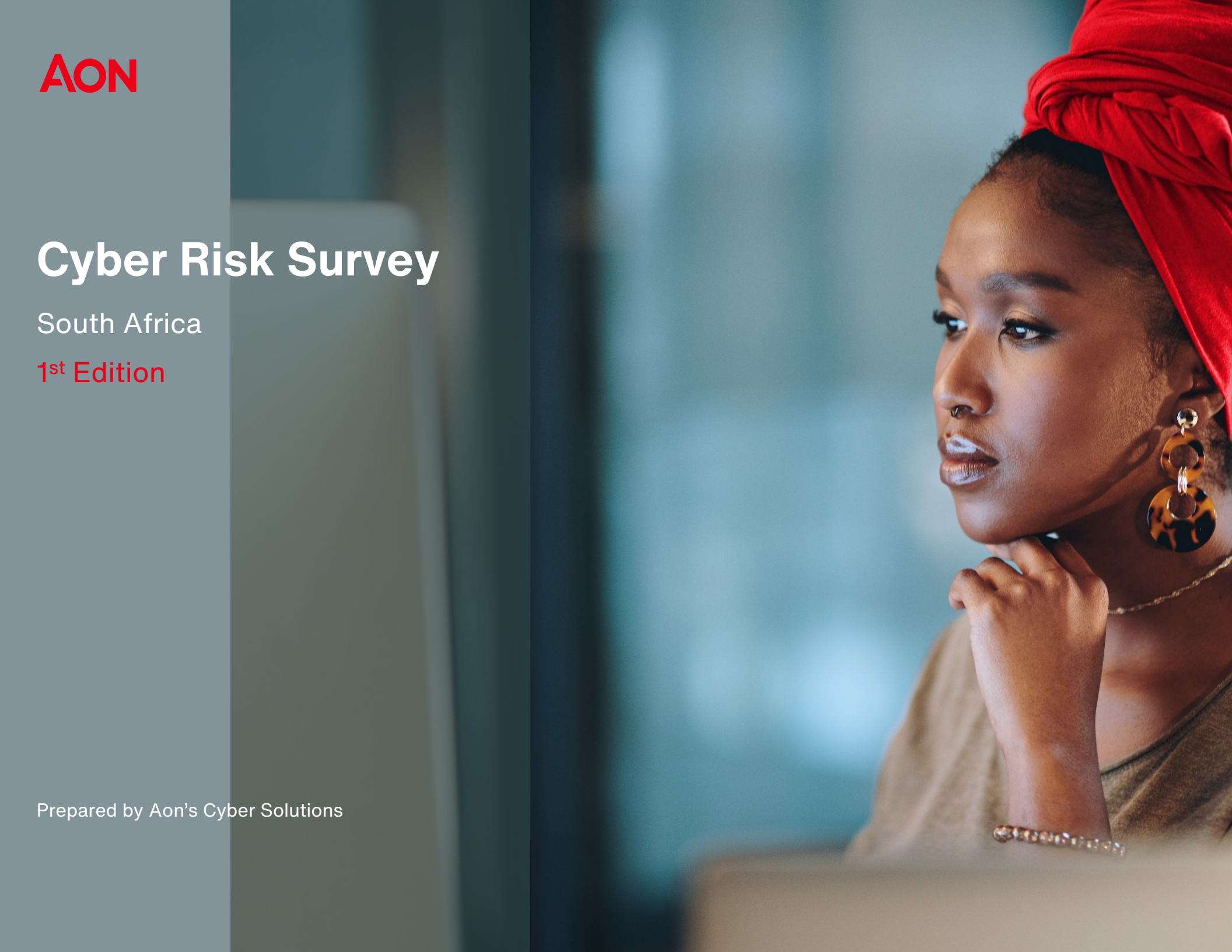
AON

Cyber Risk Survey

South Africa

1st Edition



Prepared by Aon's Cyber Solutions

Overview

Aon's 2023 Cyber Risk Survey for South Africa, is designed to provide insights on current trends in cyber risk governance practices being deployed for South African companies in various market segments.

Summary of Findings

Cyber Risk Survey Key Metrics

Overview

The survey offers commentary on the future direction of cybersecurity given the rapidly evolving manner of the risk, it's solutions and legislative policies, to provide forward looking guidance to organisations.

With the changes to the velocity and severity of the risk drivers associated with cyber, organisations should consider the following:

1. Is there sufficient awareness of the risk, from a governance perspective?
2. Is there sufficient protection against it, from a business resilience perspective?
3. Is there sufficient balance sheet protection?

