Deloitte.

A Namibian Perspective on the Governance of Cyber Security

February 2020

Deloitte.

The Governance of cyber security from a Namibian perspective

Drive your business or get driven out of business

1. Introduction

In light of continued efforts by the Namibian Government to promulgate an effective law that recognises and regulates electronic transactions, cyber security is an emerging topic within the Namibian business environment.

Deloitte Namibia has therefore circulated our annual Corporate Governance Survey to respondents within the public and private sectors of business in Namibia to better understand the governance landscape. A key focus area for governance in Namibia is cyber security and how this is perceived and managed.

Consistent with our findings from the Deloitte Corporate Governance Survey for Namibia for 2019[1], a study estimated the cost of cyber-related incidents in Africa at a staggering US$3.5bn in 2018, a 75% increase from the previous year[2]. According to industry pundits weighing in on the subject, emerging economies are a favourite target of cyber criminals as they are perceived to be the "low-hanging fruit". Moreover, another report found Namibia as a key target in Africa [3].

Information security encompasses details pertaining to the dissemination of information in an organisation, and cyber security is a subset of information security whereby the latter involves the use of Information Technology infrastructure.

"Information security governance is a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organisational resources responsibly, and monitors the success or failure of the enterprise security programme"

- (IT Governance Institute [ITGI], 2006)

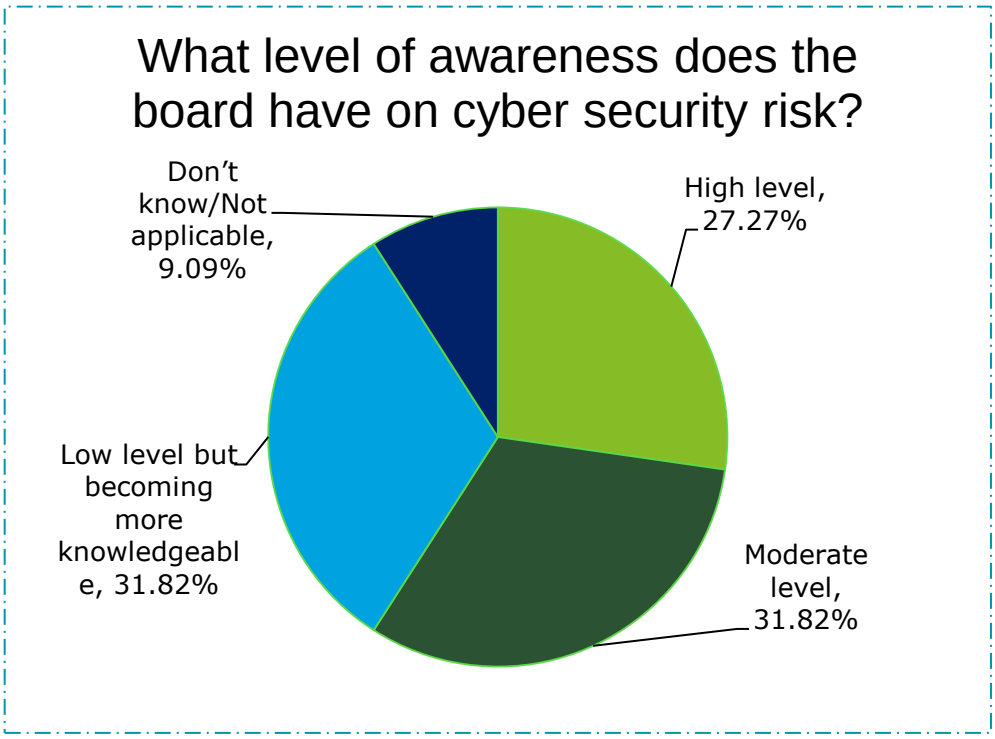
[1] https://www2.deloitte.com/na/en/pages/governance-risk-and-compliance/articles/na_2019_Edition_of_the_Deloitte_Corporate_Goverance_Survey_for_Namibia.html
[2] https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf
[3] http://www.itwebafrica.com/security/513-africa/246563-cybercrime-namibia-most-targeted-country-in-africa

Deloitte.

