Cybersecurity risks and situation awareness: Audit committees' appraisal

Didier Fass, Stéphanie Thiéry

Cybersecurity risks and situation awareness: Audit committees' appraisal

Stéphanie Thiéry 1,3 Didier Fass1,2

1 ICN BS 86 rue du Sergent Blandan, Nancy, France
stephanie.thiery@icn-artem.com
2 Mosel Loria UMR CNRS 7503, Université de Lorraine,
didier.fass@loria.fr
3 CEREFIGE, EA 3942, Université de Lorraine

AUTHORS VERSION

Abstract. The issue of cybersecurity has become a challenge for companies and boards of directors. Cybersecurity is not only an IT topic but a risk extended to all operations of the companies. Indeed, cybersecurity potentially has an impact on financial reporting quality, this attribution being one of the duties of audit committees. Using Endsley's model, our exploratory study seeks to determine the levels of cyber situational awareness of audit committee members, how they comply with it and if this appraisal matches the steps identified within the model.

Keywords: Cybersecurity Awareness · Board of Directors · Audit Committee · Safety by Design · Cyber-resilience

1. Introduction

Cybersecurity is nowadays a significant topic within organizations since the last 25 years, assets of companies have evolved from physical assets to the digital [1]. Intangible assets valued according to international standards are particularly sensitive to internal or external manipulation and attack. However, taking cyber risk into account mainly covers the IT (internal IT) technical risks. The human and organizational factors aspects are neither clearly known nor clearly identified, in particular by decision-making bodies such as Board of Directors. Thinking the company as an integrated system "critical security" and the risks inherent to its field of activity are a theoretical and practical issue.

If the explicitly described missions by regulation were discussed in the literature, only few studies related to cyber-attacks management exist at board level [2] or, specifically, at audit committee level. Thus, the literature on boards and audit committees has not operationalized the examination of this risk by governance institutions. Indeed, the criticism of organizational data is a well-known issue of actors who are responsible for, as indicated by [3], since the developed model in their study allows to take into account the data owners', senior management's and legal experts' point of views to give a framework to data security assessment. Authors also recommend an implication of internal audit and information technology functions [4].

However, these works do not consider the direct appropriation of this issue by governance institutions as board of directors or audit committees. Yet, regulation seems to have integrated the topic, requiring firms to perform a cyber-risks assessment, with associated costs and consequences or a description of occurred cybersecurity issues

including their costs and consequences [5]. Clark and Harrell [6] however highlight that if SEC current recommendations (disclosure of data breach issues) became obligations, directors of public companies could incur lawsuit risks, in addition to the decrease of share price. For this reason, Lunn [7] indicates the questions directors should ask in case of cyber-attack in order to protect their responsibility if the latter was engaged. He advocates to consider some factors in their monitoring role: existence of monitoring process of cyber risks, probability and consequences of loss related to cyber-attacks, existence of consequences which may adversely affect human lives or the survival of organization or implementation of action plans to mitigate cyber risks.
Recommendations are given in order to limit directors' responsibilities, such as training directors to cybersecurity issues or recruiting directors having an experience in this field. Von Solms [8] takes up an assessment model of board maturity in terms of cybersecurity device review. This model allows an assessment of cyber governance knowledge within board members, giving insights on their understanding of the issue and the implementation degree of cyber governance. However, if this model contributes to the self-assessment of the directors' actions, it seems that it does not exist any study building a state of directors' competences and received information (particularly of audit committee members) in terms of cybersecurity. To our knowledge, the appraisal of audit committee members on the review of cyber risks has not been investigated in the literature: are audit committee members aware of issues related to cybersecurity?
There are still unanswered questions regarding the audit committee functioning process in general [9] and, specifically, as for cyber issues and those process issues remain neglected by researchers. In order to answer our previous question, we favored a field study and a qualitative approach. This leads us to determine if audit committees address significant cybersecurity topics and / or face cybersecurity breaches. Our work in progress seeks to determine if audit committee members are aware of the issues linked to cybersecurity, in order to improve both cyber-resilience and safety by design decision-making.

