

# **CISO** Alliances

Cape Town Chapter

6th March 2019

**Feedback**





**Clint Abels**  
ICT Risk, Security  
and Compliance  
Manager  
Distell



**Amr Awad**  
MEA IBM Technical  
Consultant: Incident  
Response  
IBM



**Michelle Barnett**  
IT Risk and  
Infrastructure  
Manager  
Cape Union Mart



**Philip Greef**  
Head of IT  
Coronation Fund  
Managers



**Yashin  
Raghavjee**  
Head of IT Southern  
Africa  
British American  
Tobacco



**Renaldo Jack  
Engen**



**Sylvia Brouwer**  
Information Security  
Independent



**Scott Carver**  
Western Cape,  
Hybrid Cloud  
Software Leader  
IBM South Africa  
pty Ltd



**Louis de Kock**  
South Africa  
Country Business  
Development  
Varonis Systems



**Christine Fahlberg**  
IT Security Manager  
Truworths



**Sheldon Hand**  
Business Unit  
Leader - Security  
IBM South Africa  
pty Ltd



**Ravindra Jugdav**  
Information Security  
Manager  
Rentokil-Initial



**Werner Lunow**  
CISO  
Allan Gray



**Dr. Nontobeko  
Mabizela**  
Head of Impact  
Assurance  
Allan Gray Orbis  
Foundation



**Charlie  
Hinde**  
Senior Manager:  
Information Security  
Foschini Retail  
Group



**Vikesh Ramdayal**  
Program Manager  
Information Security  
The Foschini Group



**Ebrahim Makda**  
ICT Operations  
Manager  
**Van Schaik Bookstore**



**Wessel Matthee**  
Information Security  
Manager  
**PicknPay**



**Andrew Meyer**  
Head of IT Group  
Security, Risk and  
Governance  
**Woolworths**



**Suren Naidoo**  
Head of Enterprise  
Architecture,  
Information Security  
& GRC  
**The Foschini Group**



**Mahomed Osman**  
IT Audit Manager  
**Clicks Group**



**Faseeg Osman**  
Manager: Information  
Security Operations &  
Architecture  
**The Foschini Group**



**Johan Rabie**  
Risk and  
Compliance  
Manager  
**CapitaSA**



**Celeste Rogers**  
Group CIO  
**MTO Group**



**Abongile Monqo**  
Regional Manager  
**Popcorn Training a KnowBe4 Company**



**Terence Tuwe**  
Client Technical  
Specialist  
**IBM Global Markets**  
- Cognitive Solutions  
Unit Industry  
Platforms (Geo)



**Samantha Rule**  
Group Information  
Security Head  
**Maitland**



**Michelle van Heerden**  
Consultant  
**GTconsult**



**Deon White**  
Head of Information  
Systems &  
Technology  
**Allan Gray Orbis**



**Sibonelo Zikalala**  
Systems Engineer  
**Varonis**

# Overall Theme – Making InfoSec Real

## Areas of focus – Strategy for People, Process, Technology

08:00 – 08:30

**Registration**

08:30 – 08:45

**Welcome Remarks & Housekeeping**

Sylvia Brouwer - Independent

8:45 – 10:30 - Open Forum

Leigh Thomas - Director - CISO Alliances

10:55 – 11:10 – Scenario Overview / 11:10 – 11:40 – Open Forum

**Framework / Best Practices for Incident Response Orchestration and Automation**

Amr Awad - MEA Regional Technical Leader - Resilient - IBM

11:40 – 12:25 – Open Forum

Leigh Thomas - Director - CISO Alliances

12:25 – 13:30

**Networking Lunch**

13:30 – 14:00 – Conclusion


**Conclusion from the day, collate, revert, action**

Leigh Thomas - Director - CISO Alliances

## 1. Update on POPIA

- Partially enacted and when signed off, 12 months to comply
- Issue – Cost of compliance
  - Areas – Lawyers, consultants, regulators with conflicting guidelines
  - ‘Experts’ in POPI have subjective views
    - Security
    - Ethical
    - Moral
- ‘Hidden’ areas of the act, meaning systems to ‘action customer requests’
- Regulations are not prescriptive
- Opportunity to leverage Overlays POPI & PCI
- Predicting sign-off from international data privacy acts as well as the National Credit Act & Section 19 Security (Recognised standards) ISO 27001
- Is there a challenge with industry specific ‘Data Laws’ or can there be cross-vertical data compliant processes? (FSI are writing their own security code to be accepted/ recommend change by regulator)
- How compliant do you need to be now?
  - Where/ When do the processes become more ‘Act’ friendly?
  - How much do you impact processes (new & old)?
- Consequences of a breach
  - Board jail time
  - Up to R10 Billion
  - Is this enough of a deterrent or does the cost of compliance out way the consequence?
- Future – will there be too much data to ‘comply’ and data becomes freely available?

## 2. What is being done to protect our national assets from being hacked? Does the government have concrete plans in place to address this? Failing infrastructure and poor maintenance seems to indicate otherwise. Does anyone have insights into this?

