# MSCI ESG THOUGHT LEADERS COUNCIL

FROM MSCI ESG RESEARCH INC.

PRIVACY AND DATA SECURITY | DECEMBER 2014

## INTRODUCTION TO THE MSCI ESG THOUGHT LEADER COUNCIL

The goal of the MSCI ESG Research Thought Leaders Council is to maintain our leading edge in research methodology by regularly seeking feedback and opinions from external experts in key industries and relevant ESG issue areas. The MSCI ESG Research Thought Leaders Council consists of a series of about four panels annually, with three to seven members on each panel. We aim to assemble international experts with recognized leadership and expertise on the topic area related to the panel.

The fourth council was held on December 6, 2014 on Privacy and Data Security. Panel members were asked to review MSCI ESG Research's proprietary IVA Rating methodology, as well as specific industry and company reports before participating in the official panel call with MSCI ESG Research analysts.

## KEY TAKEAWAYS

- The panel recommended that we use more financial data, for example financial costs incurred in a data breach and expenditure in data security systems and programs, to better highlight the materiality of issues related to privacy and data security.
- Participants identified several industries, which they felt were more exposed to the risk of data theft and financial security breaches, including industries in the Financial Services sector and Telecommunication. The healthcare sector, and in particular hospitals, were also mentioned as increasingly vulnerable to risks of data breaches nowadays, with a lack of expertise in safeguarding electronic medical records and patients' personal information and surge in data breach in this sector.
- Participants felt that MSCI ESG Research risk management assessment was too heavily focused on policies, and not enough on the actual performance of companies. The panel indicated that the analysis would benefit from including more performance indicators beyond controversies, which provide an incomplete picture of a company's performance.
- Participants remarked that the provisions of the upcoming EU Privacy Law are currently unclear and at this point it is difficult to say whether it will be an efficient tool to mitigate risks related to privacy and data security. However companies may have to adopt a tailored data security model for their EU operations.
- The panel recognized that the trend of increasing data breaches and the raising awareness of privacy and data security matters represent significant business opportunities, in particular for insurers that offer cyber security insurance policies and companies that provide information security services. However, this is still a nascent field.

## COUNCIL MEMBERS

**Avner Levin**
Ryerson University

**Ramin Safai**
Jefferies

**Claudia Diaz**
KU Leuven

## KEY DISCUSSION POINTS

1. FINANCIAL METRICS

   Overall, the panel indicated that adding more financially-relevant data would be useful for investors in order to better inform investment decisions. Additional indicators that were suggested include financial data in the aftermath of serious data breaches (e.g. remediation costs, revenue losses, litigation costs, fall in share price), and the proportion of revenue spent by companies on data security. In particular, participants recommended that the MSCI ESG research include more information and assessment of the impact of major data breaches (e.g. financial impact, follow-up remediation measures).

2. IDENTIFYING RISKS

   The panel expressed their views that in analyzing companies' exposure to risk of breaches, countries that have stringent privacy regulations should be considered of lower risk than those with no regulatory oversight. When analyzing exposure to risks related to privacy and data security (e.g. propensity to data breaches, increasing compliance needs), participants advised us to look at the nature of the data handled, in order to identify its sensitivity and assess the potential for abuse, however recognized the challenges of predicting and quantifying such potential.

   To identify industries most vulnerable to risks of data breaches, adding differentiation between the types and intents of threats (organized crime, internal threats, government surveillance) would yield a more granular assessment of the potential "attack vectors". Telecommunication firms were seen as more prone to risks related to government surveillance, whereas financials companies were deemed to be more prone to threats linked to organized crime. Within financials, participants differentiated between business to business (B2B) and business to customer (B2C) models based on their exposure to risks of data breaches, with higher need to protect privacy and data security in the B2C sector, where the traffic volume is extremely high and the transactions are small. One sector that participants felt was insufficiently protected is the healthcare sector, which handle substantial quantities of sensitive personal data, yet invest less money to protect this data.

