Towards a cyber governance maturity model for boards of directors

Professor Basie von Solms
Centre for Cyber Security
University of Johannesburg
Johannesburg, South Africa

Keywords
Cyber Security, Boards, Directors, Maturity Model, Cyber Governance

Abstract

Cyber Security, and specifically the lack thereof, has become a serious head ache for Executive Management and Boards of Directors of companies. Cyber Governance has clearly established itself as an integral part of good Corporate Governance, and the challenge to Boards of Directors is to get a good handle on these cyber risks to their companies. The purpose of this paper is to present a Cyber Security Maturity Model for Boards of Directors of companies. The Model will determine the cyber maturity (understanding, awareness and knowledge level) of the Board as a whole as far as cyber related aspects are concerned. To determine the cyber maturity of the Board as a whole, the cyber maturity of each Board Member will be determined individually, and the results will the aggregated to reflect the maturity of the Board as a whole. The final results will then reflect how well the Board understands their accountability and responsibility towards the cyber risks arising from their company's use of Cyber Space, and how prepared they are to address these risks.

Introduction

There can be no doubt that cyber issues have risen to the top of the management structures of many companies, and are now expected to be a standing item on Board agendas. It is widely acknowledged and accepted that managing cyber risks, which we call Cyber Governance, has become an integral part of Corporate Governance Boards of Directors must therefore be able to understand cyber risks and act accordingly and cannot claim ignorance or a lack of knowledge. However, in many cases, Board members are not necessarily prepared for these cyber responsibilities. One important reason for lack of preparedness, is the fact that few real measurement models exist which the Board can use to get a handle on how well cyber aspects are governed in their companies.

This paper presents such a measurement model - a model which can help to determine the cyber maturity level of a Board to help prepare such a Board better for its accountabilities and responsibilities.

In paragraph 2 we will provide a general overview of the present risks related to using Cyber Space in a company, and in paragraph 3 we will investigate literature related to the present commitment of Board of Directors as far as Cyber risks are concerned.

Paragraph 4 will provide a brief overview of the idea of a maturity model, and paragraphs 5 and 6 will introduce the Categories of our Maturity Model, i.e. what do we want to measure with the Model.

In Paragraph 7 we introduce our Maturity Levels.

Paragraph 8 provides the core of the Model, i.e. what must be satisfied for every Category to be on a specific Maturity Level – we call these the Indicators.

The challenge after having presented the full Maturity Model in paragraph 8, is the operational application and implementation of the Model. This is investigated in paragraph 9, where an individual self-assessment approach is proposed.

Paragraph 10 describes this individual self-assessment approach for a part of the Model.

In paragraph 11 some references are made to potential legal implications, and paragraph 12 provides a Conclusion.

We start with an overview of the cyber risk landscape.

2 . 'Cyber Risk – A Severe and Present Danger'

Risk management in a company has always been an important, if not the most important, item on the agendas of the meetings of Boards of Directors. Risk Management is a core component of Corporate Governance, and Corporate Governance is the main responsibility of the Board of Directors. The types of risks getting the attention of Board members have traditionally been very stable in the sense that they cover the well-established types of risks encountered by a company. Top of the list is probably financial risks, with others like human resources, competitors, brand name, legal compliance and many more. Managing Information Security risks had for many years been an important risk, but did not receive so much attention on Board level as the traditional mainframe environment was well-secured with dedicated and well-secured networks where used. However, the Internet, the multiplicity of systems using the Internet and the immense level of interconnectivity of such systems, has changed all that sense of security, and introduced a totally new form of risk – that of using Cyber Space. Literature clearly indicates that in the last few years, the risk of venturing into and transacting in Cyber Space has become one of the major risks to be handled by companies of all sizes. Cybercrime has become the one of the biggest forms of crime internationally and compromises of companies' and countries' IT systems have become a common occurrence.

