Q&A

WEBINAR "AT THE JUNCTION OF CORPORATE GOVERNANCE AND CYBERSECURITY"

-

QUESTIONS RAISED BY PARTICIPANTS

1. ***We regularly see businesses failing to include their key outsourced IT service providers in regular cyber risk disaster scenario planning, how businesses can effectively address this challenge?***
2. ***Should there not be a 4th line of defense - external cooperation/ assistance?***

Philippe:

The more we go into digitalisation, we more we need to include this external environment (providers, suppliers, partners…) within the overall exposure of the company. Therefore, a cyber risk governance group is necessary because the operational business people are the most effectively connected with these external environments. They can best imagine the various scenario where the company can be harmed in the most efficient and credible way.

Julie:

A company's 'supply chain' or 'ecosystem' is a critical dimension of its business context and thus key to understanding cyber risk and mitigation strategies. As companies identify critical business processes and develop cyber risk disaster scenarios and mitigations, key partners involved in delivering that business process should be included. Importantly, we all know that security is only as strong as the weakest link, so it is not just first line partners but also their partners and subcontractors to be considered. Companies can take a layered approach to ensuring that key providers are included by setting up guardrails to guide business leaders in proactive vetting and oversight of key providers as well as triggers in processes such as procurement, contracting, payment, etc. to further identify supporting partners such as IT infrastructure and cloud services providers. A Cyber Risk Governance Group that includes representatives from lines of business, HR, finance, etc. helps ensure the collaboration necessary to evaluate and manage cyber risk holistically in business context.

To be addressed – the question about a 4th line of defense with authorities, agencies, insurance as cooperation and assistance 3rd parties?

A 4th line of defense is an interesting concept to consider! Having an understanding of and relationships with relevant authorities, agencies, insurance providers, industry associations, standards bodies and others for external cooperation and assistance enables a business to operate smoothly efficiently. From a cyber risk perspective, external collaboration, appropriate trust and sharing of data related to threats and vulnerabilities, attack scenarios, mitigation effectiveness, etc., helps to evolve cyber security tools and capabilities and inform holistic mitigation strategies. Just as a cross-functional Cyber Risk Governance Group supports a company in managing its cyber risk, such cross-functional external collaboration holds the potential for supporting global prosperity.

3. What is the maturity of the cyber risk assessment regarding the accurate estimation of the business impact of a cyber failure?

Julie:

One thing to consider adding would be to reiterate the two dimensions of a company's digital evolution – the use of technology (their own and procured from partners) within in the company to do their day-to-day business and the use of technology (again, their own and procured from partners) to deliver their products and services – and the importance of regularly updating risk assessments from both perspectives. While both must consider inside and outside threats and vulnerabilities, mitigation of the former tends to focus more on capabilities for business continuity while the later tends to include data loss, legal/regulatory/contractual fines/penalties, loss of business, reputation, market/product failures, etc…

4. Can you provide some guidance on how you quantified the financial impact of your cyber risk exposures?

Philippe:

Cyber risk is a new way for a business risk to happen. Therefore, the first step is to assess how a business risk could materialise through cyber means. Cyber risks must be assessed from a business point of view to translate the impacts in business figures. This exposure will also evolve overtime as the company uses more a more digital technologies and strategies. It must be updated regularly.

Ideally, a methodology should be put in place in priority for catastrophe level scenarios identified and agreed by the cyber risk governance group. It includes working collaboratively across the organisation to define what inputs are needed, such as the number of affected clients, business interruption duration, number of notifications, product recalls…etc. Finally, the exercise will lead to a calculation of the potential financial impact of the cyber disaster on the organisation.

The exposure should be defined for each scenario, relying on the company's business model and assessed all along the timeframe of the event.

Julie:

Quantification of cyber risk, especially financial quantification, can be challenging in part due to the complexity of the technical environments and threat landscape and due to many companies' evolving understanding of cyber as a business risk beyond IT. There is research in progress and some emerging models that are helpful. As these mature, some points to consider include the importance of cross-functional collaboration on both asset-based and outcome-based risk scenarios in order to surface as many dimensions of a cyber risk as you can. Also, it may be necessary to begin with more subjective values (High, Medium, Low) as you evolve to ranges (e.g.: What do we mean by Medium? – for some companies that will be $1-2 million, others it may be $75-100Million, etc.), then increase precision as you evaluate information in context of your business, such as vulnerability and loss data, technology lifecycle and controls maturity (your own and partners'), legal/regulatory fines assessed by regulators, etc.

5. ***What would be the specific expertise you think to be necessary for the components of the steering committee?***

***Julie**:*

Based on experience, there would be 2 key components.

One is to bring the people who have an expertise of their own, local risk management functions. For instance, dealing only with privacy matters, providing a precious expertise in privacy controls, privacy design consideration, regulations and data subject expectations. Deep expertise in whatever function is critical for the organisation should be represented in the steering committee.

The 2nd component is the level of influence within the organisation, not based on the title on their decision-making power and the trust that these persons have in the organisation. These profiles are trusted advisors, thinking strategically, maybe less self-interested that specific expert functions. People who can make decisions (senior management, director, executive director). Deep understanding of their business by being able to look across functions.

***Philippe**:*

It is interesting to compose the steering committee with some operational non-IT people who have a global view of the business, who can put themselves in the shoes of the attackers. Vast majority of attackers know their target business very well.

This will allow to identify the weakest points of the business, and not just from an IT perspective. Having also legal people will be helpful to identify the third-party losses (customer indemnification…etc) in addition to the first party losses.

On the security side, the committee will need people with a knowledge of the mindset of the attackers, in order to establish which attack scenario are making more sense from an IT perspective.

These two profiles (business and security) can come up with the most credible scenarios, about what could go wrong, what could happen. A deep IT expertise will come at a later stage.