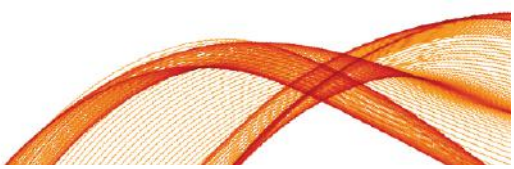
mobius
ACTUALISING CHANGE

CYBERSECURITY
WHERE DO I START?

Version: 1.0
Date: January 2016

TABLE OF CONTENTS



1 INTRODUCTION AND DEFINITION

Cybersecurity is increasingly in the spotlight with daily media reports of organisations that have been hacked by cyber criminals. Not only is the number of hacking incidents increasing, but the net effects on organisations are worsening. A report by the Centre for Strategic & International Studies estimates that cybercrime in South Africa is costing the country approximately R5.8 billion a year.

The era of teenagers hacking and defacing a web site for fun is over. The new era is driven by greed, ideology, politics, terrorism and highly skilled attackers that are focused on stealing trade secrets, committing fraud and disrupting business. The new era is an entire industry of cyber criminals that has access to the resources they require to pursue and achieve their objectives.

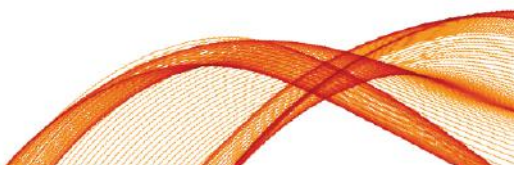
> **CYBERSECURITY** - IDENTIFYING CYBER-RELATED RISKS AND IMPLEMENTING CONTROLS REQUIRED FOR THE PROTECTION OF DIGITAL INFORMATION ASSETS FROM EXTERNAL THREATS, AND BEING ADEQUATELY PREPARED TO DETECT AND RESPOND TO A CYBERATTACK

No organisation can afford to ignore these risks any longer. Organisations must be in a position to not only understand the risks, but to also muster the knowledge and resources required to protect the organisation against cyber-related threats. Management and business leaders must understand the concept of cybersecurity, the associated risks, and how to effectively protect against cyber-related threats.

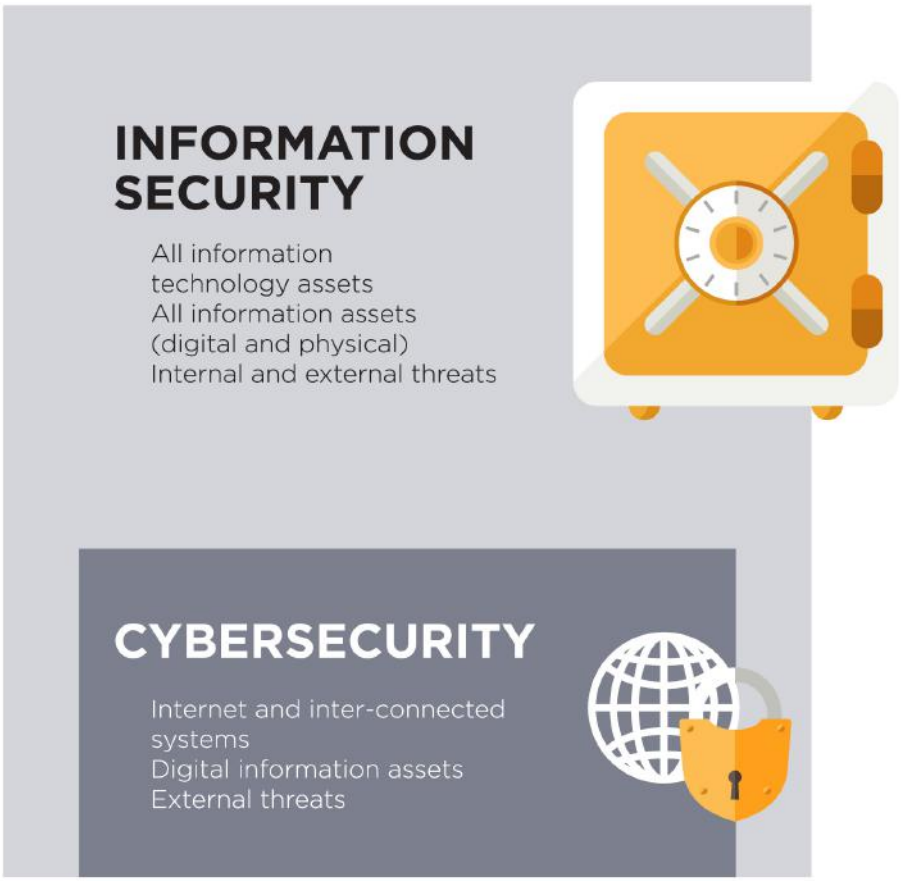
One of the first steps for many business leaders is to gain an understanding of what cybersecurity is and how cybersecurity is different to information security.

