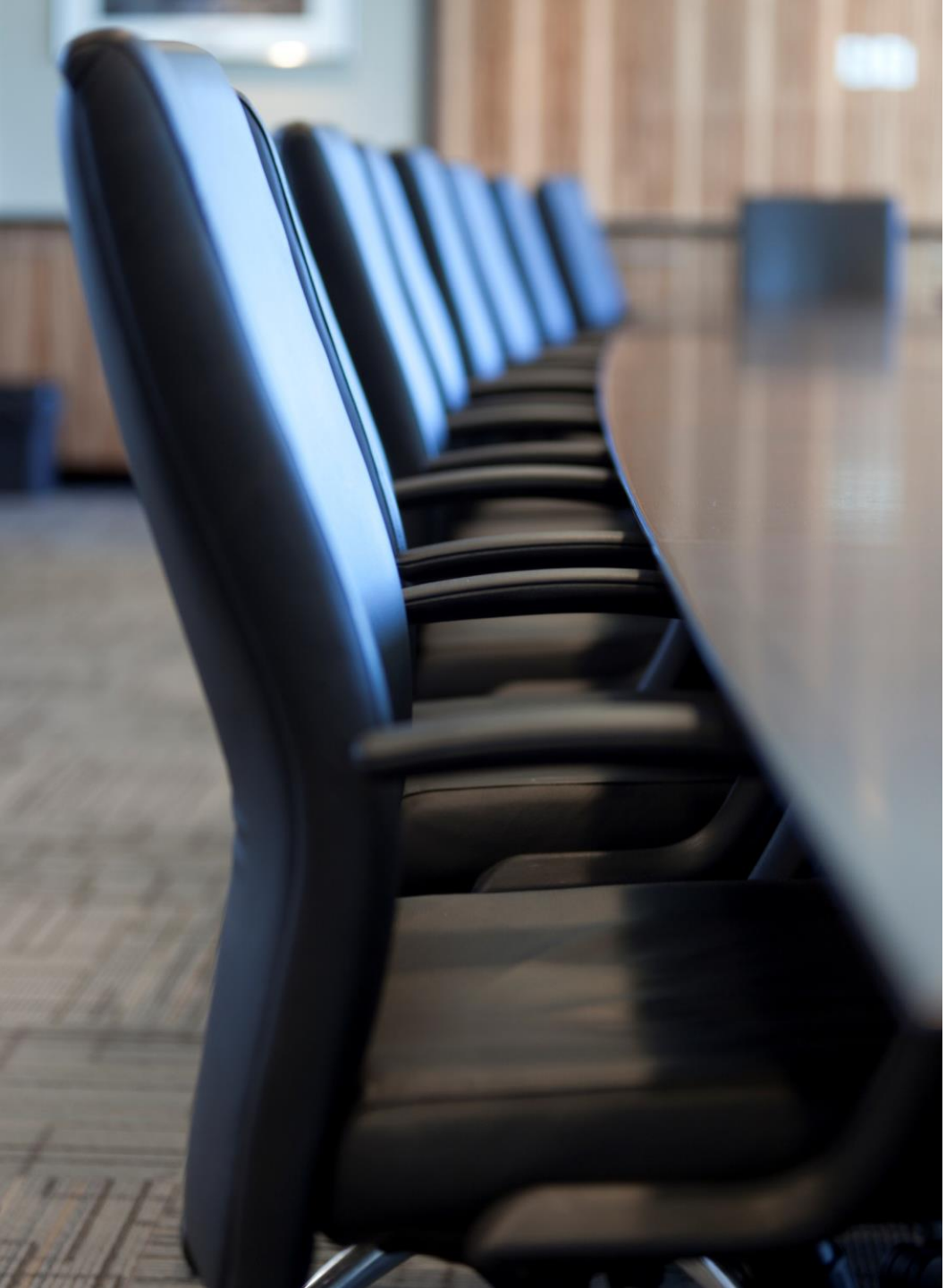
Cyber Risk

and the role of Directors on the Board

RISCCO | March 7, 2022 | 8 minutes | 1686 words |
(updated August 2024)

CONTENT

RISCO



1. Introduction

The Board of Director in our latitudes, for the most part, have invested time in reviewing financial performance, deciding on the strategic plan and approving key staff appointments.

