INSTITUTE OF DIRECTORS
SOUTHERN AFRICA

Governing Body's Role in Cyber Resilience

Corporate Governance Network

pwc

Contents

Page

First release date of paper: April 2018

Introduction

"Cyber security" is consistently rated as one of the top risk exposures in the world today and one to which all governing bodies[1] need to pay attention. The risk is real. It is real for all sizes and types of organisations and it has real financial and sustainability impact. The impact of the lack of cyber resilience has included: significant financial loss; litigation; reputational damage and negatively impacted share prices; suspended operational activities and an eroded competitive advantage. Cyber security breaches are also occurring more frequently - most experts now view such events as inevitable - no longer "if" but "when" and due to the pervasive nature of technology this means very few organisations are exempt. Most governing body members are aware of the issue but in many instances they have not provided adequate direction to effectively guide their organisations in this matter.

Purpose

Governing bodies need to guide and direct their organisations in addressing this risk. They need to set the direction their organisations should take; delegate responsibilities to management; review and approve management's research, responses and plans; and oversee and monitor the operational results. Most importantly, governing bodies need to ensure that their activities and decisions result in a continually and rapidly improving cyber resilience competency:

"Cyber resilience - the ability of an enterprise to anticipate, withstand, recover from, and evolve to improve capabilities in the face of adverse conditions, stresses or attacks on the supporting resources it needs to function[2]."

This paper sets out some practical considerations and steps governing bodies can take to demonstrate and exercise their fiduciary duties relating to cyber resilience.

The governing body's oversight role

The National Association of Corporate Directors (NACD) latest edition of its Director's Handbook on Cyber-Risk Oversight[3] provides the following 5 principles to assist governing bodies further understand their oversight role of cyber risks from an international best practice perspective:

1) *Understand and approach cyber security as an organisation wide risk management issue, not just an IT issue.*

2) *Understand the legal implications of cyber risks as they relate to the organisation's specific circumstances.*

3) *Have adequate access to cyber security expertise and give cyber risk management regular and adequate time on governing body meeting agendas.*

4) *Set the expectation that management will establish an organisation wide risk management framework with adequate staffing and budget.*

5) *Management discussions should include identification of which risks to avoid, which to accept and which to mitigate or transfer through insurance.*

1 Governing body as defined in King IV to mean "the structure that has primary accountability for the governance and performance of the organisation. Depending on context, it includes, among others, the board of directors of a company, the board of a retirement fund, the accounting authority of a state-owned entity and a municipal council."
2 The MITRE Corporation, https://www.mitre.org/
3 National Association of Corporate Directors (NACD), Director's Handbook on Cyber-Risk Oversight, 2017 (revised edition), accessible via www.nacdonline.org

The Global Network of Director Institutes[4] further recommends that the governing body should extend the above principles to include the following in regards to its oversight of the general effectiveness of the people, processes and technology within the organisation:

a) *Consider placing cyber security as a specific accountability of one of the executive director's reporting to the governing body (or other executive director which then reports to executive governing body director or who attends meetings as an invitee to provide report back) and as such consider cyber security needs as part of the key functions needing executive director-level attention.*

b) *Should inform themselves of specific operational, reporting, and compliance aspects of cyber security, using at least one recognised framework (as needed, adapted or supplemented) to do so. [Specific reference here to the 5 principle approach above.]*

c) *Consider adding a member with some knowledge of information technology (including digitalisation and cyber security) onto the governing body, specifically in governing bodies of organisations where IT is business enabler and/or is identified as a core competence required due to the type of business or industry in which the organisation operates.*

How should the governing body carry out its oversight role?

The governing body should consider at least the following phases in conducting its oversight responsibilities. The following questions will assist it to assess whether it has adequately considered and integrated the need for cyber resilience into its strategy, risk management and overall thinking.

1. Planning and oversight

A critical part of cyber resilience lies not only in the ability to respond to incidents, but to plan in advance so that they are either avoided or, if they occur, to be able to deal with them in an effective manner.

- Is the tone established at the top appropriate? Do we have a cyber-focused mind set and conscious culture? Does the organisation's culture support or hinder these security efforts? How can the governing body influence the organisation's culture in this regard?
- Is there clear accountability for the responsibility for cyber resilience?
- Does the organisation have a 'map of evolution' that describes its cyber resilience journey?
- Has management developed a cyber-risk matrix, and is cyber risk integrated into the overall risk assessment and management process? See Annexure A for an example of a cyber-risk assessment framework.
- Has the organisation identified the business outcomes to be avoided by a cyber-attack, for examples, the loss of ability to sell its product?
- Have detective and monitoring controls been put into place?
- How does the cyber resilience plan cater for changes in the risk landscape i.e. is it flexible and adaptable?
- Have cyber-attack simulations been planned for?
- Has the organisation identified how a cyber breach would affect its ability to meet it legislative and compliance responsibilities?
- Has appropriate Directors and Officers liability insurance cover been procured? Has cyber liability insurance been included in this cover?
- Has the above been considered for both our own functions as well as services provided by third parties?

