Wednesday, April 3rd 2024 - 00:00 Europe/Paris
928 words - 4 min

L'AGEFI

COMPANIES

: L'AGEFI

Directors urged to take digital security seriously

The French Institute of Directors is about to publish a dedicated guide, inviting boards to engage in dialogue and challenge executive management.

At a time when artificial intelligence (AI) is opening up new possibilities and cyber-attacks are multiplying, administrators need to get to grips with these issues. To help them do so, the Audit Committee Chairmen's Club of the French Institute of Directors (IFA) is about to publish a guide to best practice in "security".
digital and governance". The IFA's 2016 guide to the audit committee's role in cybersecurity, highly innovative at needed an update. Especially as the subject concerns all directors. In both France and the United States In the United States, "comexes have become aware of cyber issues, but boards of directors have not. They tend to pass the buck to the CIO or the insurers, as the subject is outside their comfort zone", confides Marie-Noëlle Brisson, rapporteur for the group of and co-founder of CyberReady LLC. The aim of this guide is to help them relax and enrich their dialogue with senior management and investors.
Simply raising awareness of these issues is not enough, especially as the cost of cybercrime was estimated at $8,000 billion worldwide last year by CyberSecurity Ven- tures. Administrators need to be able to interact "*at the right level, with operational experts (CISOs, CIOs, Security Directors) and corporate risk and compliance experts*", explains the guide. This requires a minimum level of training in cybersecurity issues. Directors need to be trained in an ever-increasing number of subjects, if they are to understand them properly. A real challenge for boards of directors.

For the most exposed companies, a dedicated committee (digital, num- rique, technological...) or a director trained as part of a certifying course would be a plus for the board. Marie-Noëlle Brisson admits: "*This is a widely debated issue. Be careful not to recreate a 'codir' on the board, with a specialist for each subject. All directors need to understand what*'s at *stake.* As with all "specialists", this must not be allowed to overburden the rest of the Board, which remains collegially responsible. The board's by-laws must stipulate when and how the committee or specialist director communicates with the board.

Read also: Sustainability calls for greater commitment from boards of directors

Training to understand the issues

In concrete terms, how can we take action? The board must formalize its involvement in digital security issues through dialogue with senior management, and verify its real involvement in setting up and deploying the cyber plan. Marie-Noëlle Brisson continues: "*Effective dialogue requires pertinent questions and a clear understanding of the answers. Digital security is better dealt with by the boards of major groups, particularly in the banking sector, although there is always room for improvement. On the other hand, it is still much less present on the boards of small and medium-sized businesses, which are less well equipped.*" As with many areas of board activity, "*one of the pitfalls would be to limit ourselves to compliance, which is necessary but insufficient, and which does not allow us to seize strategic opportunities*", warns Marie-Noëlle Brisson.

The question of intrusion "*is no longer if, but when it will happen*", stresses the report. It is therefore a question of anticipation. The guide proposes three lines of thinking.

Firstly, preparation. How does management dynamically structure its preventive actions (technical, or- ganizational, financial and human resources for identifying and monitoring risks and internal control, as well as training). What level of information is required? What human, technical and financial resources are deployed, and with what audit? Are cyber-attack exercises carried out regularly? While digital security is both a strategic and operational subject, "*one of the difiiculties is to position the cursor correctly between steering strategy and managerial interference*", warns Marie-Noëlle Brisson. *It all depends on the quality of the questions and the trans- parence of management. For example, we don't go into the details of the continuity plan, but we do look to see if it has been prepared, rehearsed and practiced.*"

Secondly, how the company anticipated and organized crisis management during an attack, and built up its business recovery plan. If investors are increasingly demanding trans- parency, external communication must be handled with care. "*Investors, rating agencies and proxies need to hear that internal procedures are robust and practiced,*" continues Marie-Noëlle Brisson. Disclosing incidents and attacks within a reasonable framework is no longer perceived negatively, since no one is immune.

Thirdly, how management views cy- ber insurance. "Transferring risk to the insurer *doesn't solve all the issues*," says Marie-Noëlle Brisson. All the *more so as policies are becoming increasingly expensive and exclusion cases are multiplying.*"

Read also: AI challenges the habits of business leaders

Preparing for the integration of AI by the company

Boards ready to tackle digital security issues will also be armed to adapt to the arrival of artificial intelligence. "*The best preparation involves good data governance and the implementation of procedures,*" anticipates Marie-Noëlle Brisson. *Faced with pressure from regulators, it's essential to prioritize and map data. We can't protect them all.*" This data governance process covers all aspects of data qualification (sensitive, critical, etc.), reliability, use, processing and storage. It also includes a carbon footprint analysis, essential to the company's customer transition strategy. A reminder that administrators need to be present on all fronts at once.

photo European Union -

by Brunoderoulhac@agefi.fr(bruno De Roulhac)

c879e5788c25a980c6e41b18d903e15f089A6a665Zc6G6af9cf6085