The dependence of organizations on information technology has forced issues such as cyber-risk to be part of the agenda of the Board.

The sophistication and impact of technological threats-risks demands that the Directors on the Board adopt a proactive, decisive and continuous role on the impact of cyber-risk on the organization.

All of the above becomes much more complicated with the poorly controlled growing use of artificial intelligence (AI) and generative AI in corporate decision making.

1. Introduction

It is healthy to mention that there are two terms that are generally used in organizations as if they were the same, when in fact they are not.

Cyber-risk

It is the risk of financial loss, interruption of operation or damage to the reputation of an organization due to some kind of failure of its information technology systems.

Cyber-security

It is the art of protecting networks, devices and data from unauthorized access or criminal use in order to ensure the confidentiality, integrity and availability of data.

In the next pages, we answer eight questions we are usually asked about the role of Directors on the Board in connection with cyber-risk.

2. Cyber-Risk and the role of the Board

1

Is cyber-risk so critical in the organization to require the attention of Directors on the Board?

Cyber-risk is critical. According to Forbes magazine, the risk is not just financial, reputational or legal; now even people's lives and safety are at stake. According the security company Check Point, in Q2 2024, organizations experienced an average of 1,636 cyber attacks per week, representing a 30% year-over-year increase. Cyber attacks on companies are becoming more frequent and sophisticated. Regulators are demanding more protection for customers' personal data. The FBI indicated that in 2023, Cybercrime cost Americans over USD12.5B

2

There is a Director on the Board who is an accountant but took some courses on information technology, why is it necessary for Directors to know about cyber risk?

Knowing about information technology does not mean knowing about cyber-risk and/or cyber-security. By analogy it would be to expect a dentist to do open heart surgery and the anesthesia is applied by a cardiologist. They are all doctors, but with different specialties. The same goes for cyber-risk, cyber-security and information technology; they are related themes, but with different approaches, frameworks for action and perspectives.

RISCCO

2. Cyber-Risk and the role of the Board

3

If there is a Risk Committee and a Technology Committee, Why do the Directors in the Board have to be aware of cyber-risk?

Because each one has different roles. The role of the Directors in the Board has ceased to be a governance body, very formal, sometimes unattainable for employees, which meets regularly to analyze financial indicators. Today, The Directors in the Board have a more active role on key issues that were previously seen only by the Management. Cyber-risk is just one of them. In addition, regulators expect that cyber risk is part of the Board of Directors' agenda regularly and not occasionally.

4

The Directors in the Board approve the purchase of technologies to protect computer systems and networks. That's being aware of cyber-risk, isn't it?

It's not. It is positive that the Directors in the Board approve the purchase of technologies and consulting services to protect the networks and systems of the organization. However, the role of Directors in the Board in terms of cyber-risk is broader and more strategic. In the answers to questions six and seven, we expand on this topic.

RISCCO

2. Cyber-Risk and the role of the Board

5

The Directors of the Board have diverse knowledge. Why should we be experts in cyber-risk?

Directors at the Board are not expected to be experts in cyber-risk, but they are expected to handle basic language to make appropriate decisions when the experts in risk, technology and information security bring important issues that require the attention and judgment of the Directors of the Board. When asked if only one Director or all Directors should know about cyber-risk, we are the opinion that everyone should be. To this end, Directors in the Board must receive basic and continuous training on cyber-risk, cyber-security and emerging technological risk-threats like the risks of using artificial intelligence in taking corporate decisions.

6

What should be the role of the Directors in the Board in terms of cyber-risk?