International reports list cyber risks as amongst the top risks which must now be managed. The 2014 Global Risk Report of the WEF (WEF, 2014) lists cyber-attacks amongst the top 5 Global risks in terms of likelihood, and critical information infrastructure breakdown also amongst the top 5 Global risks in terms of impact.

A few supporting quotes are:

'Cyber risks: A severe and present danger. Cyber Security is now a persistent business risk' (PWC, 2015).

'Global finance pros pick cyber risk as number-one worry' (Erin Ayers. 2015)

With this very severe and present danger to companies, there is also no question about who is accountable and responsible for this new form of cyber risks – the buck is squarely on the table of the Board of Directors. As can be seen from the quotes above, and many more, Cyber Risk Management is now as important as Financial Risk Management, Brand Name Risk Management and more, and Boards are accountable.

'Cybersecurity in the Boardroom: The New Reality for Directors' (NYSE, 2015) and 'Cybersecurity and Director and Officer Accountability' (Frances Floriano Goins, 2014) are but two of many such documents holding Directors accountable. Some looming court cases against Directors of for eg Target (Frances Floriano Goins, 2014) prove this accountability.

Having now established the importance of Cyber Risk Management and Cyber Governance in general, as well as the level of accountability, it is interesting to investigate the level of acceptance of this risk by Boards of Directors.

We will do that in the next paragraph.

3. How committed are Boards to Cyber Risk Management

Literature provides many ideas and comments about this aspect, but for this paper, we refer to the representative Global State of Information Security Survey published in 2015 by PWC

(PWC, 2015). This survey was conducted on a global basis and the results based on the responses of 9700 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and Directors of IT across more than 154 countries.

The results are an eye opener in the light of the discussion in the previous paragraph.

The Survey concludes (p 28):

'.. organisations clearly have not elevated security to a Board-level discussion. We know because we asked. Only 42% of respondents say their Board actively participates in the overall security strategy and 36% say the Board is involved in security policies. Just 25% say Boards are involved in review of current security and privacy threats. At most organisations the Board of Directors does not participate in key security activities'.

Many reasons are offered why this worrying state exists. Literature identifies several, for e.g.

Many Boards see Cyber Security as a technical matter to be handled on lower levels than the Board

Cyber matters, if presented to the Board, are often concentrating on technical aspects (jargon?) losing the Board members

Many Boards do not realize or understand the strategic risk to their companies caused by cyber risks

Boards do not always understand that Information and Cyber Security Governance is an integral part of their Corporate Governance responsibilities

There exist very few benchmarks against which the level of cyber involvement of a Board can be measures

No real comprehensive (self-assessment driven) maturity model exist which can help a Board to self-assess their level of cyber accountability

It is specifically the last bullet point above which is the main objective of this paper - to present a Cyber Security Maturity Model for Boards of Directors (CSMMBoD).

The purpose of the Model is to determine the maturity of the Board as a combined body of members. This will be to help Boards to self-assess the Board as a body as far as their knowledge and understanding of the impact of Cyber Risks on their company are concerned.

Generically, the Model will be indicated as the CSMMBoD.

The next paragraph will provide a brief introduction to the concept of Maturity Models.

4. The concept of a Maturity Model (MM)

There are different approaches on which maturity models are built. We will not review all these approaches, but choose one which is easy to understand and easy to use.

Firstly, of our model will have a set of Categories. These Categories can be seen as the 'aspects' for which maturity is to be determined, or 'what the MM measures'.

Secondly, for every Category, there will be a number of Maturity Levels (MLs) indicating the progression of maturity for the specific Category.

Thirdly for every Category in every Maturity Level, there will be a set of Indicators which will indicate what the body under investigation, in our case the Board, must conform to in order to be on the specific ML for the specific Category.

Categories will indicate 'what the model measures in terms of maturity'. We discuss that in paragraph 5.