2. Cybersecurity awareness and human factors at board level

Management and production information systems and digital informations, especially if they are strategic assets for the company, are safety-critical. Consequently, the impact of deficiencies of cybersecurity can have global consequences: loss of intellectual property, risks of legal or regulation-linked penalties, reputation loss, costs to restore clients' confidence and to give explanations to authorities [10].
To prevent that systemic risk, one needs to be able to estimate related human factors such as situation awareness and processes responsible for maintaining it.
Three categories of main components impact cybersecurity at each organizational levels of the socio-technical system : technical risks / factors, human risks / factors and organizational risks / factors. Misunderstanding or underestimation of cyber-risks is thus a danger for the company that must be dramatically considered at board level. Because cyber risks are not only virtual but actual, taking into account this serious danger is a question of situation and risk awareness depending on knowledge, cognitive bias or emotional states which participate to the perception of the risks and which influence decision-making and control process [11] [12] [13].

Just like aeronautics, i.e airplane piloting and air traffic control, enhancing cyber situational awareness at board and audit committee levels is a major issue. Thus, board of directors seem to be considering the topic since, according to NACD 2016-2017 public

and private company governance surveys, 81% of surveyed boards address cybersecurity issues during meetings and that 51% of respondents claim that cybersecurity should be considered at audit committee level. In order to evaluate the cyber situation awareness of audit committees' members, we favored Endsley's framework [14] and its three levels. This enables us to assess the perception, the comprehension and the projection of the audit committee's members.

3. Directors' appraisal of cyber issues

3.1. Method used, Data collection and analysis

Our collection of empirical material is driven by our exploratory study. We both rely on invaluable observations of audit committee meetings, interviews with audit committee members and participants, publicly available reports and internal documents. Interviews lasted, on average, between 60 and 120 minutes and on-site observations around 150 minutes each.

First, we reviewed publicly available documents (10-K reports) to gain understanding on how organizations formally report on audit committees' appraisal of cyber issues. We next got closer to the field and supplemented our empirical material, with an source of data constituted by on-site observations of two audit committee meetings. Furthermore, we carried out 27 semi-structured interviews with audit committees' members but also with individuals who attend the meetings, such as partners of audit firms and chief audit executives. Interviews are a relevant data collection mechanism, complementary to observation-based material [15]. Having completed on-site observations with, first, documentation and, second, interviews was a powerful tool in order to help us gathering evidence of their appraisal of cyber risks and cyber issues.

Firms addressing cybersecurity topic / cyber risks	Firms hearing the Head of IT department during audit committees
Arkema, Biomérieux, Bouygues, Burelle, CGG, Dassault Systèmes, Engie, Essilor, L'Oréal, Renault, Saft, Sanofi, Technicolor, Total (*14 firms*)	Endered, Essilor, Saft, Valeo (*4 firms*)

Table1. Content Analysis (66 listed French firms)

3.2. Level 1 SA - Perception: Disclosed cyber-awareness to the public and individual returns of experiences

Listed firms communicate and disclose both their internal control concerns and their risk assessment. Being part of the most important emerging risks, cyber issues are disclosed within the 10-K reports. This is confirmed by the content analysis we achieved on our 2015-2016 annual reports of French firms. On 66 firms for which we examined the audit committee reports, 18 made explicitly reference to a review of cyber risks (table1). Out of our 2 on-site observations and 27 interviews conducted, only one on-site observation and three interviewees mentioned and analyzed cyber issues. This is far more less than the 51% of firms supposed to address cyber risks at the level of audit committee [1]. Hence, according to our field work, some audit committee members highlighted a basic perception of cyber situation awareness : " we have an extremely high risk (…); on particular points with can be presented and studied in depth by the audit committee".

3.3. Level 2 SA - Comprehension

However, it seems that only 54% of global organizations have carried out an assessment related to fraud or economic crime. In particular, less than half of firms have achieved a vulnerability assessment related to cyberattacks and only 30% have implemented an action plan [16]. Furthermore, for members of audit committees and, more generally, for boards, "cyber" is new for many directors, and is certainly far from intuitive" [17].

As our interviewees stated : “we have to perform regular checkup and that, basically, we acknowledge that some persons may have non-restricted accesses to the system (…) This must be the subject of a presentation and in-depth study while audit committee meetings”.

