



ADMINISTRATRICES
ET ADMINISTRATEURS
ENGAGÉS

The central graphic consists of a large orange circle centered on a dark blue rectangular background. Inside this orange circle is a smaller dark blue square. Within the dark blue square is an orange circle, and inside that is a dark blue triangle pointing downwards. The text 'Digital security and governance' is written in white, bold, sans-serif font, centered within the orange circle.

Digital security and governance

MEMBERS OF THE WORKING GROUP:

Marie-Noëlle Brisson
Damien Chaminade
Christine Dubus
Nathalie Kestener
Anne-Hélène Monsellato
Marie-Hélène Rigal

INTERVIEWS:

Vincent Lorient, ANSSI
Lumena Duluc, CLUSIF
Henri d'Agrain, CIGREF
Christian Poyau, former commission chairman, co-chairman of MEDEF'S
Technological Change and Societal Impact Commission

«IFA has decided to enhance directors' skills in the challenges of digital and technological transformation by publishing two guides, one on cybersecurity and the other on artificial intelligence. Indeed, in addition to being a strategic asset, data has become an issue for all organizations, which boards of directors must address from the angle of strategy in general, and digital strategy in particular.

The acceleration of digitalization, but also regulatory pressure, are increasing directors' responsibility, particularly in terms of the impact of strategic choices, but also in terms of monitoring risks and allocating resources.

Training is a major tool for understanding data, and is essential for all informed and collegial decision-making. The IFA will soon be adding to this with a guide to data governance, which is essential for contributing to data quality and protection, and for examining sensitive data and its use within a sovereign framework.»

EXECUTIVE SUMMARY

The responsibility of boards of directors for digital security issues is growing rapidly in a constantly changing global context, which is becoming increasingly complex in regulatory, geopolitical and technological terms.


Organizing governance around these issues becomes imperative, by ensuring that directors are regularly trained to bring the subject to board discussions, either directly, or via a specialized committee or a designated director. In addition to simply raising awareness, directors need to be empowered to interact with operational experts (CISOs, CIOs, Security Directors) and with the company's risk and compliance experts, at the right level. In certain cases where the company's exposure is deemed to be high, bringing in outside expertise or a director who has completed a certification program will clearly enhance the board's skills.

Digital security is a major strategic issue for the board of directors, and facilitates a practical approach to data governance, from creation to destruction. This process includes the qualification of data (e.g. sensitive or critical), its reliability, use, processing and storage, underlining the importance of the associated carbon footprint. Data governance is the cornerstone of digitalization, if we are to take full advantage of artificial intelligence.

The board must clearly express and formalize its involvement in digital security issues in a dialogue with senior management, and ensure the latter's involvement and commitment in setting up and deploying the cyber plan.

To ensure solid preparation at all levels, the board's approach on this subject should focus on three key areas. Because the question of intrusion is no longer if, but when, it will happen, and because a crisis cannot be prepared for on the day of a critical incident, the board must question how executive management:

1) proactively structures its preventive actions (technical, organizational, financial and human resources for identifying and monitoring risks and internal control, as well as training);



2) anticipates and organizes crisis management to manage an attack (the right reflexes) and build its business recovery plan;



3) and what considerations it has given to cyber insurance.

The existing framework needs to be adapted, with the implementation of a structured approach. In fact, cybersecurity brings to the fore tools that were previously little known: data governance, cyber risk analysis, crisis management, disaster recovery planning, penetration testing, vulnerability scans, to name but a few. Boards must therefore make these tools and new processes their own, especially as some of them are compliance requirements (e.g. NIS2, GDPR).

Far from being merely a technical debate, discussions around cybersecurity issues are building another, equally important form of corporate resilience, by opening up a genuine digital and data strategy, and thus a new field of possible opportunities.

TABLE OF CONTENTS

FOREWORD	3
EXECUTIVE SUMMARY	4
SECTION 1	
GLOBAL CONTEXT AND DIGITAL SECURITY RISKS	6
1.1 A story in constant and rapid evolution	7
1.2 What is cybersecurity?	9
1.3 A key element in strategy	11
1.4 A more transparent and reassuring regulatory and legislative framework, that remains complex	12
SECTION 2	
CHALLENGES FOR THE BOARD	13
2.1 Structuring the board to meet these challenges	14
2.2 Individual and collective responsibility	18
2.3 Board and director training	20
SECTION 3	
WHICH ARE THE BEST BOARD PRACTICES TO ENSURE CORPORATE RESILIENCE?	22
3.1 Data governance	23
3.2 Is the company prepared? - Prevention	25
3.3 Business continuity plan (BCP)	31
3.4 Anticipating a critical incident - The crisis unit	34
3.5 Insurance(s)	36
3.6 Does the company know how to deal with an attack?	38
CONCLUSION	41
APPENDICES	42



Access full guide (opens new website) <https://www.ifa-asso.com/mediatheques/guide-securite-numerique-et-gouvernance-english/?cat=363>

View Guide launch on YouTube (in French). <https://www.youtube.com/watch?v=0rZT9eX-Gzw>