2. Monitoring

Having established a plan, the role of the governing body is to monitor how that plan is being executed. In this regard, the following questions may be useful:

- Have we identified what our key cyber resilience metrics are? What will success look like?
- Have there been attacks on the organisation? How have the planned defences worked, what was the root cause of the attack and what remedial procedures have been instituted?
- What was the time frame between when the organisation was attacked and when the attack is identified?
- What have the results of external assessments of the organisation's cyber resilience over the period been?
- Has the organisation effectively allocated sufficient/appropriate resources based on its risk appetite and tolerances?
- Are the management reports we are receiving timeous, transparent and accurate enough to support effective decision-making?

4 Global Network of Director Institutes, Perspective Paper: Guiding Principles for Cybersecurity Oversight, 27 November 2015, accessible via http://www.gndi.org/

3. Responding

The governing body needs to play an active and timeous role in the cyber response plan should there be a cyber-attack/breach. We have seen in recent cases that the time it takes an organisation to respond and communicate with stakeholders after an incident can either break or save an organisation's reputation. Timing is thus key and an appropriate response plan and team needs to be put in place.

- Is there a clear reporting and decision path for actions and communications in response to a cyber-attack/breach? i.e. is there an adequate response plan in place?
- Has a rapid response team been created? Who is on the team and are they aware of their role and responsibilities?
- Does the response plan include notification to the governing body, when governing body involvement is required and activation of the rapid response team?
- What lessons has the organisation learnt from an attack and what remedial actions has been instituted?
- Does the organisation have a cyber-security playbook for responding to an attack, including communications with stakeholders, an understanding of legal and compliance requirements?
- Have the business continuity plans been stress tested?
- How different was the attack from simulations and were the planned responses sufficient to deal with the adverse consequences of the attack?
- Have all required stakeholders been identified, are communication / engagement plans in place, are these plans appropriate in terms of the organisation's risk appetite and tolerances, have we received suitable assurance in this regard?
- Is the governing body sufficiently appraised of recent developments both internally as well as in the external environment, and how have the plans and strategy discussed above been adapted?

See Annexure B for a more detailed guideline on the type of questions which the governing body or applicable governing body committee responsible for IT governance can ask management to illicit the information the governing should be getting.

Conclusion

Cyber security requires an organisation wide plan of action that includes creating a culture in which information security is top of mind and which anticipates and responds to threats effectively and efficiently. Even with the best plans in place, cyber risk cannot be completely eliminated. Breaches are often inevitable, and responses are required to minimise the exposure. The governing body has a duty to ensure the organisation's cyber risk readiness and resilience measures are in place and are substantially minimising the risk exposure.

Being resilient requires those at the highest levels of an organisation to recognise the importance of avoiding and proactively mitigating risks. The governing body is thus responsible for including cyber resilience into the organisational strategy. Cyber security is however only one aspect, and organisations must also develop strategies to ensure durable networks and take advantage of the opportunities that digitalization can bring. An important aspect of cyber resilience is to avoid getting locked into any single approach.

The principles set out above are not intended to be prescriptive. There are various factors that may influence cyber security oversight such as the organisation's industry, location, regulatory environment and culture. The approaches taken will thus vary according to the organisations circumstances and needs, but all governing bodies should find the principles outlined above useful in guiding them in what to consider to ensure their effective oversight and limit the personal liability should negative circumstances occur.

Additional Reading Material

Institute of Directors New Zealand (Inc.), Cyber-Risk Practice Guide: Put cyber security on the agenda before it becomes the agenda, 2017, accessible via *https://www.iod.org.nz/Portals/0/Publications/Cyber-Risk%20Practice%20Guide.pdf*

