Sanlam

Benchmark 2019

Enabling Financial Resilience

Information Insecurity

by Tebogo Legodi

Digital Lead
Sanlam Employee Benefits


V.S.

CYBERCRIMINALS

- Sophisticated Networks
- Global
- Ruthless
- Skilled

- Organised Crime
- State sponsored hacks


Employee Numbers
Fund Values
ID No’s
Gender
Tax No’s
Names
Age
Salaries
Employers
Contact details (Cell & Email)
Beneficiary Details

INFORMATION SECURITY

Practice of preventing:

- Unauthorised use
- Disclosure
- Disruption
- Modification
- Inspection
- Recording or
- Destruction of information, whether physical or electronic

LEGISLATION

Protection of Personal Information Act 4 of 2013 Section 19:

(1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—

(a) loss of, damage to or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.

(2) In order to give effect to subsection (1), the responsible party must take reasonable measures to—

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risks identified;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

(3)The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations."

CYBERCRIME BILL

- Obligation to report acts of cybercrime
- Preserve evidence (confiscation or seizure)

KING IV

IT Governance addressed in detail for the first time Information Governance Framework

KEY RISK GLOBALLY

- 2019 Allianz Risk Barometer of Top Business Risks
- 2,415 Respondents
- Cybersecurity Top alongside Business Interruption
- Within Business Interruption, Cybersecurity is most feared threat
- 5th in 2015 … 1st in 2019!
- Primary asset = Data

IBM X-FORCE THREAT INTELLIGENCE INDEX

- Unmanageable levels of cyberthreats
- Ever-growing attack landscape
- Increased risk of exposure

IBM X-FORCE THREAT INTELLIGENCE INDEX

- Most Attacked Industry
- Finance & Insurance - 19% of Global Attacks
- Data monetized rapidly
- Direct profit or Resale

IBM X-FORCE THREAT INTELLIGENCE INDEX

- 3rd Most Attacked Industry …
- Professional Services (eg. Consulting firms)
- Rich personal information of clients
- Smaller budgets
- Limited staff
- Immature security position

IBM X-FORCE THREAT INTELLIGENCE INDEX

“Vulnerable and Lucrative”

COST OF CYBERCRIME

- 2018 **Refinitiv** Revealing the Cost of Financial Crime Survey
- 2,373 Global Respondents
- 123 from RSA
- 20% have experienced Financial Loss due to Cyber Crime

COST OF CYBERCRIME

- Average cost has increased 62% over 5 years
- Typical cost per breach - $4m
- $600Bn pa
- $208Bn pa average loss from natural disasters over past 10 years

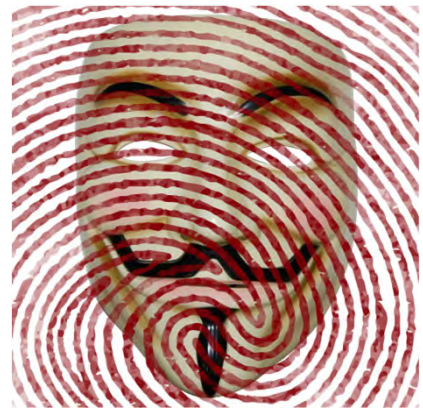
COST OF CYBERCRIME

- Fraudulent Transactions
- Litigation by Members, Employers, etc.
- Liability (Trustees, Consultant, Administrator)
- Reputational damage
- Business Interruption
- Regulatory Sanction
- Mass action

EXAMPLES

- Personal Information
- Sold & Resold
- Aggregrate stolen information with data from other sources

Ultimately used for Identity Theft



POOR INTERNAL SECURITY PRACTICES

- Phishing
- Social Engineering
- Weak Password Practices

KEY ENABLERS OF CYBER RESILIENCE

People. People. People.

- Culture
- Training
- Structure

CONSULTANTS' VIEWS

- Evaluating Cyber Risk least important business challenge
- Cyber security lowest ranked risk to EB Consultants
- Data analytics & IT expertise least cited differentiator

- Lack of awareness and skills

CYBER RESILIENT?