5. The Categories of the CSMMBoD

As stated above, the Categories of a Maturity Model I indicate 'what the model measures in terms of maturity'. As far as Boards are concerned, many Categories can be defined – however we stated earlier that we want to use ‘businesses speak, i.e. use terminology which can be digested by non-technical Board Members.

In paragraph 3 we referred to the PWC Global State of Information Security Survey of 2015, which provided some results in terms of Boards’ involvement as far as cyber aspects are concerned. In determining these results, the PWC Survey used 6 criteria which were:

5.1 Security Budget
5.2 Review roles and responsibilities of security organization
5.3 Security Policies
5.4 Security Technologies
5.5 Overall security strategy and
5.6 Review of current security and privacy risks.

These 6 criteria provide a very good summary of what Board members should be aware of and knowledgeable about, and we really think this is a starting point for determining the Categories of our Model. We will adapt these criteria, drop some and add some more. Our list of Categories will be:

Category 1: Understanding the strategic role of Cyber Risk in the company
Category 2: Understanding and providing guidance on the Cyber Strategy of the company
Category 3: Understanding and reviewing the Cyber Security budget for the company
Category 4: Understanding and evaluating the Cyber Security policies of the company

Of course, we can add many more, but again it will just make the Model more complex. Future versions of the Model will most probably expand on this Version 1 and add more Categories and maybe even more Maturity Levels.

Before we formulate the Indicators for each of these chosen Categories, we will first provide a short motivation for each Category.

7. Our Maturity Levels

We will use the following 4 MLs:

ML 0: Nothing exists at all
ML 1: Very Basic position
ML 2: Progressed position
ML 3: Stable position

The names given to the different MLs are not really important, as long as a higher ML indicates a progression from the lower ones.

We also limit our Model to 4 levels, although many maturity models use 5 or 6 levels. As this is Version 1 of the Model, we want to keep it simple and depending on the success of the Model, levels may be increased.

With our Categories and Maturity Levels now in place, we can define the Indicators (Is) required for each Maturity Level for each Category. We will not define any Indicators for ML 0, as that as seen as a situation which cannot even be evaluated in any way.

8. Formulating the Indicators for every chosen Category

8.1 Category 1: Understanding the strategic role of Cyber Risk in the company

ML 1: Indicator 1: Board Members are aware the company makes use of Cyber Space and some Board members are Cyber Security aware in the sense that they realize that using Cyber Space can cause risks to the company. There is no general understanding of the wider strategic impact of the company’s cyber based systems and no general understanding or appreciation that managing cyber risks is part of their Corporate Governance responsibilities.

ML 2 : Indicator 2 : A significant number of members understand that the company is exposed to Cyber risks, and understand that such risks, if materialized, can cause the company serious harm, They also understand that they have a Corporate Governance responsibility and accountability to manage such risks.

Indicator 3: A significant number of members understand the strategic consequences if some of these risks should materialize, and the impact it can have on the image and brand name of the company

Indicator 4: Most members understand the value of the cyber assets of the company (customer/client/patient) data, the privacy of such data and the legal consequences if such cyber assets are compromised.

ML 3: Indicator 5: The majority of members understand their Corporate Governance responsibility and accountability towards cyber risks in the company

Indicator 6: The majority of members understand the types of cyber threats which can arise against the company and the strategic impact it can have on the company

Indicator 7: The majority of the members are able to appreciate the concept of cyber crime

Category 2: Understanding and providing guidance on the Cyber Strategy of the company

ML 1: Indicator 1: The members had been briefed on the Cyber Strategy of the company and how it fits into the corporate strategic strategy

Indicator 2: Some members have some idea of how the materialization of cyber threats may impact the company and that if the company is cyber compromised, it may have serious consequences

ML 2: Indicator 3: Most of the members appreciate the dependence of the company's use of Cyber Space and the way the company's products use Cyber Space

Indicator 4: Most members also understand what cyber risks are, and what type of compromise and exposure such risks can cause to the company

Indicator 5: Most members are knowledgeable about the state of Cyber Security in the company as compared with peer companies.

