Cybersecurity: How Ready Are Belgian Directors and Boards?

GUBERNA Sounding Board Committee on Cybersecurity

Authors: Alex Driesen, Dirk Schilders, Iwona Muchin, Jochen Maertens, Marc Vael, Olivier Braet

GUBERNA
INSTITUUT VOOR BESTUURDERS
INSTITUT DES ADMINISTRATEURS

Contents

Introduction

GUBERNA's Cybersecurity Sounding Board Committee has conducted two exploratory surveys with its community of Belgian directors, focusing on cybersecurity governance. These surveys aimed to evaluate directors' perceptions of cybersecurity within their strategic frameworks, their awareness of cybersecurity issues, and their depth of knowledge on the topic. Specifically, we explored how governance maturity can be achieved through various approaches, such as the frequency of cybersecurity discussions on the board’s agenda, the existence of clear incident response plans, well-defined accountability frameworks, and the regular conduct of cybersecurity audits. We hope this report will inspire directors to assess and refine their cybersecurity governance to match the specific needs and risk profiles of their organisations. You can read a two-page overview of the main conclusions from the Sounding Board Committee for Cybersecurity here. For more information about the Sounding Board Committee for Cybersecurity, visit this link.

1. Cybersecurity’sstrategicimportance

As part of the corporate strategy, cybersecurity is now seen as critical in protecting organisational processes and reputation. The governance of cybersecurity is mainly driven by existing industry standards and guidelines, and their ecosystem of peers and organisations.

Cybersecurity as a strategic topic

As a strategic topic in today’s global context, cybersecurity is first and foremost viewed as critical in protecting internal and external organisational processes, and the organisation’s reputation. External pressures from regulators or from customers are ranked as the second and third most important choice. Only a smaller group of directors in the survey rank cybersecurity as a strategic differentiator, or as a mere default cost of doing business today and tomorrow. Finally, almost no director views cybersecurity as not being critically relevant to the corporate strategy.

	1st choice	2nd choice	3rd choice	4th choice	5th choice	6th choice
Cybersecurity is critical in protecting organisational processes or reputation	88%	9%	2%	0%	2%	0%
Cybersecurity is obligatory because of regulatory compliance	2%	36%	14%	34%	14%	0%
Cybersecurity is demanded by the customers	5%	21%	41%	22%	9%	2%
Cybersecurity is a strategic differentiator	3%	24%	31%	26%	12%	3%
Cybersecurity is mostly a default cost	2%	9%	10%	17%	53%	9%
Cybersecurity is not critically relevant for our strategy	0%	2%	2%	0%	10%	86%

Strategic drivers of cybersecurity

A majority or directors report that their current cybersecurity approach is mostly driven by **industry standards or guidelines** (34%). As second and third choice, input by professional organisations (25%) and influence of industry peers (23%) are also important drivers for adopting a cybersecurity approach. Surprisingly, existing regulation is seen as one of the smallest drivers for tackling cybersecurity (10%). Some directors mentioned other drivers such as pressure from their insurance company, from an auditor, from the holding company, or from internal staff demands.

2. Awareness and knowledge of cybersecurity

Directors are well aware of cybersecurity risks and are familiar with their organisation's cyber risk procedures and policies. The most important risks are integrity and security of their internal and customer data. Most directors feel that they are knowledgeable on the topic and feel comfortable discussing the topic on the board level, with a sizeable minority expressing some gaps in cybersecurity knowledge. One out of three directors have not (yet) followed any trainings on the topic, which could be point of attention in the context of the knowledge gaps of board members in specific domains.

Awareness of and familiarity with cybersecurity

GUBERNA's Directors are aware (57%) to strongly aware (28%) of cybersecurity risks. Only 16% considers themselves averagely aware of the risks, while no one considers themselves weakly aware or not aware at all.

When asked what kinds of cybersecurity risks are top of mind to them, the majority of cybersecurity risks mentioned are aspects of data security, confidentiality, and integrity (financial, production or commercial data, confidential data, or data in the cloud). Data leaks and ransomware are seen as top damages to the organisation (through hacking, cyber-attacks, fraud resulting in identity theft, social engineering).

Our directors are strongly familiar (19%) to familiar (43%) with the cybersecurity policies and procedures in their organisation(s). Smaller groups are averagely familiar (22%) to somewhat unfamiliar (16%), but nobody reported that they are completely unfamiliar with the topic. This implies that those cybersecurity policies and procedures are presented and sent to them on a regular basis. In the context of cybersecurity risk but also of cybersecurity incident preparedness, this makes sense.