Information security is the broad practice of protecting information assets and information technology. The scope of information security includes both digital and physical formats of information, and includes both internal and external threats.

Cybersecurity on the other hand is more specific and narrower in scope. The word "cyber" generally relates to computer systems and the internet. The many definitions of cybersecurity all attempt to explain the scope and focus of cybersecurity using similar themes - internet, cybercriminal, external threat, data and hacking. Cybersecurity can be described as securing digital information and protecting internet facing and interconnected systems from external threats.



As the diagram depicts, cybersecurity should be treated as a subset of, and integrated to, information security.

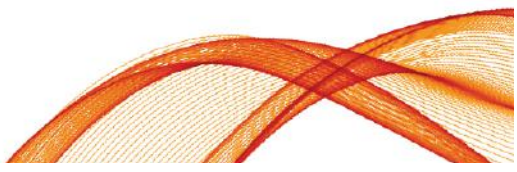


Cybersecurity threats are relatively new compared to traditional information security threats, and organisations have to extend information security practices that will enable them to adequately detect, prevent and respond to these new and advanced threats. This includes implementing new controls, updating the organisations information security capability to deal with cyber-related threats, and most importantly understanding the risks. The new capabilities that are required are not sufficiently addressed by traditional information security management practices.

As part of South Africa's response to the growing cyber threat, Cabinet approved a National Cybersecurity Policy Framework in March 2012 which seeks to centralise the coordination of cybersecurity activities, strengthen intelligence collection, confront emerging cyber threats and foster cooperation and coordination between government, public, and private sectors. Further to this, The Department of Justice and Constitutional Development has released the draft Cybercrimes and Cybersecurity Bill for public comment in August 2015. The Bill aims to put in place a coherent and integrated cybersecurity legislative framework for South Africa and clarify the criminal nature of cybercrimes.

This whitepaper is intended for business leaders and management and explains practical steps that organisations should follow to guard themselves against ever-growing cyber risks. It is intentionally written in simple business, and non-technical, terms in order to apply as broadly as possible, but every organisation would need to further interpret how to implement these steps within their own situation. The key steps include:

- Assign responsibility for cybersecurity
- Adopt a practical approach to cybersecurity
- Understand the risks and threats applicable to your organisation



2 ASSIGN RESPONSIBILITY FOR CYBERSECURITY

Organisation-wide risks, such as cybersecurity, that could have significant impact on the organisation's bottom line, reputation or continued operational capability require business leaders to assume accountability. A lack of clear accountability and commitment is one of the key challenges facing cybersecurity and is thus one of the first things that should be clarified within an organisation.