3. RISK MANAGEMENT

   Overall, participants felt that our risk management assessment was heavily focused on policies, and should be more dedicated to the assessment of actual performance of companies. Companies have privacy policies in place to deflect potential liabilities but the key aspect to look at is whether they are actually implementing these policies. Involvement in controversies was judged to be a good, yet insufficient indicator, and the panel recommended more performance indicators.

   To assess good practices, indicators include who has access to the data, whether companies are explicit about how user data is used and shared with third parties, and if data is encrypted. One best practice identified by the panel was to limit the data collection as much as possible. An example was cited one of a company that provides communication services without collecting any kind of information about its customers.

While the use of third parties is fairly common, the participants' view was that third parties should not be provided with highly sensitive information. In-house data protection procedures and systems were assessed as the most secure ones, but require companies to have solid expertise. A key approach to minimizing third party risks is to monitor third parties closely, with key features of solid third party oversight including: requiring third parties to have cyber security insurance policies, conducting auditing of these third parties, and running background checks of third parties' employees. Participants pointed out that the best way to protect data was not to entrust it to the internet and the cloud completely.

4. **DATA SECURITY PROCEDURES**

To assess the strength of data security procedures, participants recommended that we look at companies' security architecture and the technologies deployed. In particular, companies that limit employee access to sensitive data and limit data collection are the ones with less risks of incurring data breaches. Limiting employee access to personal data was also seen as a best practice.

Certification to the ISO 27001 standard should be seen as a minimum to assess the strength of data security systems, and a more aggressive effort is the adoption of the SSAE16 soc2 standard, which the participants considered as a more up to date and higher auditing standard. With the ISO standard alone, some areas are missing, and recent hacking attempts (e.g., Target, Sony, Kookmin) have brought to light the depth of vulnerabilities that companies face.

5. **REGULATORY FRAMEWORKS**

All participants agreed that the upcoming EU Privacy Law is currently unclear and that at this point it is difficult to say whether the EU regulation will be an efficient tool to mitigate privacy and data security related risks. Their opinion was that big companies will likely be more affected by the regulation than smaller ones. The panel recognized the upcoming EU regulation as a source of concern for companies, as it may force them to adopt dual business models to get compliant, and that generally the approach seems to be "wait and see".

6. **RISKS VS. OPPORTUNITIES**

The panel recognized that privacy and data security matters represent significant opportunities, in particular for Financial Services companies (especially insurers) and Security Services firms. Smaller companies (mostly start-ups) are now providing services of communication where they cannot see the content of data exchanged, thus protecting themselves from breaches and regulatory scrutiny over the data collection and usage practices. However, this is still a nascent field. One trend identified by the panel was the purchasing of insurance against data breach.

7. **AMAZON VS. FACEBOOK**

Participants were sent the MSCI ESG Research IVA Rating profiles of Facebook and Amazon. They felt that the weight of the Key Issue Privacy & Data Security should be higher for Facebook, and also higher relative to Amazon, as they assessed Facebook as much more vulnerable to risks of data breaches. In addition, the view was that Amazon, because it physically holds and delivers goods, should be assessed on more environmental Key Issues than Facebook.

## ABOUT MSCI ESG RESEARCH PRODUCTS AND SERVICES

MSCI's ESG products and services are provided by MSCI ESG Research Inc. and are designed to provide in-depth research, ratings and analysis of environmental, social and governance-related business practices to companies worldwide. ESG ratings, data and analysis from MSCI ESG Research are also used in the construction of the MSCI ESG Indexes. MSCI ESG Research is produced by MSCI's indirect wholly-owned subsidiary MSCI ESG Research Inc., a Registered Investment Adviser under the Investment Advisers Act of 1940.

## ABOUT MSCI

For more than 40 years, MSCI's research-based indexes and analytics have helped the world's leading investors build and manage better portfolios. Clients rely on our offerings for deeper insights into the drivers of performance and risk in their portfolios, broad asset class coverage and innovative research. Our line of products and services includes indexes, analytical models, data, real estate benchmarks and ESG research. MSCI serves 98 of the top 100 largest money managers, according to the most recent P&I ranking. For more information, visit us at www.msci.com.