Cyber Losses

22%

have suffered a cyber incident in the past 5 years

Risk Management

67%

participants deploy a cyber risk management tool

Board Support

50%

have a board-level cyber champion

Cyber Insurance

72%

Purchase cyber insurance

Introduction

Cyber Risk in South Africa

Development & Relevance

The regulation of the risk management or governance of Information Technology assets, has developed in other regions (i.e., European NIS2 Directive) and whilst South Africa has commented on increased IT governance (i.e., principle 12 of King IV), there isn't any clear guideline or regulation of how IT assets must be secured.

Cyber attacks/data breaches are commonly referred to as the leading concern for C-Suite members[1] and with South Africa being rated amongst one of the top countries globally rife with cybercrime[2], the subsequent governance should be top of mind.

The aim of this survey is to provide insights as to how companies are currently addressing this problem and provide an overarching framework that can assist in remediating this issue.

Actionable Outcomes

This survey was put together with the hopes of putting forward to IT and Risk executives, an awareness around how their organization compares with it's contemporaries and furthermore, provide a framework for how they can address their cyber risk management concerns.

1. *Aon, Global Risk Management Survey 2023*
2. *Surfshark, Data Breach Impact 2022*

Cyber Risk Management

Is Cyber Risk Management Top of Mind?

Cyber Risk Management

A cyber risk management assessment is a tool that assists companies in identifying their vulnerabilities and provides subsequent mitigation plans. This is not to be confused with penetration or vulnerability testing. Cyber risk management is about whether or not the company has the appropriate tools to protect the business – the governance of cyber risk.

This could look like a recommendation to implement multifactor authentication for remote access into your business environment, or perhaps updating the password policy. These risk management tools allows the business and its directors oversight on how the business is being protected, then ties in market developments to ensure that a business always has the most relevant mitigation measures in place.

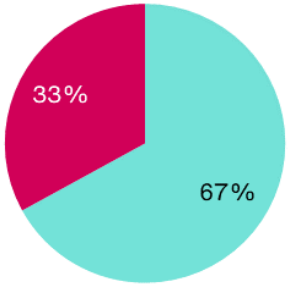
As cyber risk is an ever-evolving risk, due to threat actors continuously finding new and innovative ways to steal data or gain access into protected systems, the solution space develops commensurate to the threat activity – so the antivirus you bought last year that was state-of-the-art, most likely isn't a year later.

Findings

Cyber Risk Management

Overview

Over 67% of the participants of the survey reported deploying a cyber risk management tool



+67%

Deploy a cyber risk management tool

Negative(s)

Negative correlation between revenue generated and the deployment of a cyber risk management tool.

Which could be interpreted as either companies finding the cost of proactive risk management too high, or alternatively that there is a perception that the risk is only reserved for companies with a higher revenue bracket.

-43%

Less than 50% of the companies with revenue of less than R100m deployed a risk management tool

Positive(s)

There is an apparent adoption of cyber risk management tools in higher revenue bands, which could lead to the qualification that more often than not the deployment of a cyber risk management tool should be seen as a prerequisite to all companies as part of their overall IT governance strategy.

+80%

Companies with revenue of over 100m deployed a cyber risk management tool

Takeaways

A company generating over R100m in revenue and not having a cyber risk management tool can be considered immature.

SMMEs do not have a cyber risk management tool in place, which could lead to the assumption that these types of businesses are far more susceptible to a cyber/data breach incident.

Senior Leadership Support

Does IT risk have visibility at the highest level in an organization?

Support from Senior Leaders

Cyber attacks ranked #4 in Aon's 2022 Executive Risk Survey (superseded only by high inflation concerns, a financial crisis and energy concerns), however visibility of board level champions of this risk is somewhat vague in South Africa, even in the listed space.

Whilst companies with a larger footprint or who have a particular focus on technology/digital would necessitate having a Chief Information and/or a Chief Information Security Officer, smaller companies may not have the luxury of a full-time resource focused on cyber risk – given this, it is to be anticipated that some difficulty would be faced when trying to procure budget to protect an organization from cyber related threats.
In an ever more increasing regulated environment (especially when it comes to the processing and storage of data i.e., the Protection of Personal Information Act), senior leaders cannot afford to have this overlooked, as this can potentially have an impact on them personally.

The findings of the survey also indicate that there is sufficient EXCO level support, however not so much at Board level.