ML 3: Indicator 6: Several members are knowledgeable enough to constantly question the state of protection of the company's exposure to Cyber risks and question the value and success of cyber security countermeasures

Indicator 7: Members can evaluate the cyber countermeasures proposed for new systems to be rolled out

Indicator 8: At least one member has made a study of Cyber Security countermeasures and can be seen as a reasonable expert in this area

Category 3: Understanding and reviewing the Cyber Security budget for the company

ML 1: Indicator 1: Members provide very little input to the cyber component of the Information Security budget of the company

ML 2: Indicator 2: Some members are able to ask informed questions about the cyber component of the budget

ML 3: Indicator 3: Some members are knowledgeable enough to query some expenses in the cyber component and suggest alternative solutions.

Category 4: Understanding and evaluating the Cyber Security policies of the company

ML 1: Indicator 1 : Members realize that corporate Cyber Security related policies and procedures are important, but do not really have an understanding of the importance of corporate cyber related policies and the role such policies play in the company

Indicator 2: The members had been briefed on what cyber related policies and procedure do exist in the company

Indicator 3: Members do not realize their Corporate Governance responsibilities towards overseeing the existence and compliance to such policies

Indicator 4: No real reporting mechanisms exist to report the level of compliance/non-compliance to cyber related policies

ML2: Indicator 5: Some members understand the crucial importance of such policies and the oversight and compliance enforcement of such policies

Indicator 6: Some form of reporting mechanisms exist to report the level of compliance/non-compliance to cyber related policies

Indicator 7: Some members realize that they are as responsible as all other employees to comply with all such cyber related policies and procedures

ML3: Indicator 8: Some members are knowledgeable enough to know what cyber related policies should exist in the company and can also evaluate existing policies in terms of peer and best Indicator comparisons

Indicator 9: A comprehensive set of metrics exist by which the Board can determine compliance to such policies.

The operational application of this Model is a challenge which has to be investigated to ensure that the Model can be applied as easily and hassle-free as possible. That aspect is discussed next.

9. The Operational application of the Model

The normal way in which such a Maturity Model is operationally implemented is through the involvement of a facilitator which will use sets of questions and supporting material, to determine the answers. In the case of our model, that may cause problems because of the way the Indicators are formulated.

One approach is for the facilitator to have a session with the Board as a whole, and (try to) get answers related to the different outcomes of the Indicators. That may take a lot of time, and it will be difficult to get objective answers from Board members when they are questioned in a group.

Another approach is for the facilitator to have meetings with individual Board members and then combine the results to get a Board-wide view. This involves a lot of duplication and needs the availability of such members whose time generally is at a premium.

The best approach is possibly an adaption of the second approach mentioned above. If the Model is 'individualized' in the sense that a Board member can do a self-assessment (anonymous if so chosen) in his/her own time without the facilitator present, the whole process can be simplified. The facilitator can then receive all the self-assessments and combine that and create the Board-wide result.

This last approach is the one we will be using for the operational implementation of our Combed.

In the next paragraph we 'individualize' the model - the Indicators are phrased in terms of a personal individual evaluation. Every Indicator now has a tick box where the Board member can indicate a YES, NO or UNSURE. Completing the full evaluation on this basis will not take more than 15 minutes.

However, as there is a length restriction on this paper, we only illustrate the questions in Category 1. The full model can be found in (von Sols, 2015).

10. The individualized Operational evaluation

10.1 Category 1: Understanding the strategic role of Cyber Risk in the company

ML 1: Indicator 1: I am aware the company makes use of Cyber Space and I am Cyber Security aware in the sense that I realize that using Cyber Space can cause risks to the company. I do not really have an understanding of the wider strategic impact of the company's cyber based systems and no general understanding or appreciation that managing cyber risks is part of my Corporate Governance responsibilities.