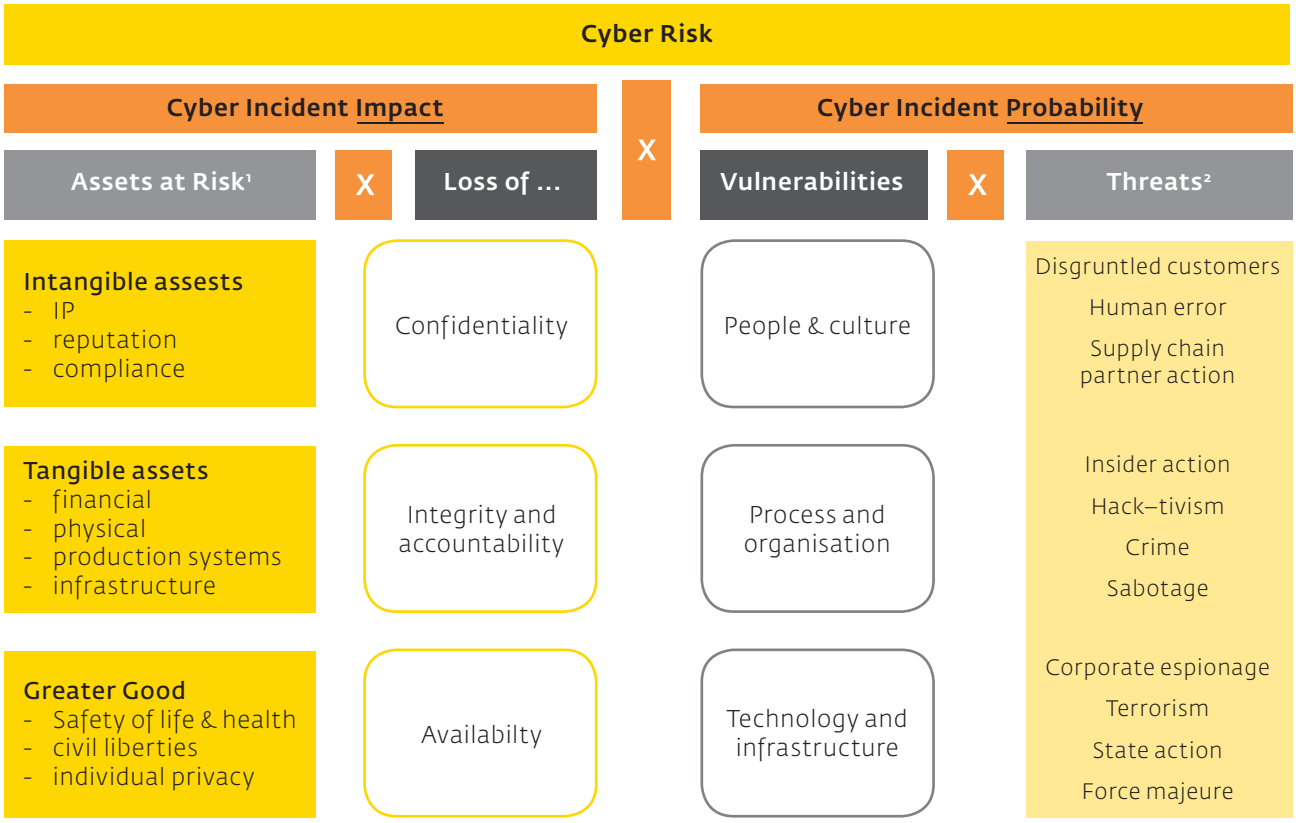
Christophe Veltsos, NACD Publishes Five Cybersecurity Principles Every Board Director Needs to Know, 8 February 2017 accessible via *https://securityintelligence.com/nacd-publishes-five-cybersecurity-principles-every-board-director-needs-to-know/*

John Reed Stark and David R.Fontane, Boards of Directors and Cybersecurity: Applying lessons learned from 70 years of financial reporting oversight, Docket Media LLC – Cybersecurity Docket, 2016, accessible via *http://cybersecuritydocket.com/wp-content/uploads/2016/01/Boards-of-Directors-and-Cybersecurity-Applying-Lessons-Learned-from-Financial-Reporting.pdf*

Annexure A

World Economic Forum: Board Cyber Risk Assessment Framework

The following framework has been proposed by the World Economic Forum to aid Boards in the assessment of cyber risk. Detail on how to use this framework as well as further guidance on the subject can be found in its white paper entitled Advancing Cyber Resilience: Principles and Tools for Boards released on 18 January 2018 via https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards



1 Example for assets
2 Selection of examples, sorted in ascending order of available resources

Annexure B

2nd Level Questions the governing body/committee should consider asking

If the governing body does not receive regular information from management on the organisation's position with regard to cyber risks, it will be difficult for the governing body to provide adequate oversight or to effectively approve management's plans and initiatives. The following are examples of practical questions which the governing body or applicable governing body committee responsible for IT governance can ask management to source information and ensure it understands what is being done within the organisation and ultimately fulfils its fiduciary duty. This is not an exhaustive list of questions but rather provides a general overview of the types of questions or considerations that should be had under each area.

Information Management

1) Have management identified the key assets and what process was followed in their identification?

2) What is the level of interaction of the key assets with the remainder of the business? Has the ecosystem around those key assets been considered from a risk perspective?

3) What is the impact on the organisation of a loss or breach of its information assets?

4) How does managements planned controls consider both internal staff as well as external parties like contractors and third party software providers? What assurance do we have over third party cyber responses?

Cyber Risk Management

1) Is there an organisation wide risk management framework in place with adequate staffing and budget to oversee multiple simultaneous organisational risk events?

