

Mitigating cyber-reputation risk

By [Andrea Bonime-Blanc](#) on Mar 21, 2016

Companies that suffer a cyber-attack can find the biggest damage is to their reputation. Protecting themselves from this ‘risk of risk’ should be top priority for every organisation

The Economist Intelligence Unit published a prescient report in 2007: “Reputation: The Risk of Risks”, which was if not the first, then certainly the most prominent and thoughtful treatment of the issue of reputation risk at that time. Today, almost 10 years later, we find ourselves in the unenviable position of not only living through the age of reputation risk but also through the age of cyber-risk.



Sony Pictures HQ in Los Angeles. Its cyber hack cost it dear

These two risks – reputation and cyber – are often strategically important risks to any given organisation – whether a corporation, government agency, non-profit group or university. And the combination of the two – cyber-reputation risk – is a new and powerful strategic issue.

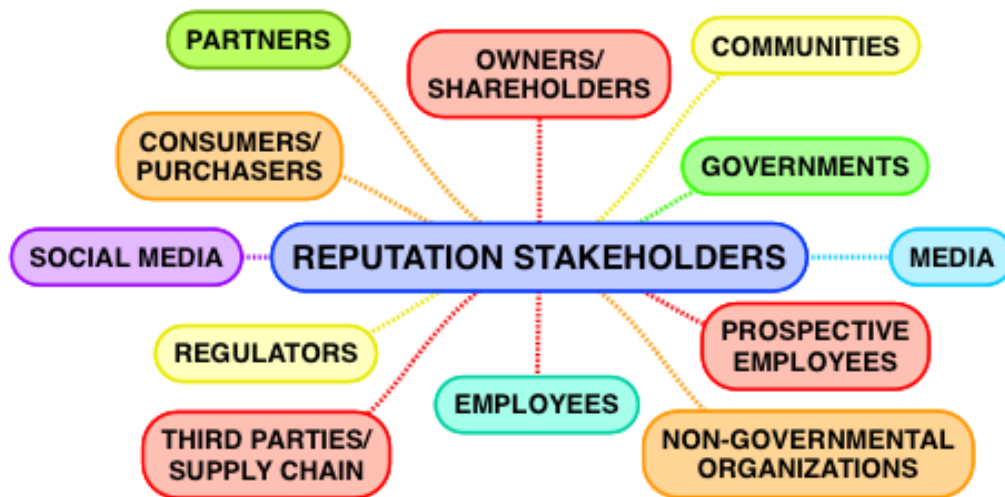
In this article I will make this case and issue a call to arms to all leaders – whether corporate executives, boards of directors, heads of non-profits or of government agencies. Leaders need to be sensitised to the fact that in addition to reputation risk and cyber-risk individually, the combination of the two is today's strategic "risk of risks", turbocharged.

What is reputation risk and why do stakeholders matter?

Reputation risk as it relates to organisations is unlike almost any other risk – it is pervasive and cuts across many other kinds of risk. In "[The Reputation Risk Handbook](#)", I offer the following definition:

"Reputation risk is an amplifier risk that layers on or attaches to other risks – especially ESG risks – adding negative or positive implications to the materiality, duration or expansion of the other risks on the affected organisation, person, product or service."

The role of stakeholders in the reputation risk equation is critical: knowing who your stakeholders are, understanding their expectations of your organisation and how to prioritise them has everything to do with effective reputation risk management. Below is a depiction of the most common types of reputation risk stakeholders.