YES NO UNSURE

ML 2: Indicator 2: I understand that the company is exposed to Cyber risks, and I understand that such risks, if materialized, can cause the company serious harm. I also understand that I have a Corporate Governance responsibility and accountability to manage such risks.

YES NO UNSURE

Indicator 3: I understand the strategic consequences if some of these risks should materialize, and the impact it can have on the image and brand name of the company

YES NO UNSURE

Indicator 4: I understand the value of the cyber assets of the company (customer/client/patient) data, the privacy of such data and the legal consequences if such cyber assets are compromised.

YES NO UNSURE

ML 3: Indicator 5: I understand my Corporate Governance responsibility and accountability towards cyber risks in the company

YES NO UNSURE

Indicator 6: I understand the types of cyber threats which can arise against the company and the strategic impact it can have on the company

YES NO UNSURE

Indicator 7: I am able to appreciate the concept of cyber crime

YES NO UNSURE

11. Combining the Individual Self-assessments

Paragraph 10 is basically a duplication of part of paragraph 8 where the only difference is the individualization/personalization of the relevant Indicators.

The facilitator can actually start off by giving the full Board a brief overview of the Model and an explanation of the Individual Self-assessment form. The self-assessment can be done on a mobile device like a smart phone or tablet, and on completion, sent to the facilitator. Of course, such devices and the transmission of the data should be implementing a high level of security, as the data can be very sensitive.

On receipt of the completed self-assessments, the facilitator can combine the results to produce answers to the Indicators as defined in paragraph 8.

These Board-wise results can then be reported to the Board and corrective actions can be decided on.

11. Legal implications

Discussing the Model and operational implementation with different Board members, it became clear that such members have a problem in completing such a self-assessment. This worry centered on the fact that by doing the self-assessment, they may indicate that they are not aware of the different aspects related to cyber in their companies, and may be on ML 1, or even ML 0 in many cases. If their company is now compromised by a significant cyber-attack, and sensitive information is compromised, it may lead to class action against the company, and maybe the Board members themselves. If their self-assessment results indicated that they are on a low level of cyber awareness, it may be used as aggravating evidence against them which may be very detrimental personally. The general feeling of the few who were asked for their opinion indicates that they would not do such a self-assessment at all.

This aspect was discussed with several legal experts. Their general evaluation is that if the self-assessments are done anonymously, and the anonymous results destroyed immediately after consolidation of the results, what an individual Board members has indicated on his/her self-assessment form, cannot be used against him/her in any way.

This matter however, needs more thorough investigation, as does the legal position of the Facilitator.

12. Conclusion

In this paper a Maturity Model was presented to determine the level of Cyber Governance knowledge of Board Members. The Model used an anonymous form of self-assessment and eventual consolidation of results. Implementing the Model can give Boards of Directors insights into their own understanding and implementation of Cyber Governance.

Some legal consequences however needed to be researched in more detail.

References

WEF, 2014, 'Global Risks 2014, Ninth Edition', http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

PWC, 2015, 'Managing cyber Risks in an interconnected world', http://www.pwchk.com/home/eng/rcs_info_security_2015.html

Erin Ayers. 2015, 'Global finance pros pick cyber risk as number-one worry', http://www.cyberrisknetwork.com/2015/05/13/global-finance-pros-pick-cyber-risk-as-number-one-worry/

NYSE, 2015, 'Cybersecurity in the Boardroom: The New Reality for Directors', (https://privacyassociation.org/news/a/cybersecurity-in-the-boardroom-the-new-reality-for-directors)

Frances Florian Goins, 2014, 'Cybersecurity and Director and Officer Accountability', http://apps.americanbar.org/buslaw/committees/CL996000pub/newsletter/201404/fa1.pdf

Von Solms, SH, 2015, 'Measuring the Cyber Maturity of Board Members', paper in preparation – contact basievs@uj.ac.za