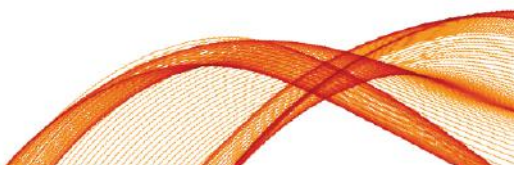
Similar to other organisational risks of this magnitude, business leaders need to invest in establishing a corporate mandate around cybersecurity, and to assemble a team to effectively manage cybersecurity and be able to respond to cyberattacks.

A breakdown of some of the typical responsibilities of cybersecurity is:

- The Board of Directors - provide strategic direction through a governance program, monitor that cyber risks are being managed and provide oversight related to cybersecurity.
- Executive management - establish the cybersecurity functions, allocate resources and ensure operational support of the cybersecurity team.
- Chief Information Officer (CIO) and IT management - ownership for risk management related to critical IT and information infrastructure.
- Chief Risk Officer – ensure cybersecurity risks are adequately reflected on the organisation's risk register and given the necessary focus at risk committees.
- Information Security Officer (ISO) / manager (ISM) - develop the cybersecurity strategy and implement the cybersecurity programme and risk mitigation strategy, ensure compliance of cybersecurity policies and manage cybersecurity incidents and their remediation.
- Cybersecurity practitioners - design, implementation and management of cybersecurity processes and technical controls.

Business leaders must take accountability (A) for the following:

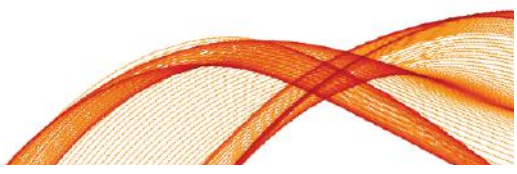
- A Understanding the risks - identify critical infrastructure and the key threats that could impact the business and setting acceptable levels of risk must be top of mind for all business leaders.
- A Establishing and ensuring appropriate governance - implement an effective cybersecurity governance structure, and ensure cyber-related risk is part of risk management.
- A Constituting a cybersecurity team - appoint a team that will ultimately be responsible for managing cybersecurity.
- A Mandating a cybersecurity programme - provide the team with the necessary mandate and resources to implement a programme that leverages leading practices relating to cybersecurity.
- A Providing cybersecurity oversight - oversee the management of cyber-related risks and regular reviews of resources required for cybersecurity, incident reports, risk assessment results, and high level cybersecurity policies.
- A Communication of cybersecurity matters and cyber-related risks to regulatory bodies, industry associations and government.



The diagram below is a typical RACI (Responsible, Accountable, Consulted and Informed) model for cybersecurity within a private enterprise.

	Board of Directors	Executive management	Chief Information Officer	Information Security Officer	Cybersecurity Practitioners
Provide strategic direction through a governance program and provide oversight related to cybersecurity	A	C	R	R	I
Demonstrate that cyber-related risks are being managed	A	R	C	C	
Establish the cybersecurity functions	I	A	R	C	
Allocate resources and ensure operational support of the cybersecurity team	I	A	R	C	I
Ownership for risk management related to critical infrastructure	I	A	R	C	I
Develop the cybersecurity strategy and implement the cybersecurity programme	I	I	A	R	I
Develop a cyber-related risk mitigation strategy	I	I	A	R	C
Manage cybersecurity incidents and their remediation	I	I	C	A	R
Design, implement and manage cybersecurity processes and technical controls		I	C	A	R

R *Responsible* A *Accountable* C *Consulted* I *Informed*

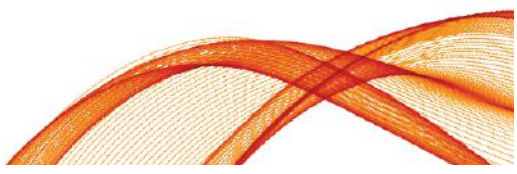


3 ADOPT A PRACTICAL APPROACH TO CYBERSECURITY

Cybersecurity is a complex and technical challenge for most organisations. In our experience many organisations get bogged down in this complexity and a simple, practical approach is thus called for in order to enable adequate progress.

