Cyber Risk: Can the organization provide assurance that this has been addressed adequately?!

nCyRisk facilitates the business to assess, manage and monitor its cyber threats and risks measured against an international standard of controls. A standards compliance report can be drawn based on the assessment of controls performed (NIST, ISO, CSF)

As the 21st century progresses, we are seeing rapid growth and global revision in connectivity and digitalisation on a scale never contemplated before. This is, to a large extent made possible by the vast leaps in technology, communication and globalization fueling rapid digitalization and automation.

Without the effective application of suitably designed, configured and implemented risk management tools, techniques and methodologies, effective cyber risk management cannot not be implemented.

Failure to identify, assess, and manage the major cyber risks facing any organization's business model, will most certainly and unexpectedly result in a significant loss of stakeholder value or possibly total failure.

Boards and Senior leadership must of necessity implement processes to effectively and efficiently manage all substantial cyber risks confronting the organization. This can only be achieved using structured methodologies, appropriate tools and technology and best practice implementation by suitably skilled specialists.

When structured methodologies, based on acceptable codes and standards, with integrated tools are correctly applied to Cyber Risk Management, it is possible to provide key individuals with an understanding of critical cyber risk exposures. This facilitates the balancing of expectations and allowing for an increased potential of resilience necessary for survival subsequent to an attack, ensuring uncompromised business sustainability.

It has become imperative that all boards and leadership teams of businesses and organisations have a thorough up to date understanding of their threat landscape and associated controls to ensure the implementation of cyber resilience within their operations.

Cyber Resilience, based on an informed assessment methodology will ensure that :

- Business are adequately prepared for mitigation of the cyber-attack damages
- The most valuable digital and physical assets are adequately secured and protected
- All staff within the organisation / business are educated, informed and trained to prevent attacks but also to effectively respond when attacks occur
- Appropriate and adequate cyber insurance cover is in place at an affordable rate

PRODUCT DESCRIPTION

nCyRisk is a Software as a Service (SaaS) assessment tool that allows the organization to assess the cyber-risk controls that have been implemented.

The nCyRisk process entails:

1. An Asset review, whereby organization categorizes the impact of potential loss of each asset as one of 'Catastrophic', 'Severe', 'Material' or 'Low'.
2. A Threat Environment review, whereby organization identifies the threats to which it is inherently exposed by virtue of its industry and trading environment.
3. A Controls assessment, whereby the organization confirms the application of controls deployed to mitigate threats, together with the related quality and the maturity of their implementation.
4. A listing of Residual Risks for Board and EXCO consumption, encompassing the related assets and threats.
5. The Remediation Action recommended as optimal, to additionally mitigate the risks to which the organization is exposed.

FEATURES

- **Ease-of-use for initial 'self assessment' and set-up**
- **Completeness of 'threats' and controls**
- **Enhances transparency and oversight capability of the governing body**
- **Facilitates quantification of risks for scoping insurance cover**
- **Assurance reports of implemented Cyber Standards**

"There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked!"

- John Chambers CEO Cisco
(BDO Current situation regarding Cyber Security 54th April 2018)