Satisfaction with cybersecurity knowledge

The largest group (39%) reports being satisfied with their personal knowledge level on the topic cybersecurity. A significant minority (19%) is only medium satisfied. Very few directors are completely satisfied (2%) or completely dissatisfied (9%) with their level of knowledge. A point of attention is that one out of three directors signals to be dissatisfied with their personal knowledge level. A recommendation is that directors bring this topic on the agenda of board meetings. This should be coupled with some director level trainings.

As a consequence, a majority of the surveyed directors feel somewhat comfortable (40%) to very comfortable (19%) about the cybersecurity topic when it is raised. Only a very small minority of 3% feel very uncomfortable about the topic, but one out of four (26%) feels somewhat uncomfortable. The remaining group (12%) lies in the middle. A recommendation is to always speak up and ask for more explanations if the cybersecurity topic is not entirely clear to the director.

Knowledge of current and upcoming legislation

When asked to consider how informed they consider themselves on the **current** Belgian and European laws/regulations on cybersecurity and board member liabilities, 16% considers themselves fully informed. A large cohort is partially informed (50%) to not informed (9%) but these two groups can rely on their colleague board members for further information. More worryingly, one out of four directors in this survey (26%) considers themselves not properly informed and cannot rely on colleague board members for support. This requires a specific message to all those reporting cybersecurity topics to board members to ensure the content is understood by all board members.

The same pattern applies to knowledge of any **future** Belgian and European laws/regulations on cybersecurity and board member liabilities, albeit more strongly. 7% consider themselves fully informed, and 41% as partially informed. 21% are not informed but they can rely on colleague board members. Again, a rather sizeable group of 31% considers itself not informed and cannot rely on colleague board members. This implies that one out of two directors consider themselves not informed about future laws and regulations impacting their liabilities as board members.

Training or certification

Besides the importance of practical knowledge obtained through years of experience, many directors wish to follow tailor made courses to update their knowledge on cybersecurity. 34% of surveyed directors have not followed any specific training or obtained any specific certification on cybersecurity. One out of three directors have followed an in-house training (36%), while one out of five directors followed an external training (22%) or obtained an external certification (7%).

Of the group that followed any kind of cybersecurity training, most participants felt neutral (50%) to satisfied (26%) with the courses they followed or certificates they obtained. One out of five directors (21%) reported being dissatisfied though, so there is still room for improvement in providing useful content to board members. Nobody was completely satisfied with cybersecurity courses, and only very few people (3%) reported being very dissatisfied.

3. Directors' barriers and needs

Given the importance assigned to cybersecurity as a board topic, and the high awareness and relatively high knowledgeability of the topic, some important barriers remain present. Knowledge barriers, time restrictions, and a lack of awareness and resources are quoted as barriers. To overcome these barriers, directors expressed in the survey a need for more pertinent (read: tailor-made) information, briefings, or trainings. They also expressed a need for a better "helicopter" or even "satellite" view of cybersecurity within the organisation, and the presence of people that are able to translate operational cybersecurity details to a board-level dashboard. This is obviously a cornerstone for any topic discussed at board level and thus an important point for improvement.

Finally, regular external inputs are requested such as benchmarks with industry peers or cybersecurity evolutions (like the impact of AI on cybersecurity).

Barriers

When asked which are the most important barriers that prevents directors from being more cybersecurity-aware or cybersecurity-resilient, a first cluster of responses are about knowledge issues. Directors indicate that the cybersecurity topic is very complex and fast evolving, making it very hard to obtain the proper knowledge on the existing cybersecurity maturity with an overview of which protective and reactive measures exist and actually work. In particular the technical dimension of cybersecurity is still perceived as daunting to many directors. This is similar to any IT or digital systems topic in general which is handled at board level. Because the cybersecurity topic can become technical quickly (especially terminology, technological and legal aspects and impact on other topics or departments), it is hard to obtain and/or understand a proper "helicopter" or "satellite" view on the state of cybersecurity at an organisation.

A second cluster of quoted barriers is time. Directors report time constraints caused by the complexity of the cybersecurity topic (making it necessary to invest more than time compared to other board topics in keeping up to date and going in-depth) and by conflicts with other time commitments and priorities.