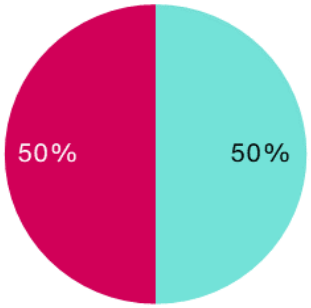
AON

Findings

Visibility of Cyber Risks in Senior Leadership

Overview (Board)

Board level visibility was split evenly between all participants of the survey.



+50%

Of the participants noted they had a board-level cyber champion

Takeaways

There was a higher adoption of having a board level cyber champion in companies generating over R1bn, however it was only marginal given the data set (62%). That number further reduces in the companies that are listed.

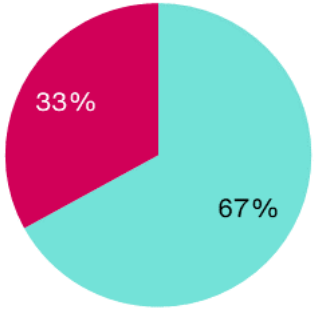
It doesn't seem there is any wide spread adoption of having a board level cyber champion, which is not congruent with the principle 12 in King IV.

+62%

Of the participants generating over R1bn noted they had board level cyber champions.

Overview (EXCO)

EXCO level cyber champion were pretty standard across all participants generating over R100m.



+67%

Of the participants surveyed have an EXCO level cyber champion

Takeaways

EXCO level cyber champion were pretty standard across all participants generating over R100m.

There was additionally a direct correlation between companies having a cyber risk management tool and having an EXCO level cyber champion.

+91%

Of the participants surveyed generating over R100m had EXCO level cyber champion.

Cyber Incidents

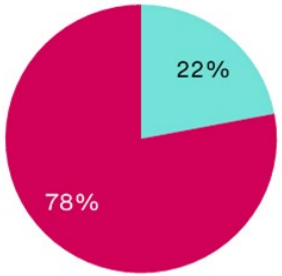
Do companies only “beef up” after an attack?

Cybersecurity before and after an incident

The hypothesis posed by this survey question was whether companies that have suffered a cyber attack would have better cyber risk management practices, than those who did not suffer an attack.

The results somewhat agree with the hypothesis. Of the companies that were surveyed, only 22% suffered a cyber attack, of those 22% they all had:

- A Cyber Risk Management tool
- Executive level cyber champion
- Cyber Liability Insurance
- Directors & Officers Insurance
- Commercial Crime Insurance



When comparing the subset of companies that suffered a cyber attack against those who haven’t, there’s an inconsistency of the aforementioned mitigation controls in place, i.e., the percentage of the dataset who haven’t suffered a cyber incident show a less than 50% uptake on mitigation controls.

Additionally, even in lower revenue bands post a cyber incident, companies generating less than R100m, we still not as mature as their contemporaries that suffered a cyber incident in higher revenue bands.

Cyber and it's Insurances

Breach Liability and Cybercrime

Cyber and other related insurances

The insurance market has rapidly changed to remain a sustainable solution to transfer the balance sheet risk companies have from cyber risks. Various lines of insurances have started to include cyber exclusions (i.e. property, directors & officers etc.). As these exclusions have started to trickle in, companies need to be cognizant that they have appropriate coverage in relation to their overall insurance portfolio.

With the South African Banking Risk Information Centre reporting that South Africa loses approximately R2.4bn on cyber attacks and INTERPOL's 2022 Africa Cyberthreat Assessment report, it is evident South Africa has a high amount of cybercrime and cyber related attacks, however it is important to differentiate the impact of insurances when it comes to theft of money and theft of data– these types of incidents are different to incidents that would fall within a traditional cyber policy. A simplistic differentiation between commercial crime and cyber is that:

- Commercial Crime covers the theft of money
- Cyber Liability covers the theft of data and impact to system/data access

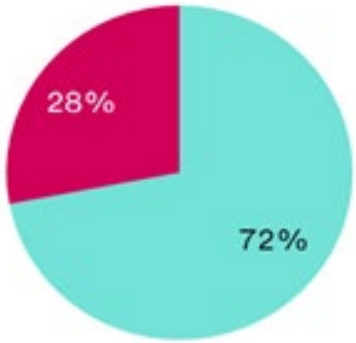
Additionally, following on with the cadence of understanding the importance of senior leadership in cybersecurity, there have been developments of shareholders directing lawsuits to directors and officers in their personal capacity, as a result of a loss of shareholder value, post a cyber incident impacting the respective company. Further highlighting the importance of cybersecurity and its governance; business owners and managers should ensure that the appropriate oversight, resources and processes are in place to manage this key risk.

Findings

Insurance purchase(s)

Cyber Insurance

A majority of the participants purchased cyber insurance. All companies generating over R1bn purchased cyber liability insurance.

