FERMA
Federation of European Risk Management Associations

CONFERENCE ON CYBER ISSUES

OFFICIAL EVENT OF THE SLOVAK PRESIDENCY OF THE COUNCIL OF THE EU

Measuring Digital security and risk management in an industrial group

Philippe COTELLE

Head of Insurance Risk Management

AIRBUS DEFENCE & SPACE

AIRBUS DEFENCE & SPACE

CYBER SECURITY RESEARCH AND DEVELOPMENT –CPPP ON CYBER AND H2020

Airbus is usually a company which is taken as example of the success of Europe. I am sure that you have heard already the expression ***building the Airbus of X*** when referring to an ambitious European construction.

The role of Risk Manager is sometimes unknown or unclear. Its main task is to identify the risks, assess them and propose solutions to the top management to mitigate and transfer them.

Risk Manager of Airbus Defence and Space, I am also vice President of the Cyber Commission of AMRAE the French Risk Management Association. Because cyber risk typically ignores the frontiers, it is of utmost importance to develop an international view and this is the reason why we are convinced that Europe shall play an important role to address cyber and more generally digital issues.

This is the reason why, as risk Manager, I support Ferma through my membership to Amrae. FERMA is the European federation of risk management with 22 national member associations representing almost 5000 risk and insurance managers in Europe. FERMA current activities includes European Affairs (for a better recognition of the profession), Events (to increase our network), Education (with our European certification rimap, to update and develop the skills of risk professionals) and Research (with specific publication and reports). Ferma has been extremely active on the field of cyber, identified as one of the critical risk that we need to address, with many initiatives illustrating the influence and the visibility of this federation.

In most corporations, digital security has long been seen as the responsibility of IT experts only. Their main tasks was to identify threats and provide technical solutions to respond to incidents or attacks when they occurred.

Today, in an era where companies rank digital risk as one of the most significant threats they face, the approach to corporate digital security has changed radically. It calls for global and regular assessment and upgrades. It requires a highly coordinated approach across all departments, under the supervision of the risk manager.

While there is no commonly agreed methodology or standard to assess corporate digital risk and security, Airbus has recently launched an initiative to progress in this field with a methodology developed and tested internally since 2015, named SPICE (*Scenario Planning for Identification of Cyber Exposure).*

SPICE: feedback on Airbus experience in digital risk quantification

The quantification or more precisely the valuation of a firm entails to quantify a combination of tangible assets (like buildings, factories, etc) and, with a consistent increasing share, intangible assets – such as its reputation, intellectual properties, datas.

Assessing the risks related to intangible assets which are specifically vulnerable to digital risks turns out to be complex. How many companies have actually performed a complete business impact analysis

related to their digital risks? From my discussion with my counterparts and with business associations, I would say that the answer is: very few. Why? I see two main obstacles.

Firstly, the governance of digital risk *within the companies is most often unadapted to the rapid progress of digitalization*. The risk manager has still to find its way in credibility when discussing with the Chief Information Officer who used to address those risks so far on its own. But not only. The operationals have to understand and appreciate the legitimacy of the risk managers to address this and not to refer purely to IT. Finally security officer have to be comfortable that this process is not just listing the vulnerabilities of the company and therefore provide a very useful map for anybody planning to attack this company. IT people may accept as well this process not as an audit which would highlight the flows of the system they have built but more as a support for justifying future investment. Board members have to be comfortable with the fact that an internal analysis may put into light a significant financial exposure which if not properly communicated may create some anxiety on the market. And such document would trigger mandatory response at Board level, in their mandate to secure the development of the company. So this is going to be potentially a quite sensitive and controversial document!

Secondly, ***the quantification of loss scenarios is in itself very challenging***. Talk Talk firm suffered a major cyber attack on Oct 2015. Its share price dropped from 317GBP in Oct 09th to 225GBP in Oct 26th, a fall of 30%. One year later, its share price is 201 GBP, highlighting that a major attack has long lasting impacts. This drop reflects the variety of negative financial impacts affecting the company, including loss of future market, loss of income even after restoration of the system, loss of internal efficiency raised by a tight up of security procedure, legal prosecution or loss of intellectual property. These long-tail impacts are as effective as difficult to assess. And they are complemented by other costs like reparation cost, restoration of data, and notification costs. You can appreciate from this list how a cyber incident may rapidly result in very disruptive losses which require immediate strategic action from the top corporate management. Such action obviously needs to be anticipated in a comprehensive digital risk management strategy.

Each company needs to circumvent these obstacles in order to respond proactively to the rising digital theat. It is all the more crucial in highly technological and sensitive industry such as that of Airbus. This is why we have worked hard to develop a method to assess the financial exposure of the firm to cyber risk, which we have called **SPICE.** Spice allows to affect a financial value to the exposure to cyber risk in case of catastrophic scenario affecting the company. Especially on cyber risk, catastrophic scenarios are often related to interaction between different players, of different organisation and you need to combine, confront them with the support of cyber experts that can evaluate the feasibility/plausibility/attractivity of those scenarios vs the efforts for the attackers to perform them. This methodology gathers informations coming from business owners around a scenario which has been built with the support of digital security experts, and quantifies the financial impact in case of failure or attack, by function and over time. This analysis which can repeated on an annual or biannual basis allows the risk manager to identify and present in a clear way to top management the exposure faced by the company and in collaboration with cyber security, propose mitigation actions tailored to those risks. This is then the basis for a sound discussion with insurance to obtain an adapted coverage.

This internal program was a major step for us, but is also made us aware of the many challenges we still have to face and the need to reach out to external public and private partners to progress in the quantification and management of our digital risk.

Conclusion

As a conclusion, FERMA, supported by its national associations, promotes the **concept of cyber risk governance embedded in the Enterprise Risk Management policy, and in particular provide the Board with a clear view on the extent of exposure and threats.** but the framework is **still a work in progress** with:

- Need to define the elements of an efficient cyber risk governance across functions (from IT to Board)
- Ensure the presence of a cross-function position to manage digital risks. Mandate of the risk manager from the Board to take responsibility for this function.
- Ensure presence of collective exercise internally to determine catastrophic scenarios which would significantlt affect the ability of the companies
- Agreeing on norms/process which would be used to quantify the related financial exposure.

The ability of organisations to **quantify and manage** their digital risks is always more crucial to their development. In a business environment, it is more and more regarded as a competitive advantage, and we anticipate that it will become an important element in the valuation of corporations.

Above all, It is essential to enhance resilience to cyber incidents which can endanger the very survival of corporations and our economies. Therefore the EU should fund **not only IT security projects but also projects treating the governance and quantification** aspect of digital risks inside organisations