A few directors report awareness in the organisation as a barrier, either because there is a lack of cybersecurity awareness and knowledge in the management team to correctly assign the cybersecurity risk level, or because of conflicting priorities.

Finally, few directors see costs or lack of resources dedicated to cybersecurity as a barrier.

Needs

Mirroring the knowledge barrier, the most important need expressed by directors is a thirst for knowledge on cybersecurity. Directors want to receive concise updates on the latest insights and evolutions in cybersecurity, director-level tailored trainings on cybersecurity, and proper information sessions on what the organisation currently does on cybersecurity, what would be an ideal state and how to get there. Directors also thirst for continued specific (to formal) trainings for directors on cybersecurity, covering terminology, technological and legal aspects and impact on other topics or departments. A suggestion might be to appoint a cybersecurity champion amongst the existing directors.

A second cluster of needs pertains to having a better “helicopter” or “satellite” view of the relevant regulatory framework(s), cybersecurity governance in complex environments, overviews of potential cyber risks and how to mitigate them to an acceptable level. Directors also look for objective evaluations/ratings to help them assess the adequacy of the cybersecurity framework used in the organisation as part of the overarching enterprise risk management framework, or various benchmarks that may exist within their industry.

Thirdly, directors see a constant need for good experts within the organisation, be it an experienced DPO (Data Protection Officer), colleagues specialised in the technological aspects (IT security) or in legal aspects (such as compliance or GDPR).

Finally, directors feel the need for more external objective information. This could come from an external audit, or from an independent third-party cybersecurity specialist. Benchmarks with information on cybersecurity incidents that actually occurred in the same industry would be helpful and inspiring, as would relevant white papers and books that provide useful insights for directors on a number of strategic cybersecurity evolutions and trends.

4. Cybersecurity governance

Cybersecurity governance can reach varying levels of maturity and complexity, depending on each organisation’s unique challenges. The topic should appear with some regularity on the board’s (or committees’) agenda. Cybersecurity governance should also include a practical plan to handle a cybersecurity incident or crisis. Ideally, the cybersecurity topic is regularly presented and discussed at board level. Organisations can conduct audits or assessments to see whether their cybersecurity framework and processes are still up-to-date, effective, and efficient. Having an appropriate cyber insurance policy tailored to the organisation’s maturity, needs and risk profile might be considered.

Anticipating risks and accountability

In 70% of the companies in the survey, directors report having an up-to-date plan to manage cyber incidents. 39% states to have a plan that has been recently tested, while one out of five directors (21%) state that the cyber incident plan has not been tested recently. 16% is developing such a plan. Only 13% signals there is no such plan in place, and the smallest group (5%) has a plan but considers it not up to date.

Four out of five directors strongly agree (55%) or agree (26%) that they have a clear understanding of who is accountable and responsible for monitoring cybersecurity within their organisation. 19% report a medium to very weak understanding of the accountability and responsibility lines.

Frequency of board discussions

Only one in five directors (19%) states to be actively involved in shaping and reviewing the organisation's cybersecurity strategy. Large sections report they are either not involved

(36%) or only somewhat involved (45%). This might be due to the frequency with which the topic is treated during board discussions, but also the topic can be daunting.

In theory, 59% of surveyed directors think the topic should be a fixed point on the board's agenda, while 41% disagree. In practice, the topic is occasionally (= twice or fewer times per year) discussed on the board level among a majority of respondents (52%). 26% have ad-hoc discussions if the situation (an incident, reporting, an investment) calls for it. A smaller group tackles the subject three or more times per year (19%) or at every board meeting (3%).

Breaking these frequencies down by organisation type, the option to tackle the topic more than twice per year increases among large unlisted companies, public organisations, or listed companies, which is logical as these often face regulatory requirements. Even among these larger organisations, putting the topic on every board meeting is extremely rare, which makes sense as it might not be needed to overburden the board agenda if there are no particular or pertinent cybersecurity updates to report on the board.

Company size	Frequently (at every meeting)	Never	Ad-hoc	Rarely (once a year or less)	Occasionally (at least twice a year)	Regularly (more than twice a year)
Small + Medium-size unlisted + social/non-profit	2,86%	2,86%	8,57%	5,71%	14,29%	11,43%
Public organisation + Listed			2,86%	2,86%	8,57%	11,43%
Large unlisted company			2,86%	8,57%	2,86%	14,29%
Total	2,86%	2,86%	14,29%	17,14%	25,71%	37,14%

Only a minority of 24% is pleased with the lower frequency the topic appears on the board's agenda. Nearly one third (31%) is not pleased, and the remaining 45% has mixed feelings about the frequency.