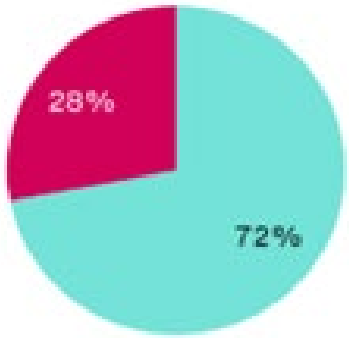


+72%

Of the participants indicated that they purchased cyber liability insurance

Commercial Crime

A majority of the participants purchased commercial crime insurance. All companies generating over R1bn purchased the insurance.

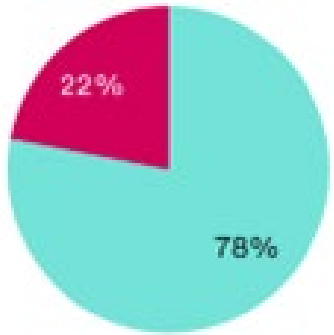


+72%

Of the participants indicated that they purchased commercial crime insurance

Directors & Officers D&O Liability

A majority of the participants purchased D&O liability insurance. Although split relatively evenly, companies over R1bn had a higher adoption rate.



+76%

Of the participants indicated that they purchased director's and officer's (D&O) liability insurance

Takeaway

All clients with over R1bn bought cyber and commercial crime insurance, the remaining revenue bands were relatively evenly distributed.

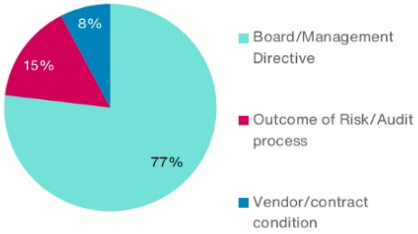
D&O coverage was relatively split with a higher adoption in the companies over R1bn.

Findings

Reason(s) behind cyber insurance purchase

Reasons for buying

Audit/risk practices and vendor/third party requirements were the other considerations for reasons company's buy cyber insurance.



+77%

Of the participants surveyed purchased cyber insurance due to board/management directive

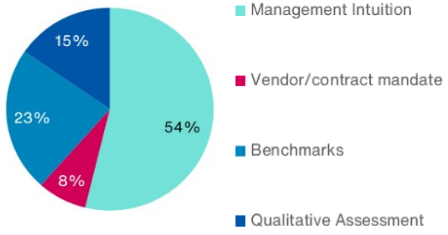
Takeaway(s)

Senior Leadership plays an important role in the governance of cyber risks and the purchase of its insurances.

Although adoption of transferring cyber risk off balance sheet was prevalent in the dataset, the reasons for buying did not evolve from a process outcome. This may support the notion that cyber risk management is not readily adopted, or furthermore recommendations from these exercises is not adopted.

What educated the limit purchased?

Barring management information, there was no consistent stance on what educated the limit of insurances for cyber liability.



+54%

Of the participants surveyed stated that management intuition was what informed the amount of cyber purchased.

Takeaway(s)

Each company is different and whilst management intuition does have some utility, it is useful to support assumptions with data and externally interrogated rationale.

Benchmarks although useful, do not take into consideration that companies operate in different geographies and data privacy acts. It is also useful to understand that not all companies (even if they operate in the same sector),, process information similarly or process the same types of information.

Way Forward

Considerations

Awareness

The survey indicates that there is a fair amount of awareness from Senior Leadership on cyber risks.

This is substantiated by the adoption of cyber insurance being primarily driven by board / management directives.

However, the lack of board level cyber champions could be improved in order to have adequate resources directed to protecting a company from cyber risk.

Cyber Risk Management

The adoption of cyber risk management whilst relatively evident in the dataset, the responses suggest that the process and outcomes commensurate with the practice, do not support the notion that cyber risk management is effectively applied.

This could be caused by Senior Leadership being unable to understand the Return on Security Investment.

Risk Transfer

Adoption of cyber insurance (and other liability related insurances), was a generally applied practice.

Companies should consider applying quantification metrics to substantiate the limits purchased, and conduct an insurability analysis to ensure that the businesses top cyber risks are well protected relative the insurance portfolio.