Jan 2019 – Mar 2019	Standalone	Umbrella
IT Policies & Procedures	64%	50%
System Protocols Revised	40%	27%
Invested in securing IT infrastructure	39%	52%
Education & Training of Staff	19%	22%
Training & Notifications to Members	22%	30%
Handled by our Administrator	11%	5%
Nothing as yet	10%	12%

YET …

- 68% indicate that they evaluate Administrators' abilities to mitigate cyber-crime when advising on placement of administration
- 70% claim to have intermediate knowledge to evaluate protection against cyber crime
- 25% indicate little knowledge
- 35% are not sure whether their administrators have implemented any strategies to protect members from the threat of cyber crime

98% believe that the administrator or sponsor should be held liable in the event of losses due to cyber crime

WHAT IF …

- Trustees and Employers rely on Consultants to provide best advice
- Including an evaluation of Cyber resilience
- Data loss can occur at the Consultant

… Far greater discipline needs to be applied to evaluate and monitor Cyber Resilience … Collective effort required

ADVICE RISK

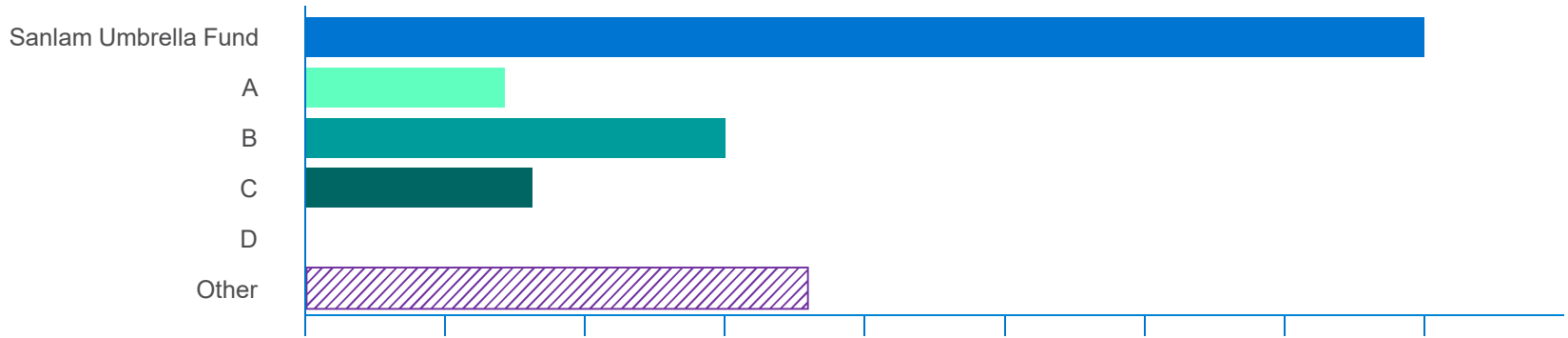
- Expert Opinion on Service Providers
- Holds great influence over decisions
- Cyber risk largely ignored
- Material differences exist
- These have not been evaluated
- Degree of Cyber Resilience can vary wildly …

FIDUCIARY DUTY OF TRUSTEES

They must exercise their powers to the benefit of the fund and in such a manner as to always act in the best interest of the fund and its members.

- Ensure that the fund employs proper control systems
- Obtain expert advice on matters where they lack sufficient expertise
- Ensure that the rules, operation and
- Administration of the fund comply with the relevant acts

MOST CAPABLE OF ENABLING FINANCIAL RESILIENCE FOR MEMBERS



2019 Sanlam Benchmark Consultant Survey

CROWN JEWELS

- Names
- ID No’s
- Tax No’s
- Age
- Gender
- Contact details (Cell & Email)
- Employers
- Employee Numbers
- Salaries
- Fund Values
- Beneficiary Details

Cyber Resilience Checklist

		SANLAM ADMINISTRATOR
Governance »	Has your administrator established formal governance policies and processes for Information security, information governance, cyber security, third party management, etc. ?	✓
	Does your administrator have cyber insurance to enable financial stability for significant cyber events?	✓
Preventative »	Does your current administrator have dedicated information security staff who proactively identify and resolve cyber security vulnerabilities	✓
	Is your administrator's information security staff trained to respond to cyber security Incidents?	✓
	Does your administrator have processes in place to manage cyber security In terms of: • Prevent data from being stolen from computers (USB port blocking and encrypted hard drives)? • Continuous monitoring of antivirus/anti-malware software to ensure that they are up-to-date?	✓
	If there are phishing attempts, is your administrator equipped to identify these events and mitigate the risks?	✓
	Does your administrator have processes in place to restrict system accessibllity? (privileged account management and segregation of duties reviews. etc.)	✓
Monitoring »	Does your administrator have a dedicated team to actively detect and respond to cyber-attack attempts?	✓
Response »	In the event of an Incident, breach or hacking activity. does ~ your administrator have a programme in place to: • Respond to a crisis; • Forensically experts to help investigate; and • The capability to recover data systems after cyber incidents?	✓

ENABLING FINANCIAL RESILIENCE

- Apply Checklist
- Seek expert guidance
- Implement corrective action
- Choice of Cyber Resilient service providers
- Repeat

ENABLING FINANCIAL RESILIENCE

- Make information security an integral part of culture and overall structure in relation to Funds, Employers, Consultants and Administrators