The approach depicted above should be able to be adopted by any organisation

- Start off by developing an understanding of cybersecurity, identifying critical assets and the possible cyber-related threats to your organisation. This initial step will create a cybersecurity threat profile for the organisation.
- The next step is to assess the organisations readiness to address cyber-related threats. The output of this step is articulation of the current and desired states of cybersecurity practices, functions and capability to respond to cyber-related threats.
- Developing a plan and strategy to address the gaps identified from the previous phase comes next. This includes developing policies, roles and responsibilities and determining how cybersecurity can be integrated into existing functions and organisational structures.
- The final step is to act on the plan and build the capability to monitor, detect, prevent, respond and recover from a cyberattack.



4 UNDERSTAND AND EVALUATE THE RISKS AND THREATS

Cybersecurity is an enterprise-wide risk management issue, not just an information technology issue. Management and business leaders must understand what the cyber-related threats to their organisations are, and monitor where cyber-related risk levels are deteriorating or improving. Understanding that the risks are not limited to the direct results of an attack (e.g. fraud, loss of revenue, operational disruptions), but also to consequences such as reputational damage, legal action and shareholder disinvestment. Organisations should understand that cyberattacks may proliferate via a trusted third-party or service provider, and that cyber-related risks are inherent in doing business in our interconnected world. It is also important for business leaders to understand that threats are not limited to large organisations – many attacks are actually focussed on small to medium sized organisations.

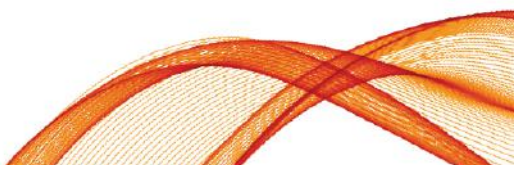
Understanding the types of cyber attackers and what motivates them is a useful tool when starting out with any cybersecurity initiative. Having an understanding of who the cyber attackers are and what they will likely be targeting within your organisation will assist with risk assessments and in selecting and designing effective controls.

The list below includes some of the most common cyber attackers and their motives:

- Cybercriminals - financial gain through fraudulent activities or information peddling.
- Social hackers - collection and selling of confidential personal information or credentials.
- Competitors - information that will provide a competitive advantage.
- Activists / hacktivists - politically motivated to achieve ideological goals.
- Cyber terrorists - disruption or destruction of national critical infrastructures.
- Nation States - obtaining intelligence that can be used against another nation.

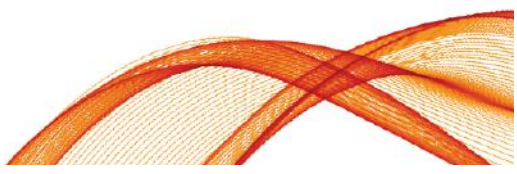
Threats can occur on an organisational, local and national level. National level threats could affect the entire country as targets for such attacks would be energy, telecommunications and other national critical infrastructure. It is government's responsibility to manage cyber-related threats against the state and state organs, as well as to introduce laws, regulations and statuary bodies that can be used to enforce cybersecurity for public and private enterprises.

Private enterprise threats are more targeted at financial gain, intellectual property theft, data theft and in some cases deliberate business disruption. It is the responsibility of the business leaders of private enterprises to manage cyber-related threats that could affect financial performance, reputation, competitive advantage or continued operational capability.