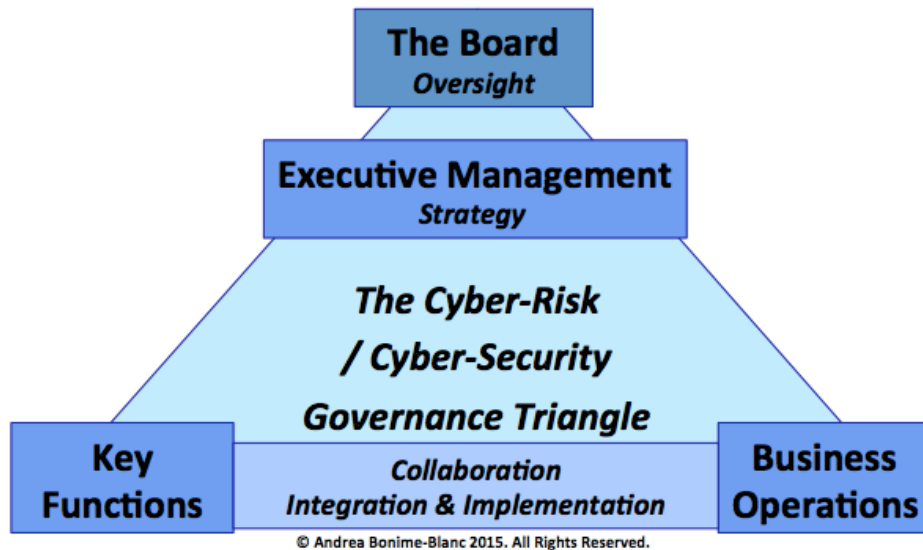


GEC Risk Advisory LLC 2016.All Rights Reserved

What is cyber risk? What is cyber-risk governance?

Cyber-risk can be defined in a variety of ways, but the simplest and most to-the-point I have seen – which interestingly includes a reference to reputation – is the following from the [Institute of Risk Management](#): “Cyber risk’ means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.”

In turn, cyber-risk governance, as visually depicted in the graphic below, focuses squarely on the top of the organisational house, asking whether the proper approach to triangulating this risk exists. Drawing from the Conference Board Report, "[Emerging Practices in Cyber-Risk Governance](#)", we can offer the following definition: “Cyber-risk governance is a framework adopted within an organisation to deal with the new and evolving risks relating to cyber space both within the organisation and as the organisation interfaces with the outside world. In this framework, the critical actors are the board, the C-suite or executive team, and frontline top management in charge of executing cyber-risk management.”



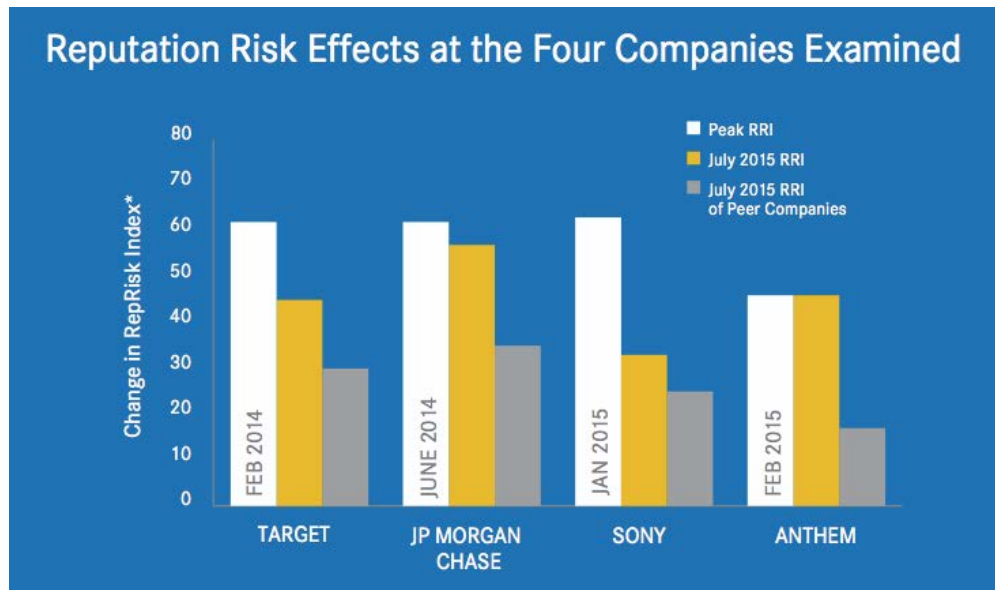
One of the 10 key take-aways of the report is the following: “Cyber risk should be considered at the top of many companies’ risk prioritisation, whether they have suffered from a major or material cyber attack (yet) or not. When a company doesn’t have the right overall cyber-risk governance programme in place, the potential reputation risk consequences can amplify the company’s exposure to both tangible and further intangible consequences that may be difficult, costly, and lengthy to repair.”

