Cybersecurity in the Current crisis

A new wake-up call for board members

September 15, 2020

ecoDa, in close cooperation with AIG, organised a webinar on «The Covid crisis and its cybersecurity implications: a new wake-up call for board members». The current environment makes it even more urgent to address the challenges of cybersecurity as cyber criminals around the world are capitalizing on this crisis to multiply their attacks. The crisis is transforming working methods in a way that is likely to be lasting, and means that businesses and board members must be all the more vigilant when it comes to cyber attacks.

The discussion, moderated by Prof.Dr. Michael Hilb, invited four distinguished leaders in cyber security governance to exchange on the main challenges for board members when dealing with cyber security.

Troels Ørting Jørgensen, *Chairman of the Advisory Board, Board Leadership Society,*
Klara Jordan*, Executive Director, EU and Africa, Global Cyber Alliance,*
Carolyn Dittmeier*, President of the Board of Statutory Auditors of Assicurazioni Generali SpA, Independent Director Alpha Bank*
Sebastian Hess*, Cyber Risk Advisor, EMEA AIG.*

The webinar echoed the principles and practical guidance of the pan **Europe Guidance on Cyber Risk Oversight** for corporate boards of directors in Europe issued earlier this year by ecoDa, AIG and The Internet Security Alliance (ISA).

As a general principle, all speakers agreed that board members should no longer fear about the unknown but treat cybersecurity as a strategic issue, in an enterprise risk management approach. In view of the growing importance of intangible assets regardless of the sector, no company should feel safe from cybersecurity attacks. Each company have to embed security into its DNA. The Covid-19 crisis has accelerated the digitalisation path, revealing that cyber has no territory, it can reach all the domains. This is why it has to be considered as an enterprise component.

Far from being a subject that should be dealt with only by IT departments, boards must be aware of the proactive role they must play in this matter. Board members should provide oversight over management's comprehensive evaluation of cyber risk management and ensure an enterprise risk-based assessment of the cyber area to determine what are their digital assets and how to prioritize them based on a cost/benefit analysis. It is important for them to identify what are the key information the company wants to secure, to understand the threat landscape and to assess control mechanisms that are already in place to protect the company. Regardless of the company size, board members are there to set the tone, to define a plan and to set the risk appetite with scenario planning, which cannot be done by

Chief Information Security Officers. Board members should look at the basics, understanding that everything could be risk-driven and a risk factor.

Specifically for large companies, it is also recommended to have a strong audit committee capable of formulating an agenda, selecting the right metrics to monitor and bring to the Board in order to quantify the risks and analyse potential incidents.

Companies must define a cybersecurity strategy that evaluates their digital assets in relation to strategic objectives and encompasses the entire value chain. Outsourcing to the cheapest suppliers might not always be the right solution if businesses want to ensure that their data are secured properly. Board needs to be agile enough to ensure suppliers have the right practical tools.

Companies can draw inspiration from the military who played a pioneering role in this area. Board members should stay informed on geopolitical developments that are often clear indicators of where the attacks could come from. Monitoring how the competitors look at those topics and how the regulatory landscape evolves, is also crucial.

The panelists could not agree more on the need to get trained, should it be through cyber risks simulators or cybersecurity experts. The closer board members get trained and exercised, the more beneficial it is for the company. Board members have to empower themselves if they want to raise the right questions and to hold the management responsible to report in a comprehensive and understandable way.

Overall, cyber resilience, defined as the ability to prepare for, prevent to the extent possible, respond and recover from a cyber threat, could be enhanced by a strong expertise at board level on cybersecurity taking into account people as well as technical factors and by embedding cyber in the long-term strategy plan of the company. Board members should not overdo, they have just to make it happen and address cybersecurity issues seriously.

To learn more on how to build businesses cyber resilience capabilities and mitigate the risks of cyber attacks, a recording of the discussion is available on ecoDa's Youtube channel.

****

Contacts:

Béatrice Richez-Baum, Director General, ecoDa: contact@ecoda.org, Tel: +3222315811

Manon Roehrig, Junior Policy Adviser, policy@ecoda.org