Many business initiatives that generate profitability, depend on the use of information technology and inevitably carry technological risks and threats. Directors in the Board should design strategies, but not articulate them. Focus on follow-up, monitoring and review activities of the initiatives that the Management carries out in terms of cyber-risk. Stay up-to-date on technological risks and threats, as well as modern trends in information security.

RISCO

2. Cyber-Risk and the role of the Board

How can the Directors in the Board ensure that the measures in cyber-risk and / or cyber-security in the organization are effective?

Regularly assessing that:

- The KPIs defined for cyber-risk and cyber-security are the values expected over time.
- There are mechanisms for employees to express at any level of the organization some concern about technological risks and threats.
- The cyber-security strategy is integrated into the organization's strategy.
- The appetite or tolerance to cyber-risk defined by Management is adequate.
- The resources and structures approved by management for the areas in charge of managing cyber-security and cyber-risk are adequate for the organization.
- In the Risk/Audit/Compliance/Technology Committees there is an independent member with strong cyber-risk and/or background.
- Be regularly updated on the latest trends in cyber-risk and/or cyber-security.

Sources: Institute of Risk Management; National Institute of Standard & Technology; Cybersecurity & Infraestructure Security Agency; Harvard Law School Forum on Corporate Governance; Cyber-security Venture, ChatGpt 4.0

