of wealth in history” (NSA Chief);
- Head of FBI, James Comey: “impossible to count”. The internet is “the most dangerous parking lot imaginable.”;
- “There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese.”
- “Only 56% of companies conduct penetration tests, and 19% fail to test at all” (professional service report);
- Cyber criminals are at world cup level, and we are at high-school soccer level (Head of FBI analogy);

Internal Controls Over Cyber Security Risk

69



Source: PwC and IRRCi: “What investors need to know about cybersecurity”

Internal Controls Over Cyber Security Risk

70

Top 15 of Source Countries (Last month)

	Source of Attack	Number of Attacks
	Russian Federation	2,450,063
	Germany	1,312,865
	Taiwan, Province of China	537,738
	United States	450,931
	Australia	379,910
	India	361,148
	Ukraine	256,047
	Hungary	237,778
	Brazil	220,515
	China	197,166
	Italy	194,981
	France	184,075
	Argentina	183,093
	Japan	151,861
	Venezuela, Bolivarian Republic of	127,862

Source: A. Renda, Cybersecurity and Internet Governance
Centre for European Policy Studies

- Human error or carelessness one of the biggest risks;
- Cyber linked to social media: 30% security incident results from social networking (NACD report);
- Less than 1/3 (Carnegie Mellon) of boards addressing RM in relation to IT operations or computer and information security;
- “Most policies currently in place,” “are too weak to reasonably ensure that systems are not breached.” (NACD report);
- Not enterprise wide, integrated, strategic, cultural;
- Due diligence, cyber security frameworks and standards;

- See social media policy database:
<http://socialmediagovernance.com/policies/>
- Social media training and attacking / crisis simulation;
- Advanced social media analytics monitoring;
- Secure the data not the device (BYOD): permitted/ supported; content applications; acceptable use; Mobile Device Management, MAM, security; App development; passwords; monitoring; storage; ownership of apps and data; example policies and best practices; device payment / stipend; policy enforcement;

Internal Controls Over Cyber Security Risk

73

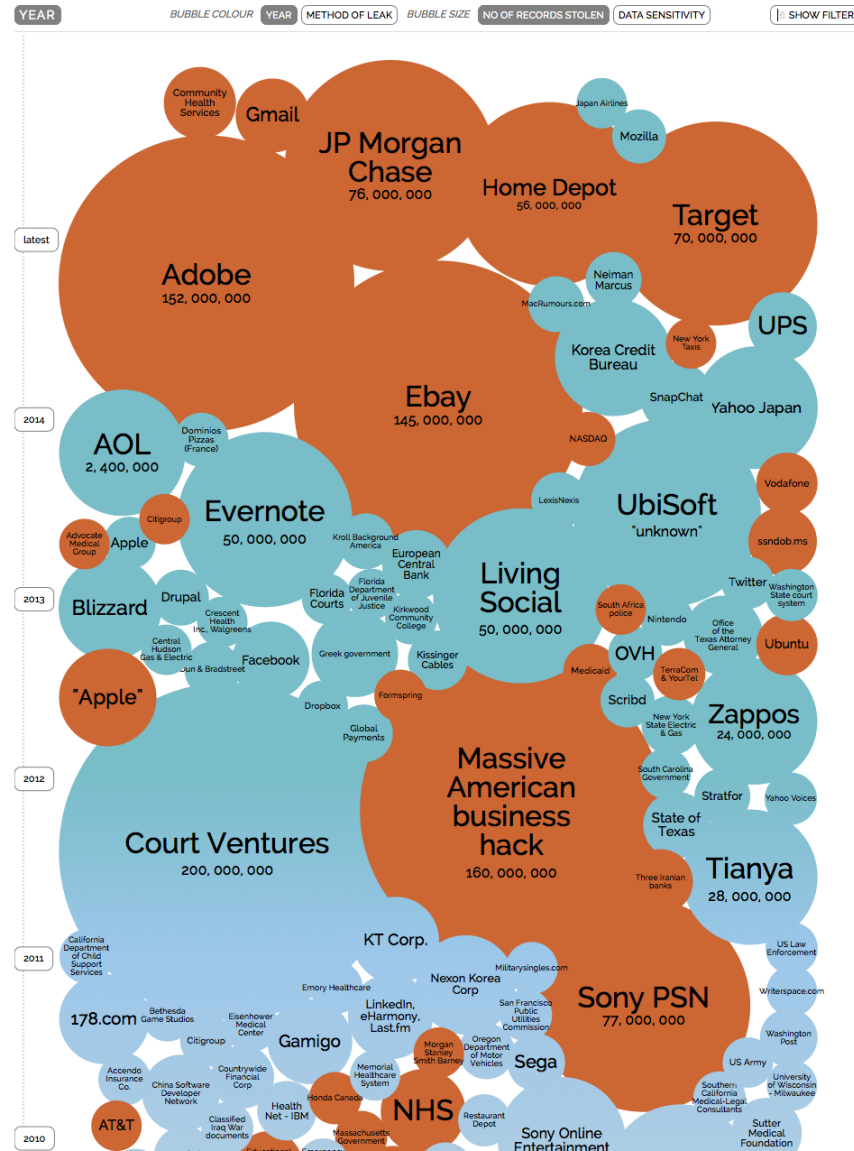


Internal Controls Over Cyber Security Risk

74

World's Biggest Data Breaches

Selected losses greater than 30,000 records



This is what strong cyber risk management looks like:

- **Organization and resources:** framework; authorities; specialists; 24/7; background security checks; training/awareness to new and existing employees;
- **Cyber risk and control assessment:** people, process, data, technology; outsourcing; IT service providers; scans and testing for client, server, network infrastructure for gaps; regular penetration testing; testing with 3P cyber mitigation services; cyber attack (including DDoS) and recovery simulation exercises; Internet outage risk;

Source: OSFI, NIST, SANS Institute, ISO frameworks;

- **Situational awareness:** Enterprise-wide knowledge of users, devices, applications, soft/hard, network maps; normalizing, aggregation and correlation of security event information; analysis of events to identify potential attacks; expert analysis follow-up; tracking & monitoring of incidents outside company; industry research;
- **Threat and vulnerability risk management:** Data Loss Detect/Prevent: Cyber Incident Detection & Mitigation: Software Security: Network Infrastructure: Standard Security Configuration and Management: Network Access Controls and Management: Third Party Management: Customers and Clients: **controls all enterprise-wide, including reputation / behaviour based;**

- **Cyber security incident management:** rapid response and mitigation; authority; documented procedures; protocols; escalation taxonomy; pre-scripted communication; recovery; systems integrity; post incident review; controls upgraded; forensic investigation; closure;
- **Cyber security governance:** Policy and strategy: enterprise wide cyber security policy and strategy; Second line of defence (RM): Third line of defence (CAE, independent control group and challenge, resources and expertise, testing of controls): Senior management and board oversight (funding, implementation, assurance): External benchmarking;

Resources for Directors, Regulatory Guidance ⁷⁸

- “You have to own this problem as a leader”: Adm. Michael Rogers, Director of National Security Agency;
- “Big Delta”: legislation may be coming;
- Lead by example: Yahoo’s CEO’s smart phone did not have a password;
- As a Director, you do not need to be an expert, but you should be technology literate and informed;
- Information, documentation and questions are your influence touchpoints and oversight;
- See technology as an enterprise risk and strategic and business issue, not a narrow IT issue;



- Watch out for fuzzy reports, recent expertise, and cottage vendors;
- Brief one of these excellent reports: Nat Inst Stds Tech [Framework for Improving Critical Infrastructure Cybersecurity](#); [SANS Institute Critical Security Controls](#), [ISO/IEC 27032](#); NACD Cyber-Risk Oversight;
- Glossary and acronyms: Brief these to understand;
- Your job is to understand, identify and oversee, not to manage: Budget, Talent, Resources, Reporting, Assurance, Disclosure: watch “technical devolution”;
- The risk: Cyber failure: Where was the Board?

- Informed, best-practice and precise questions;
- Agree on a platform or framework (see my earlier links) and direct management to have an action plan and target date for full implementation;
- Management may be adverse to the spend and controls;
- Does management show you IT, and broader enterprise risk management, how identified, controlled & assured?;
- Are you satisfied with the IT, risk management and internal audit bench strength?: these are your eyes and ears: You may need to direct changes and resources;

- Are your crown jewels/valuable assets protected, from outside, and once inside, also protected?; (Think like a thief.);
- Do you meet separately with risk, compliance, audit to assure cyber security risk?;
- Do you have scenario testing and mock exercises over digital media and cyber breaches?;
- Do you have the authority to retain a third party? Do you exercise this authority if or when you need to?
- Does your board have or need IT, risk expertise?

10. Questions and Answers

82



CHALLENGE
CREATE
EVOLVE
TH
QUESTION
INNOVATE
TRANSF
PROVO
RESEARCH
STUDY
DECONSTRUCT

Thank you!

83

THANK YOU!

Q AND A

Professor Richard Leblanc
Faculty of Liberal Arts & Professional Studies
York University

tel: (416) 736-2100 x 33744

Email: rleblanc@yorku.ca



Twitter: <http://twitter.com/DrRLeblanc>

LinkedIn Group:  Boards & Advisors

Linked  [®]

Dr. Richard Leblanc is an award-winning teacher and researcher, consultant, lawyer and specialist on corporate governance and accountability. He is a former recipient of Canada's Top 40 Under 40™ award, received a teaching award as one of the top five university teachers in Ontario, and was named to *Canadian Who's Who*.

Professor Leblanc's research expertise is in corporate governance, specifically in the effectiveness of boards of directors. He founded the discussion group on LinkedIn, Boards and Advisors, which is one of the largest and most active corporate governance groups on LinkedIn (> 25,000 members). He will provide hands on examples of how to maneuver the challenges directors could face based on his extensive service as an external advisor to boards of directors.