In companies that have subcommittees, the topic of cybersecurity is most often an agenda point on the risk committee and/or the audit committee, or on a dedicated technology-focussed committee if there is one. On **audit committees,** the topic mostly features on an ad-hoc basis or on an occasional basis of at least twice per year (25%). On **risk committees** the topic features more frequently, ranging from every meeting (28% of the cases) to more than twice per year (22% of the cases). Finally, it is also logical that if a company created a **dedicated information security** committee (or similar), the topic is treated very frequently. 42% of these debate the topic more than twice per year, and 25% at every meeting. The topic rarely features on the agenda of the **nomination committee** except ad-hoc, which is logical as the committee will only have this on the agenda if there is a specific appointment or remuneration discussion related to cybersecurity staff.

Frequency of receiving information

Directors can also receive information about cybersecurity-related matters outside of board meetings. Only 14% is pleased with the frequency of information updates, and a sizeable group of 31% is not pleased with the frequency they receive cybersecurity information outside of board meetings. The remaining 55% is on the fence regarding the frequency of information updates.

Cybersecurity framework

A cybersecurity framework typically includes policies, standards, guidelines, best practices on how to manage cybersecurity and a description of the roles and responsibilities of various internal stakeholders including board level.

A large group of directors serves in companies that either have a cybersecurity framework in place (42%) or are in the process of constructing one (21%).

Of those that have a cybersecurity framework, 75% scores it as very effective or even extremely effective (12.5%). Only a small minority (6%) sees it as only moderately effective. (6.5% has no opinion.) No one scored their framework as 'slightly' or 'not at all' effective.

Cybersecurity audits or assessments

Large groups either conducted a cybersecurity assessment (32%) or cybersecurity audit (29%) in the past 12 months, either done by an internal department / internal audit or through an external audit or independent third-party assessor, while 5% signals an audit or assessment is planned or ongoing. A sizeable segment of 26% has not conducted any cybersecurity audits or assessments in the past year or does not know of one (8%).

Looking at the distribution of these options within different kinds of companies, the absence of an audit or assessment is mostly (and unsurprisingly) situated among smaller to medium-sized companies or non-profits, although there is a respectable group among these that did conduct a cybersecurity assessment or audit the past year.

Among more regulated companies, cybersecurity assessments are more frequent in unlisted large companies, whole audits are more frequent in public or listed companies. Some of the latter have not done any audit or assessment in the past year.

	Assessment conducted past 12 months	Audit conducted past 12 months	Audit or assessment currently planned or ongoing	Don’t know	No audit or assessment conducted past 12 months
Small + Medium-size unlisted + Social/non-profit	19%	19%		12%	50%
Large unlisted company	56%	33%	11%		
Public organisation + Listed	20%	50%	10%		20%

Cybersecurity Insurance

Finally, besides all the plans and frameworks for the cybersecurity, having an insurance policy for these risks could be considered and it is important that directors are aware if their organisation has any cybersecurity insurance and what the coverage actually is. 42% report having a cybersecurity insurance policy and 8% is considering it. Nevertheless, 35% have no cyber insurance, and 16% have no opinion on the issue.

As a side comment, it is highly recommended that directors review the professional director liability insurance also in the context of cybersecurity incident liability.

Governance maturity levels of cybersecurity

Cybersecurity governance can be achieved in practice by having a cybersecurity champion on the board, by addressing it in existing subcommittees or a dedicated committee, or by fully integrating the topic throughout the governance structure. This director will, as cybersecurity champion, watch over the regular presence of cybersecurity topics on the agenda but will also help other directors with explaining and understanding specific cybersecurity topics before a decision is made at the board level.

While it is tempting to state that fully integrating the topic in all governance institutions is the highest level of maturity, there is no strict hierarchy between these different ways of governance, as there is no one-size-fits-all all approach for different organisations.

In almost 22% of all surveyed organisations cybersecurity is not formally embedded at all in the governance structure of the organisation, which cannot be considered a good practice. As shown in the table below, this practice is more prevalent among many smaller unlisted companies, medium-sized unlisted companies, and social/non-profit organisations. Other companies of this group prefer to embed cybersecurity governance through the use of a cybersecurity champion.