2) Has the risk register been updated to include cyber /IT risks?

3) What are the key metrics that are used to assess performance? For example, what is the period between when a breach occurs and when it is detected? How quickly and effectively does management respond to suspected and actual breaches? I.e. how long does it take management to identify and respond to a cyber-incident?

4) Has the organisation's risk appetite and cyber risks been incorporated into existing risk management and governance processes?

5) Is there clearly described and operationalised roles and responsibilities across the cyber risk programme?

6) Does the incident management framework include escalation criteria aligned with the cyber risk program?

7) Does the cyber risk programme address any industry specific frameworks which may be available or applicable?

8) Has the organisation conducted an external benchmark review of its cyber programme? How do our cyber incident responses benchmark to other organisations/best practice?

9) How does our cyber risk program/framework and capabilities align to industry standards and peer organisations?

10) Are stakeholder relationship and reputational risks adequately assessed and do the risk responses adequately meet the organisation's brand promises, and risk appetite and tolerances?

11) Do we have organisation wide education and awareness campaigns established around cyber risks (to all employees, third parties and contractors etc.) – awareness to specific individual job descriptions help staff.

Annexure B (cont.)

Security Management

1) How do you know that our cyber security management system will be effective in the case of an incident?

2) How do you know that our staff know how to and will follow the management policies and procedures to avoid or report a cyber-incident?

3) In the event of an incident how do you know that your plans will work?

4) Are our third parties on board in this regard? How can we be sure that they are kept current with our intentions and plans and will respond appropriately?

5) What are the security risks associated with the use or reliance of any third party contractors or service providers etc.?

Review and Awareness

1) What are the potential, attempted and actual threats experienced by the organisation? The governing body should ensure it receives regular reports on such metrics.

2) Is the organisation able to determine what potential cyber breaches have been prevented?

3) Are changes to the cyber risk landscape regularly monitored or assessed? Is the governing body made of aware of such changes and are processes appropriately reviewed and updated in light of such changes?

4) Are training programmes for employees, governing body members, third party vendors etc. included in the cyber security plan?

Third party or outsourced service providers

1) Do third party contractors have access to our networks and/or information assets? What assurance do we have over third party cyber responses? *[Repeated for completeness]*

2) What are the security risks associated with the use or reliance of any third party contractors or service providers etc. *[Repeated for completeness]*

3) Has management conducted a third party cyber security due diligence?

4) How does management ensure that third party service providers and contractors have controls and policies in place and do they align with the organisation's expectations – specifically in respect of security measures, response rates and notifications?

Cyber Risk Response Plans/ Business Continuity Plans

1) How will managements plan support the organisation's ability to restore confidence after an attack and minimize the business impact?

2) Do we have an incident response plan in place, how often is this tested, has assurance been provided in this regard, how does this plan address the identified risks, how are stakeholders engaged, have thresholds have been put in place in terms of escalations, why were these thresholds selected, what are the various levels of escalation and have differing responses been planned for each level, how are these responses aligned with the identified risks?

3) When was this plan last reviewed or updated?

4) Have we done a dry run to test the effectiveness and efficacy of the response plan in the event of a breach? If so, what were the results of the last test?

5) Does the organisation's business continuity plan include incidents of cyber-attacks?

6) Has the organisation evaluated the effectiveness of its business continuity plan in the context of a cyber-attack?

Annexure B (cont.)

7) Does the current business continuity plan need to be reconsidered and refreshed with these additional considerations?

8) Can we rapidly contain damages and mobilise diverse responses and resources when a cyber-incident occurs?

9) Are there external and internal communications for key stakeholders?

10) Is there adequate awareness and accessibility of the business continuity plans in place?

Budget, Investments and Insurance

1) Is the cyber security budget appropriately funded and is it appropriately covered from an insurance perspective? How will spending allow the organisation to see and anticipate threats, and to quickly recognise when an attack has occurred?

2) Are we focused on and investing in the right things? How do we evaluate and measure results of our decisions/ investments?

3) Does the organisation have adequate cyber security insurance? Is cyber security liability included in the current Director and Officers liability insurance?

Legislative Compliance

1) What are the legal requirements that apply to the organisation – specific regulations, standards and laws? Specifically what is the organisation legally required to do in respect of identified breaches and necessary notifications thereof?

2) What regulator issues, fines and/or penalties should the governing body be aware of?

3) How is the organisation's compliance with legislative and regulatory requirements?

4) How often is compliance with policies, industry standards and regulations assessed? Is this frequency adequate?

5) Is the organisation's disclosure requirements in line with any applicable legislative guidelines/regulations and shareholder's expectations?

Notes

Notes

Paper sponsored by:

pwc

INSTITUTE OF DIRECTORS
SOUTHERN AFRICA

www.iodsa.co.za