2. Survey results

2.1 Lack of cyber security awareness

Survey results indicated that our respondents have a moderate awareness of cyber security risk, but in our opinion, this awareness is insufficient: firstly cyber security risk appears to be underrated by Namibian boards and secondly there is a knowledge deficiency regarding the intricacies of cyber security risk, a trend that is replicated in the Deloitte CFO survey 2018/2019[4], where only 44% of the respondents considered cyber-crime a threat to their organisation. This is in sharp contrast to the results of the aforementioned Checkpoint research which clearly indicates that cyber security risk is woefully underrated, and a significant threat to organisations.



[4] https://www2.deloitte.com/na/en/pages/finance/articles/Deloitte-Namibia-CFO-Report-2018-19.html

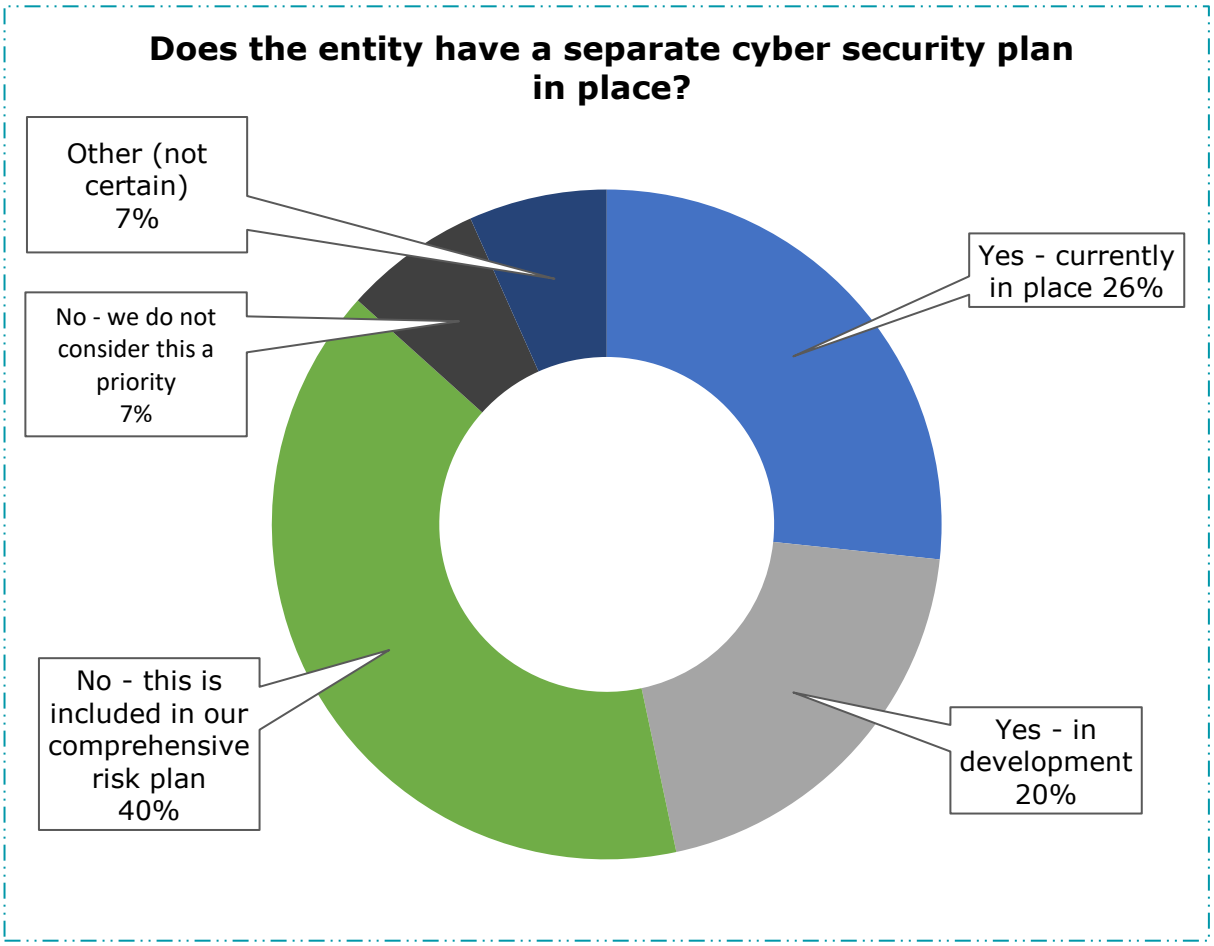
Deloitte.