Public and listed companies prefer to address the topic in one of the existing committees (risk, audit), sometimes in combination with a cybersecurity champion. Finally, large unlisted companies also veer towards having a cybersecurity champion on the board.

	Not formally embedded in the governance structure	Addressed in one existing committee	Distributed across multiple committees	Dedicated "InfoSec" committee	Cybersecurity champion	Fully integrated
Small + Medium-unlisted + Social/non-profit	17,39%	2,17%	0,00%	2,17%	13,04%	4,35%
Public + Listed	0,00%	17,39%	2,17%	0,00%	8,70%	6,52%
Large unlisted	4,35%	6,52%	0,00%	0,00%	8,70%	6,52%
Total	21,74%	26,09%	2,17%	2,17%	30,43%	17,39%

5. Conclusion

As a strategic topic, cybersecurity is viewed as critical in protecting the internal and external organisational processes, data, and the organisation's reputation today and tomorrow, but external pressures from regulators and customers also rank highly. We observe growing pressure throughout industry value chains from customers to the third-party suppliers for a variety of reasons (including the regulations they have to follow) to consider cybersecurity as a critical component in strengthening companies' operational resilience.

- Cybersecurity is a critical component and should be part of the strategic and monitoring roles of the board.
- Strive for a balanced fit between your governance maturity level in cybersecurity and your organisation's activities, size, exposure to risk, likelihood of incidents, and the size of possible impacts.
- Anticipate risks by developing incident plans, clear frameworks of responsibility, and conducting audits or assessments.
- Put the topic on the board's agenda at least twice per year, with ad-hoc treatment on a needs-be basis.
- Remain knowledgeable on current and upcoming regulations, new sudden technological developments, urgent ad-hoc issues, or to check whether the governance framework is still up to date by putting this topic regularly on the agenda.
- Organise training and courses at a frequency and the content required (e.g. companies falling under NIS2 or other legislative frameworks such as the product liability directive). For example, essential and important entities falling under the NIS2 Directive are obliged to hold training for their board members regularly, and encourage similar training for the employees.

Annex A: Cybersecurity information sources

We advise directors to consult the following external objective sources with practical schemes and tools relevant to directors.

- https://safeonweb.be/en
- https://ccb.belgium.be/en
- https://www.cyfun.be
- https://atwork.safeonweb.be/tools-resources/policy-templates
- https://www.enisa.europa.eu/

Annex B: Regulations that affects cybersecurity decisions and monitoring responsibilities

- EU NIS2 directive: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive Are you an *important* or an *essential* business in Europe?
- EU AI Act: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai Are you in a high-risk activity or a limited-risk category?
- EU Cyber Resilience Act: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act - *Will you still be able to sell and maintain your technology-enabled products in the EU?*
- EU CSRD: https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en#legislation - *Is your cybersecurity service provider in your scope 3 emissions?*
- DORA - Digital Operational Resilience Act (DORA) - European Union (europa.eu)

Annex C: Examples of published (Belgian) cybersecurity incident cases (alphabetical)

- Asco https://www.computable.be/2020/07/14/hoeveel-kostte-de-cyberaanval-bij-asco/
- AZ Herentals https://www.numerikare.be/nl/nieuws/datalek-in-az-herentals.html
- City of Antwerp https://www.antwerpen.be/info/63906c7a1477455f97247a95/impact-op-de-dienstverlening
- BELNET https://www.vrt.be/vrtnws/nl/2021/05/04/cyberaanval-op-overheidswebsites-tax-on-web-even-onbereikbaar/
- CRELAN https://www.brusselstimes.com/36335/belgian-bank-crelan-hit-by-a-70-million-eur-fraud
- Duvel brewery https://www.vrt.be/vrtnws/nl/2024/03/07/productie-duvel-moortgat-in-puurs-sint-amands-opnieuw-opgestart/
- FOD Binnenlandse Zaken https://www.vrt.be/vrtnws/nl/2021/05/25/binnenlandse-zaken-vermoedelijk-gehackt-door-chinese-hackers/
- Picanol https://datanews.knack.be/nieuws/en-toen-lag-alles-stil-wat-kunnen-we-leren-uit-de-ransomware-aanval-op-picanol/
- Stad Diest https://www.diest.be/stadsdiensten-gehackt
- Zorgnet Limburg https://limburg.net/nieuws/de-impact-van-de-cyberaanval