Why is cyber-reputation risk a turbocharged strategic ‘risk of risks’?

There is a growing body of evidence that executives and board members are beginning to accept that reputation risk and cyber-risk are two of the top strategic risks of our time; that these risks separately or, even worse, together can have a strategically significant impact on the wellbeing, longevity and profitability of an organisation and its stakeholders.

In October 2015, Marsh Risk Consulting released [an important new survey of global corporate executives](#) showing that the two top global risks concerning C-suites and risk executives today were cyber and reputation risk, but especially the reputation risk associated with cyber breaches: “79% of respondents selected reputational damage from a sensitive data breach as the most likely and high-impact risk,” the survey said.

The following chart provides a snapshot of the reputation risk impact on four companies that suffered major public cyber-security attacks over the past few years.



RepRisk AG 2016

The RepRisk Index reflects big data analytics gathered daily from global media sources with respect to each company and its risk exposure, analysed and prioritised along a 100-point system where exposure above 50 generally represents a high or very high reputation risk exposure, according to a strict methodology developed by and proprietary to RepRisk.

It can be gleaned from this data that each company retained significantly higher reputation risk consequences over time after its cyber-event compared with its peer group of companies (the grey bar in this chart).

Tackling strategic cyber-reputation risk: guidelines

While this article is not intended to rattle cages or scare directors and executives, it is a call to arms on both reputation risk and cyber-risk governance, two of today's most important strategic risks. And strategic risk is first and foremost the responsibility of boards of directors/trustees and chief executive officers, presidents, heads of agencies, and their C-suites.