Possible Solutions

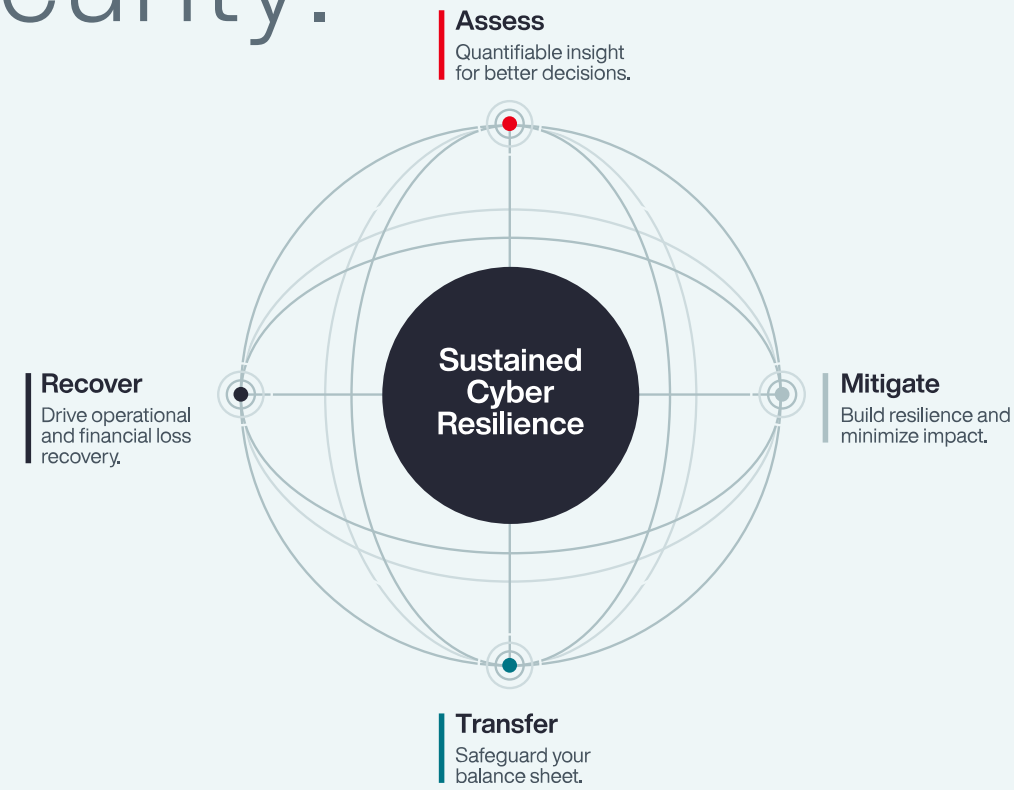
The survey suggests that smaller companies with less than R100m could benefit from having “CISO as a service” and a cyber risk management assessment, a cost effective manner that will assist SMEs in cybersecurity. Companies can also benefit from a Cyber Impact Analysis, which quantifies cyber risk and provides an insurability analysis.

There is Nothing Linear About Cyber Security.

This is the guiding principle of the Cyber Loop, a risk management model that **unites stakeholders** to make better decisions around cyber risk.

Aon's Cyber Loop model acknowledges that each organization will be at a different place in its cyber risk journey: **assess, mitigate, transfer, or recover**.

In a Loop model, businesses become informed participants in managing risk, engaged in continuous review, improvement, and investment in security – guided by data.



The Result. Sustained Cyber Resilience.

Conclusion

Cyber Risk Survey: South Africa

Key Takeaways

Senior leadership is evidently aware of cyber risk, however, they are, perhaps unclear on how to effectively protect against it. This translates into a lack of business resilience against cyber related losses. Evidence of this, is the lack of consistency on the approach to cyber risk management, ultimately leading to inadequate balance sheet protection of the materialization of cyber related losses.

Aon can assist clients demystify this risk and provide a data driven approach to cyber risk management and effective balance sheet transfer. As this risk becomes more pronounced and matures in the South African environment, it will be important for all directors to have a grasp on the governance of cyber risk.

Contacts

Aon's Cyber Solutions

Aon South Africa | Aon's Cyber Solutions

Zamani Ngidi
Aon's Cyber Solutions
zamani.ngidi2@aon.co.za

Jenny Jooste
Aon's Cyber Solutions
jenny.jooste11@aon.co.za

Kamohelo Mokoena
Aon's Cyber Solutions
kamohelo.mokoena@aon.co.za

Mapaseka Radebe
Aon's Cyber Solutions
mapaseka.radebe@aon.co.za

Tshepo Nkumbi
Aon's Cyber Solutions
tshepo.nkumbi@aon.co.za

About Aon

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Our colleagues provide our clients in over 120 countries and sovereignties with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business.

Aon South Africa (Pty) Ltd, FSP # 20555
Aon Re Africa (Pty) Ltd, FSP # 20658