- Government can do more
  - Upskill
  - Culture Change
  - Movement from Dr Kiru Pillay and the Cyber Security Hub
- 

### 3. Security spend and investment: investment vs risk- how much is enough; how do we measure ROI?

- **Focuses vary within the community and motivation is varied.**
- **Risk based decision making**
  - Maturity
  - Framework
  - POPI/ Compliance
- **Digital Drive – Business Transformational, for the majority, Cloud**
- **ROI**
  - Quantifying/ Qualifying Risk Measurement
  - Cyber Insurance
  - Communicating in the Board Language with Board Politics
  - Security means doing a lot of ‘things’ that doesn’t have ROI attached
  - Selling a cost for something that may never happen
- **Does critical mean priority**
- **Shadow IT**
- **Insider threat – Policies not being read but who is the policy there to protect?**
- **Fact: Data Breaches are down by 200 million in a year, globally**
- **Business Process – Communication!**
  - New User Inductions
  - Training for multiple levels of the workforce and business divisions. Marketing and sales are the main instigator of ‘poor’ data use
- **Measurement of adoption rate, where is it? Identifying the effective ways your workforce learn (VAK).**

### 4. The CISO role-is it a business role or IT role? Who should the CISO report to? What part of security strategy is unsourced vs outsourced? How is the security landscape changing? How does cloud impact this?

- **Typically and IT role supported by 80% of the audience**
- **But**
  - IT cannot manage data
  - Why not a business vertical of its own?
- **In vs Out**
  - Never outsource the development of strategy – Immediate disconnect
  - Insource where maturity of resource allows as well as competence.
  - Innovate around the security strategy with tactical forward thinking
- **Out**
  - PEN Testing – Shows more vulnerabilities


## 5. A dynamic security strategy: how is it evolving and changing. How dynamic should it be? Who are the core Stakeholders?

- Threat factors are changing
- Threat maturity level means more significant breaches globally that should encourage C-Level buy in
- Common challenges around innovating if, it may not happen
- Why does security need to be dynamic?
- Are your security frameworks standing the test of time? Internal transformational program as well as the risks that now exist
- Innovate and test using opensource. Identify what you need, find the use cases
- Typically, we leave it and react to the next thing. Defining the security role, but it can be dynamic
  - E.g. threat hunting, industry specific
- Categorisation of resources
- Risk Management Strategy – Be aware of the changes

## 6. Can we mentor and increase the pool of security analysts and ISOs? Find good security staff and more importantly hang onto them.

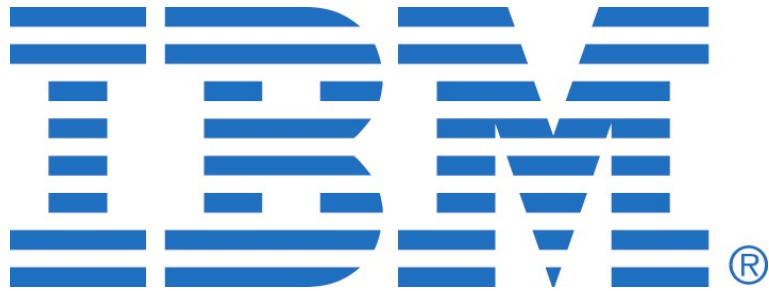
- Cyber security isn't considered a 'career opportunity'
  - As a community we need to ensure the visualised career path is promoted
- Are the roles defined or is there a culture of 'Do it all' – jack of all, master of none in SA due to the lack of resource?
- Task – Attract interns on community led internships
  - Work with Undergrads on placements to experience the good, bad and exciting areas of cybersecurity.

## 7. Africa operations; are there reliable/skilled ICT partners?

- Local support is required
  - Standardised approach is difficult
  - Upskill – treat yourself as a global company to scale
  - Healthy competition
  - What is the definition of reliable? Perception and expectations differ
  - Defining skilled – experience vs certification/ academia
- 



Use Case Partner CISO Cape Town Chapter



Click IBM logo for partner presentation





## Format reflection – what would you like to achieve? How can the alliances impact?

- Encourage start-ups to impact the alliances communities
- Diversity/ more vendors
- Agile/ Lean thinking
- Focus on session outcome and aim to achieve – measure success, measure failure, LEARN.
- Focus on less content
- Use case approach – learn from the real
- Collaborate more
- Community confidence in sharing VALUABLE opinions and not IP
- Code of Conduct
- Code of Ethics
- Charters
- CISO Alliances – Threat Intelligence Platform
- Benchmarking appropriately – vertically/ maturity
- Search Academia for moderators/ content delivery
- Giving visibility to students (Security Interns) – tap into fresh thinking

## Proposed content for the next chapter (In order of vote)

- Cloud Security Strategy
- Include End users, AWS & Azure
- Influencing & Buy-in for Security investment from the Board
- Threat Intelligence
- Socialising InfoSec Policy
- 3rd Party Risk Management

Date: June/ July

Venue: TFG HQ