2.2 Ineffective governance

The main risk areas that the respondents of our CFO survey are concerned about include corruption (74%), fraud (65%), cyber-crime (44%) and staff theft (38%). This, however, does not take into consideration the evolution of crime over the past decade. In the current environment, the majority of operations are performed via electronic means and therefore, crime has likewise evolved to take advantage of those same channels. Consequently, the impact of cyber-crime is neglected disproportionately in light of potential risks and should, we believe, be of a much larger concern for executives in Namibia.

40% of respondents indicated that they do not have a separate cyber security strategy as it is encompassed in the comprehensive risk plan, with the Chief Information Officer (CIO) or Chief Technology Officer (CTO) taking ownership of cyber security. The survey also found that managing cyber security risk is perceived to be the responsibility of IT, with limited ownership lying with the business as a whole. However, we believe that, to the high potential impact of cyber security breaches on the business, this is no longer sufficient and responsibility for the management of cyber security risk should increasingly be a main strategic concern overseen by the CEO and Board on a frequent basis. A key point to realise is that business owns the information that is targeted, exposed, corrupted and/or rendered unavailable, making cyber security a business issue.

Most worrisome to us is that, 14% of respondents do not consider a cyber incident likely or cyber security risk to be a priority. This indicates a potentially disastrous weakness for those companies, their customers, suppliers and staff. In our interconnected world, a single point of weakness could bring down the entire network of relationships and thus cyber security and information security become a pervasive issue to consider at all levels of interaction.



Deloitte.