Different industries are susceptible to different types of cyber-related threats depending on the motivation. The table below highlights some of the primary motives for cyberattacks within various industries and can be used as a starting point for your organisation to determine the potential threats relevant to you:

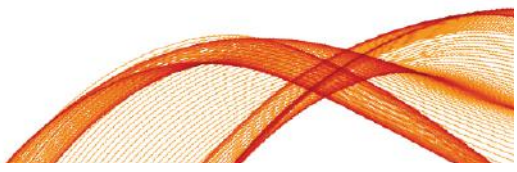
	Threat motive				
Industry	Financial gain, fraud	Theft of Intellectual Property (IP)	Theft of personal data	Disruption of service	Political gain
Education	✓	✓	✓		✓
Financial services / Banking	✓		✓	✓	
Government	✓		✓		✓
Health services			✓	✓	
Manufacturing, engineering		✓		✓	
Oil, gas and mining		✓		✓	
Pharmaceutical		✓			
Retail and wholesale	✓				
Telecommunications			✓	✓	
Transportation	✓			✓	
Utilities - power, water, gas		✓		✓	



Once the threats have been understood, management need to make decisions on how to address these risks through avoidance, acceptance, mitigation or transfer. Supporting this decision requires an understanding of what treatments and options are available, such as putting in process and technology controls or taking out insurance against a cyberattack.

Business leaders and management should be asking these questions:

- Are cyber-related risks considered as part of the broader enterprise risk management?
- How is cybersecurity oversight managed in the organisation?
- What are the organisation's top cybersecurity threats?
- Does the information security management framework include cybersecurity?
- If a breach occurs, will we be able to detect, respond and recover from it?



5 CONCLUSION

Modern organisations have adapted to become reliant on information technology, interconnected systems and the internet to conduct business. Cybercriminals have kept pace with these advances and have become highly organised and skilled at exploiting technological vulnerabilities. Cyberattacks are increasing in both frequency and severity, and these trends will continue to manifest in real risks to business. Business leaders need to champion cybersecurity within their organisations to mitigate cyber-related risks to the business goals and operational sustainability of the organisation.

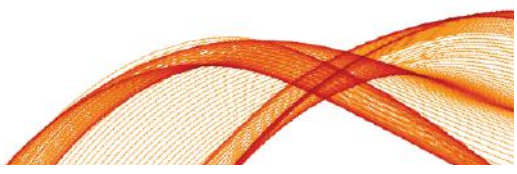
> **CYBERSECURITY** - IDENTIFYING CYBER-RELATED RISKS AND IMPLEMENTING CONTROLS REQUIRED FOR THE PROTECTION OF DIGITAL INFORMATION ASSETS FROM EXTERNAL THREATS, AND BEING ADEQUATELY PREPARED TO DETECT AND RESPOND TO A CYBERATTACK

There are many challenges in developing an approach to cybersecurity, and just as many leading practices, frameworks and standards that seek to provide guidance on how to address those challenges. Selecting a best practice or standard that only addresses IT and technical controls will not fully address all the risks. The approach should include a mix of practices, standards and frameworks that address cybersecurity across the entire organisation and at the governance, risk, functional, operational and technical levels. The approach has to include assessing the cybersecurity readiness of the organisation and developing a strategy and plan to effectively mitigate cyber-related risks.

Cybersecurity roles and responsibilities need to be defined along with key performance indicators that drive a constant improvement in cybersecurity maturity and capability.

The ultimate goal of cybersecurity is for the organisation to be in a position to monitor, detect, prevent, recover and respond to a cyberattack. The approach has to consider leveraging existing functions, and how cybersecurity can be developed as an extension or additional capability in order to achieve this success.

Business leaders need to begin the cybersecurity journey by first understanding what cybersecurity is, how it is applicable to the organisation, and what the possible impacts are of cyber-related risks.



6 CONTACT US

Contact our experienced and qualified Information Security team with multiple Information Security certifications in:

- Certified Information Security Manager (CISM)
- Certfied Infromation System Security Professional (CISSP)
- Systems Security Certified Practitioner (SSCP)
- Cybersecurity Fundamentals (CSX)
- ISO 27001 Foundations
- ISO Lead Auditor

PATRICK RYAN

+27 83 678 6788

PatrickRyan@MobiusConsulting.co.za

RAYMOND DU PLESSIS

+27 78 922 6051

RaymondDuPlessis@MobiusConsulting.co.za