THE CONFERENCE BOARD

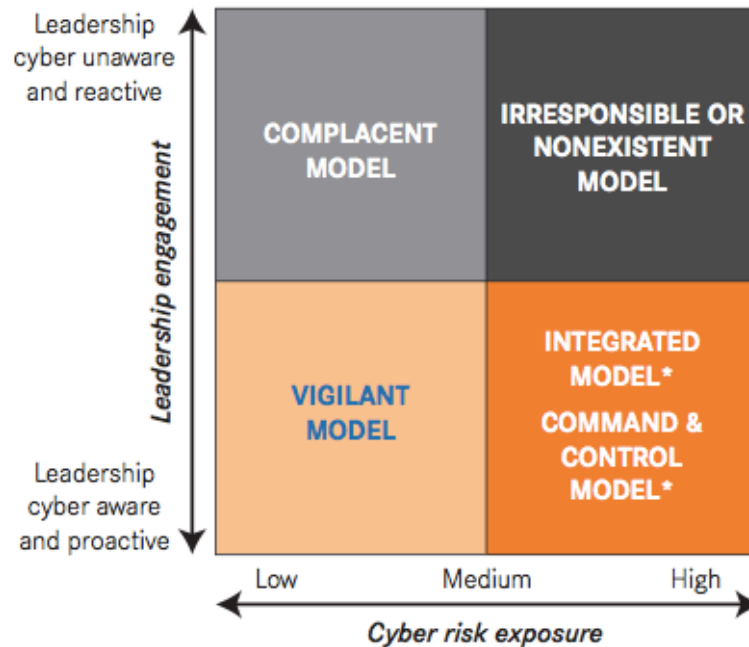
EMERGING PRACTICES IN CYBER-RISK GOVERNANCE

10 KEY TAKE-AWAYS

1. Effective cyber-risk governance requires a triangular framework including the board, the C-suite and key functional executives
2. Cyber-risk is a strategic risk closely related to another strategic risk: reputation risk
3. Effective cyber-risk governance requires knowledge of who your cyber-risk actors and stakeholders are
4. Successful cyber-risk governance requires a deep understanding of the organisation's "crown jewels" i.e. what are the highest value cyber-targets in the organisation – intellectual property, personal information, financial account, etc?
5. Effective cyber-risk governance may require engaging in a cyber-risk public-private partnership. Depending on the industry or sector involved, a private sector/government agency partnership may be necessary or useful to combat cyber-attacks (for example, the banking industry or critical infrastructure)
6. Effective cyber-risk governance requires a cross-disciplinary approach
7. Effective cyber-risk governance requires a cross-segmental/divisional approach – where all divisions or business units collaborate on creating an equivalent cyber-defence strategy
8. Cyber-risk should be an essential part of an organisation's resilience approach – meaning that it should be incorporated in any crisis management business continuity and disaster recovery planning system
9. There are five types of cyber-risk governance: only three are effective (see typology in the chart below where only the bottom three types of cyber-risk governance are effective)
10. Effective cyber-risk governance can yield business opportunities – organisations that are able to manage their cyber-risk successfully may find embedded opportunities for cost savings, process improvement and even new revenue streams

Figure 15

A typology of cyber risk governance readiness and resilience



* In this category the integrated model would be more likely for decentralized companies and the command and control model for more centralized companies.

Source: GEC Risk Advisory LLC

GEC Risk Advisory LLC 2016.All Rights Reserved

Each type of cyber-risk governance approach depicted above depends on two criteria – whether leadership is effectively addressing the issue by providing the right resources, budget and care required on this issue and whether the organisation has low/medium/high cyber-risk exposure depending on its footprint, focus, sector, etc. The Irresponsible Model is one in which leadership in a medium to high risk setting is not properly addressing the issue. The Complacent Model is one in which leadership in a lower risk environment is not properly addressing the issue. The Vigilant Model is one in which responsible leadership in a lower risk environment is properly addressing the issue. The Integrated Model is one in which responsible leadership in a higher risk environment with a decentralised business model is properly addressing the issue. Finally, the Command & Control Model is one in

which responsible leadership in a higher risk environment in a centralised business model is properly addressing the issue.



Know what your crown jewels are – and how to protect them

Finally, and more focused on the combined threat of cyber-reputation risk, here are additional guidelines that leaders (boards and executives) of any type of organisation (corporate, NGO, governmental or educational) should consider to understand and tackle the combined threats and effects of cyber-reputation risk – that new turbocharged risk of risks of our time.

- **Board risk expertise.** Have at least one independent member of the board with deep and broad risk expertise and if you're deep into technology, maybe even a technology executive
- **ESG risk focus.** Don't just think about financial risks - scan the horizon of strategic non-financial risk regularly and understand what it means to your business/sector
- **CEO risk performance.** Require your CEO/leader to spend time on non-financial risk and integrating this properly into the organisation's strategy. Measure the effect of these steps

- **Cyber-risk talent.** Have access to the right technology gurus for your organisation:

Start with the right chief technology officer, chief information security officer or chief information officer

Make sure your C-suite and board also have technology savvy player

Get the right outside experts to help you, regularly

Benchmark what others are doing both within and outside of your sector

- **Reputation risk expertise.** Reputation risk is not public relations – it's risk management that requires the participation of public relations and a number of other key players and experts.
- **Consider appointing a chief risk and reputation officer.** See our Ethical Corporation Magazine article from April 2013.
- **Cyber-reputation risk: a team resilience sport.** Cyber-reputation risk management is a team sport – not an individual one. Gather the key decision-makers and experts together and do it regularly before, during and after a cyber-reputation risk incident. This is the only way that your organisation can hope to build the long-term resilience muscle it will need to manage this turbocharged strategic risk which is going nowhere any time soon.

Dr Andrea Bonime-Blanc is chief executive of GEC Risk Advisory, a global strategic governance, risk & reputation consultancy. She is a frequent keynote speaker worldwide, board chair and chair emeritus, a widely published author including The Reputation Risk Handbook (Do Sustainability 2014 - <http://bit.ly/1284TMR>) and Emerging Practices in Cyber-Risk Governance (The Conference Board 2015 - <http://bit.ly/1NB2tJh>). She is a 2015 & 2014 Ethisphere 100 Most Influential People in Business Ethics and tweets @GlobalEthicist.