3. Standards and Recommendation

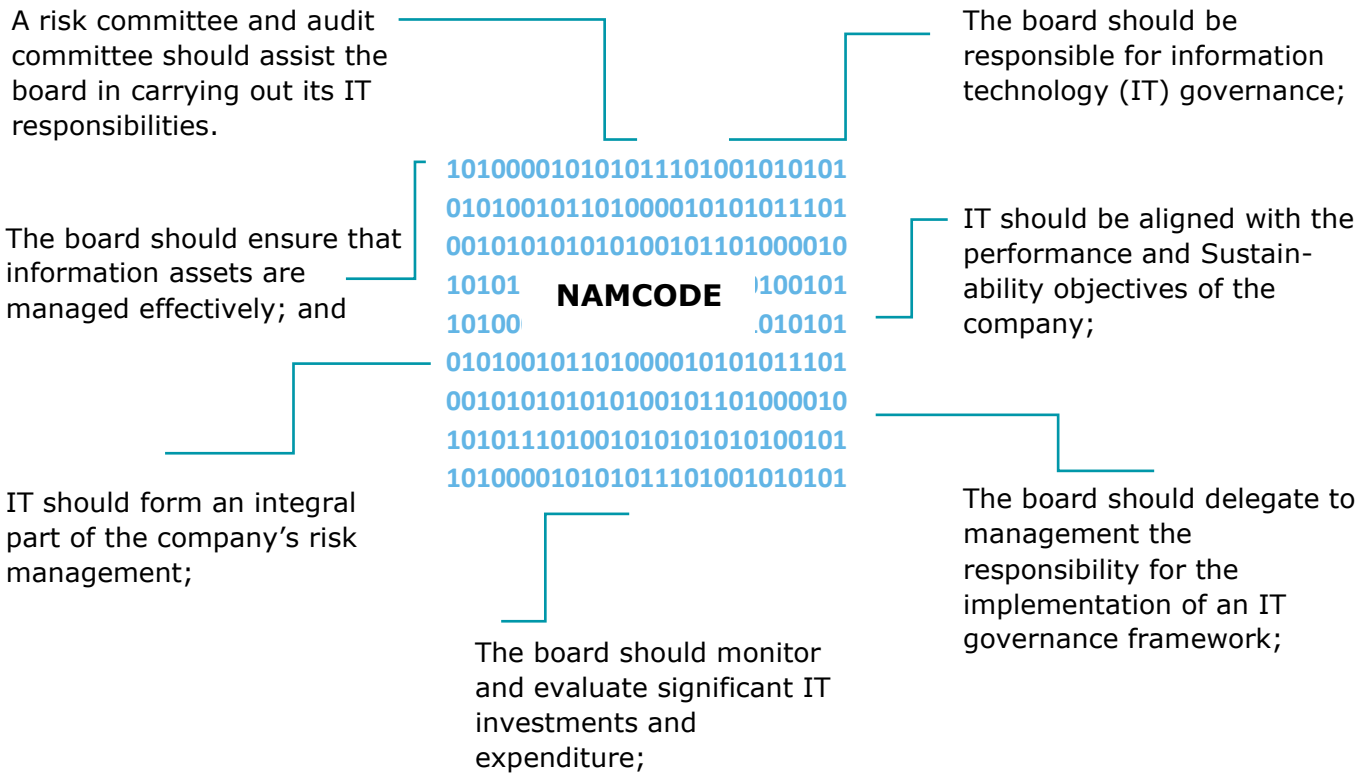
Once an organisation has established the need to address cyber security risk as a key strategic concern, there are several considerations that should be made to develop the correct strategy for the individual entity, which includes:

1. Establishing a risk-based IT governance strategy, taking into consideration various aspects, such as:
   a) The likelihood of threats based on situational awareness,
   b) Incident history in own organisation, industry and country as well as threat intelligence;

2. With reference to best practice standards such as ITIL (etc.), developing a dedicated cyber security strategy and assigning responsibility at the correct levels (i.e. a joint responsibility between the CIO and/or CTO and CEO/COO, with oversight by the Board periodically); and

3. Upskilling responsible individuals, especially at the Board level.

Namibian entities are urged to employ governance guidelines as outlined in chapter 5 of the Namcode (Namibian Code for corporate governance), as follows:



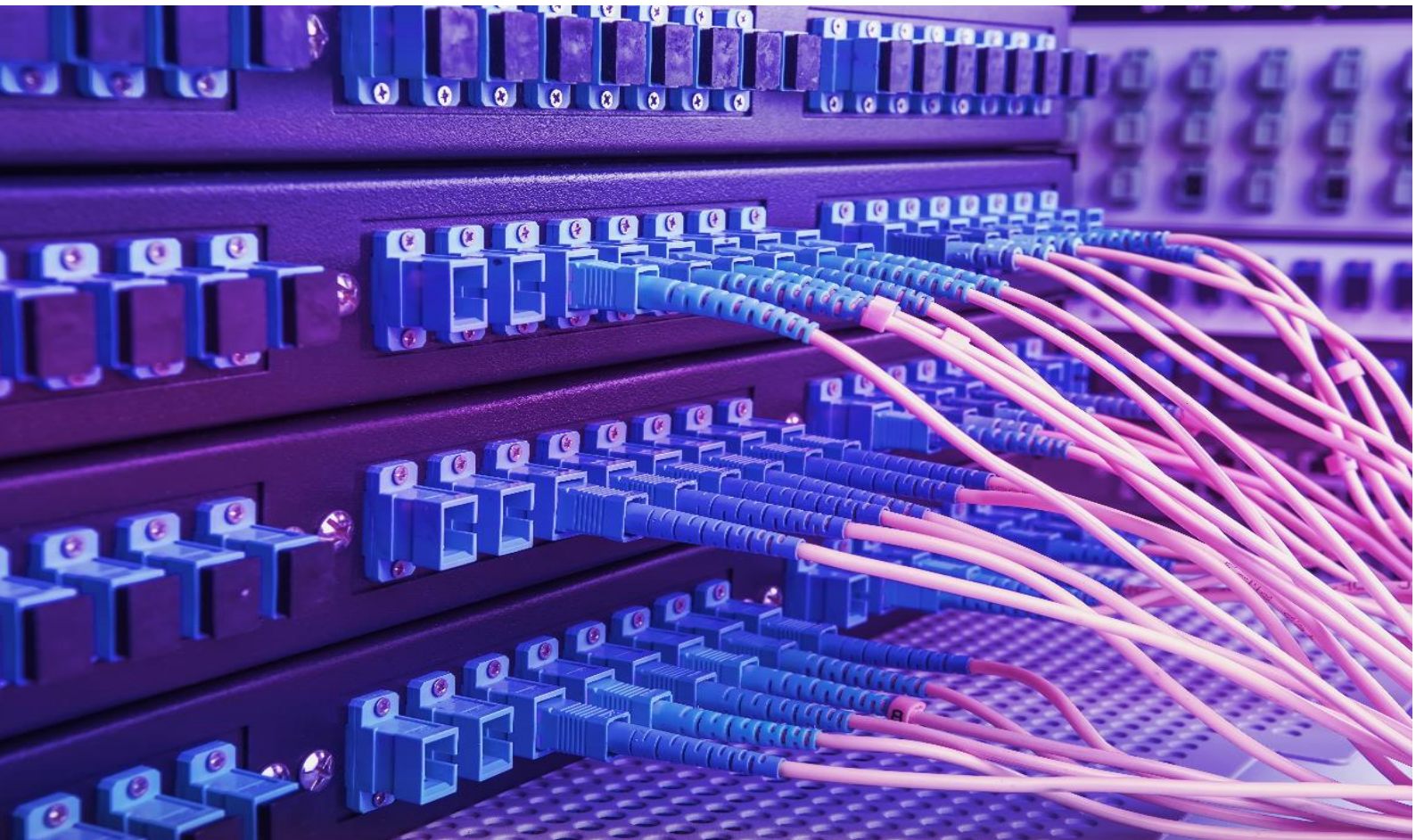
Deloitte.

These guidelines can be tailored to each entity's individual strategy with reference to international best practice standards such as NIST, COBIT, ITIL and ISO and implementation plans can be phased in incrementally, enabling even small companies to make drastic strategic improvements to their cyber security in a short period of time and closing critical gaps.

4. Conclusion

Cyber security should be considered a key business risk and managed pervasively by all levels of the entity from the board of directors down to the lowest level of employees. Appropriately managing cyber security plays a pivotal role in the governance of IT and, therefore the function requires C-suite and executive direction and authority. This is in line with the requirements outlined in the NamCode: Chapter 5 and King IV: under principle 12. Not only does this approach aid the strategic alignment of IT to the overall business but also addresses the notion that cyber security is the sole responsibility of the IT function; a tendency that is evident in the 2019 Deloitte Corporate Governance Survey for Namibia.

In a time when digitalisation may seem to be an appealing business strategy, the effective governance of cyber security will draw the line between driving business and getting driven out of business. Applying the suggested corrective actions and taking full ownership of your digitalisation strategy will enable Namibian institutions and by inference Namibia as a whole to compete more effectively on a global scale and in the long run, yield positive returns for our people.



Deloitte.

5. Contacts

Melanie Harrison

Director

Risk Advisory

Tel: 061 285 5003

Email: melharrison@deloitte.co.za

Nicoline Badenhorst

Manager Risk Advisory

Tel: 061 285 5056

Email: nbadenhorst@deloitte.co.za

Steve Shakadya

IT Audit Consultant

Risk Advisory

Tel: 061 285 5113

Email: sshakadya@deloitte.co.za

Deloitte.