3.4. Level 3 SA - Projection

Mostly our field work highlights that directors are first “cyber-risks aware” and that they intend to get a specific overview of the main cyber issues, using ever specialists or governmental agencies in order to help them appraise and improve cybersecurity: “we asked specialists and ANSSI in order not to waste time”.

Moreover, our interviewees assess that, in order to be compliant with the main internal control frameworks (COSO, COBIT), they target some specific levers of control, such as control environment (the ‘tone at the top’ and human knowledge and skills) and control activities (Segregation of duties): “we need to train our people to improve their cyber awareness and secure their accesses and behaviours(…) specifically we must disseminate this cyber awareness through operational middle management and their teams”.

4. Directors’ appraisal of cyber issues

Annual report should disclose the risks including cyber issues if it happened but only if they are material. This means that without any material effect, cyber issues are not always revealed to the public. Our analysis confirms that this disclosure is not obvious and depends on the knowledge, expertise and will of the boards. Nonetheless, our exploratory study highlights that, when audit committees tackle cyber issues, they follow Endsley’s process and that they both embrace, appraise, evaluate and disseminate the issues. Our preliminary analysis should be of course deepened with archival data in order to validate this fieldwork evidence, but our work underscores requirement and impetus for improving board cyber situation awareness.

References

1. NACD, Cyber-Risk Oversight, ed. Larry Clinton, Director’s Handbook Series, National Association of Corporate Directors, Washington DC, USA (2017)
2. Higgs, J. L., PinskerR., Smith T. and Young G., The Relationship Between Board-Level Technology Committees and Reported Security Breaches. Journal of Information Systems, vol. 30, 3, pp 79-98 (2016)
3. Rahimian, F., Bajaj, A., Bradley, W., Estimation of deficiency risk and prioritization of information security controls: A data-centric approach, International Journal of Accounting Information Systems, vol. 20, pp 38-64 (2016)
4. Steinbart, P. J., Raschke R. L., Gal G. and Dilla W. N., The influence of a good relationship between the internal audit and information security functions on

information security outcomes." Accounting, Organizations and Society. 71. 15-29 (2018).
5. CF Disclosure Guidance: Topic No. 2 - Cybersecurity - SEC.gov (2011) https://www.sec.gov/divisions/.../guidance/cfguidance-topic2.htm
6. Clark, M. E. and Harrell C., Unlike chess, everyone must continue playing after a cyber-attack, Journal of Investment Compliance, vol. 14, 4, pp. 5 - 12 (2013)
7. Lunn, B., Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine, Journal of Law and Cyber Warfare, Vol. 4, No. 1, pp. 109-137 (2014)
8. Von Solms, B., Towards a cyber governance maturity model for boards of directors, International Journal of Business & Cyber Security (IJBCS) vol. 1, 1, pp 1-9 (2016).
9. Gendron, Y., Bédard, J., and Gosselin, M., Getting Inside the Black Box: A Field Study of Practices, « Effective » Audit Committees. Auditing: A Journal of Practice & Theory, 23(1), pp 153-171 (2004).
10. KPMG, Boardroom Questions. Cybersecurity - What does it mean for the board ? https://home.kpmg/content/dam/kpmg/be/pdf/boardroomquestions/boardroom-questions-cyber-security-what-does-it-mean-for-the-board.pdf (2017)
11. Endsley, M.R.: Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal 37(1), 32-64. Human Factors: The Journal of the Human Factors and Ergonomics Society. 37. 32-64 (1995a).
12. Endsley, M.R. Measurement of situation awareness in dynamic systems. Human Factors: The Journal of the Human Factors and Ergonomics Society 37(1), 65–84 (1995b)
13. Damasio, A., Descartes' Error: Emotion, Reason, and the Human Brain, Putnam Publishing (1994).
14. Endsley, M.R., Situation awareness analysis and measurement, chapter theoretical underpinnings of situation awareness. A Critical Review. Endsley, M. R. and Garland D. J (Eds.)Situation Awareness Analysis andMeasurement. Mahwah, NJ: Lawrence Erlbaum Associates, pp 3-33 (2000).
15. Yin, R. K., Case Study Research Design and Methods. Thousand Oaks, CA: Sage (2014).
16. PwC's Global Economic Crime and Fraud Survey. https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html (2018)
17. The Corporate Governance Advisor, Cybersecurity, vol. 2, 5 (2014)