RISCCO

2. Cyber-Risk and the role of the Board

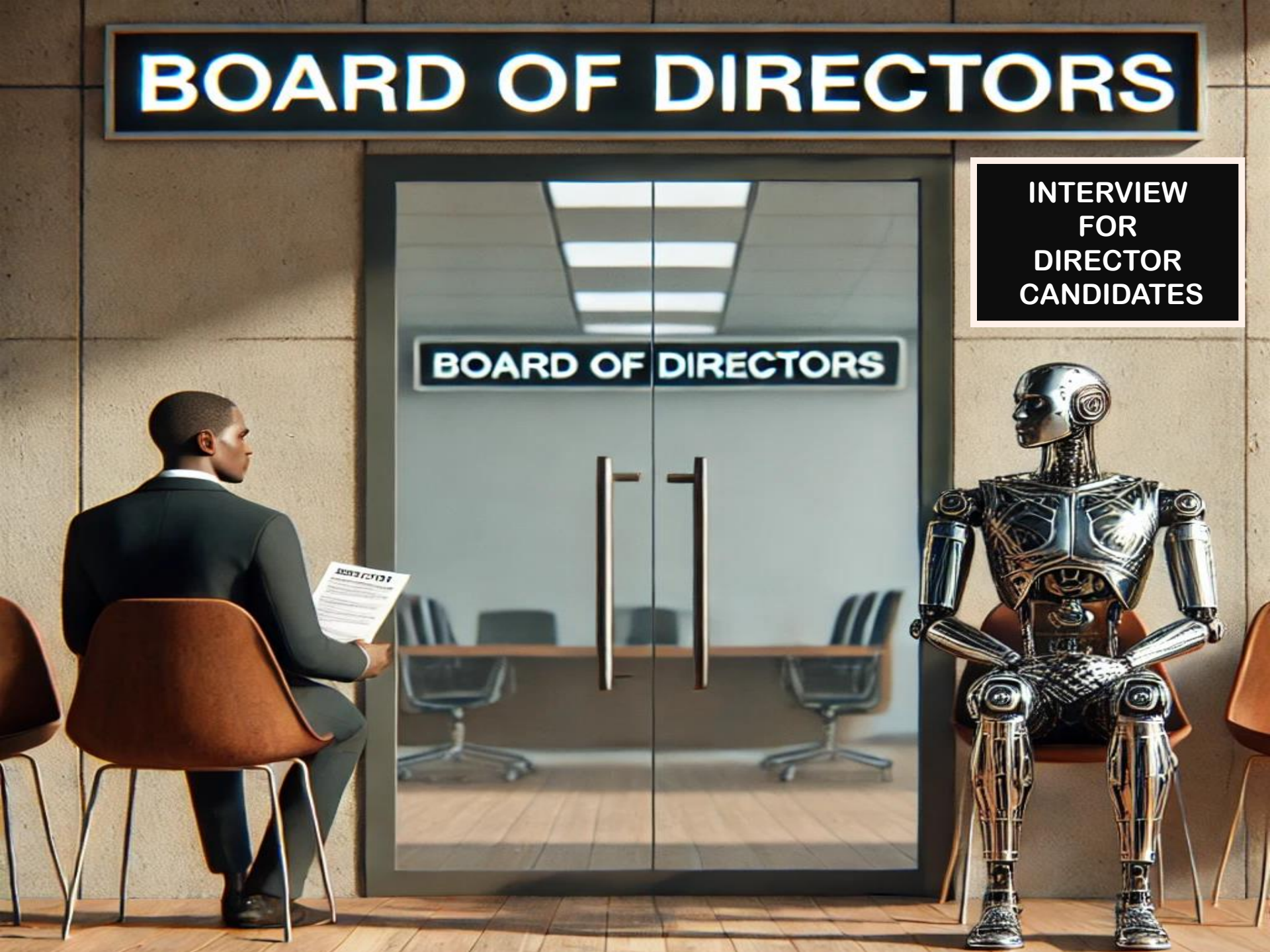
8

With the growing and poorly controlled use of generative artificial intelligence (AI) for corporate decision making, what should be the role of the Directors of the Board ?

The use of AI and/or generative AI for corporate decision-making, bring several risks like: Bias and Fairness; Data Privacy and Security; Ethical Concerns; Regulatory and Legal; Over-reliance on AI.

The Board of Directors plays a critical role in overseeing the use of AI and/or generative AI within an organization. Special attention, at least, in the following is needed:

- Ensure that the organization's use of generative AI aligns with its overall strategic goals and values.
- Establishing an AI Governance Frameworks.
- Make sure organization has in place a robust risk management process to manage the risks associated with AI.
- Confirm that clear lines of accountability are established for AI-related decisions.
- Stay informed about evolving AI regulations and ensure that the organization is compliant with current and upcoming laws.
- Ensure that both directors and management are continually educated about AI technologies, risks, and best practices.
- Consider incorporate to the board, a member with AI background.


BOARD OF DIRECTORS
INTERVIEW FOR DIRECTOR CANDIDATES
BOARD OF DIRECTORS

3. Final Thoughts

1. The role of Directors on the Board goes far beyond the traditional activities in which they have been involved so far. Having a basic understanding of cyber-risk is essential, as is being vigilant of management's key initiatives in cyber-security and/or cyber-risk.

2. As a bord member, it is a misjudge to think that decisions and monitoring of technological threats-risks are exclusive aspects of the GRC (Governance, Risk & Compliance)units.

3. Although it is understandable that some Directors in the Board feel that their limited time should be prioritized for decisions of a financial nature over others such as cyber-risk, is not acceptable anymore.

   It is always healthy, to keep in mind, that no one is immune to be a victim of a cyber risk incident.

CONTACTS

Panama and CARICOM

Antonio Ayala I., CEO
aayala@riscco.com

Roberto Delgado, Manager
rdelgado@riscco.com

Rubén Fernández, Manager
rfernandez@riscco.com

Central America

Maria Cristina Marroquín, Commercial Assessor
mmarroquin@riscco.com

riscco.com

It is an independent international company dedicated exclusively to helping organizations meet their challenges in GRC (Governance, Risk & Compliance) and ESG (Environmental, Social & Governance); composed of professionals with the knowledge and credibility necessary to translate very technical aspects into a simple language with business sense. With fifteen (15) years of having started operations, RISCCO has in its client portfolio private companies and Government Institutions in the region leaders in their field.