CISO Alliances

Cape Town Chapter

19th June 2019

Results

ALLIANCE Media Group

Alliance - 'A union formed for mutual benefit'

ALLIANCE Media Group

Executive Business Exchange

CIO Alliances

CISO Alliances

CXO Alliances

CMO Alliances

CDO Alliances

Foreword

Leigh Thomas is an ambitious and passionate executive with a desire for achieving the ideal.

With experience in numerous industries and working within C-level communities across the globe in Oil & Gas, Mining, Power & Enterprise IT across multiple divisions across the business.

Following his experience with his previous employer and working with leading CIOs & CISO's across EMEA, his understanding of B2B events grew. With his passion for achieving the ideal scenario a plan was founded to strip back what the industry is about. This is where the core values of the Alliance Chapter were born along with Alliance Media Group.

Alliance - 'A union formed for mutual benefit'.

Whilst understanding that every business will need to drive commercials to become sustainable in the modern world. Leigh believed that commercials must not be the driver but, a solution to a 'why'.

The Event Managed Services industry is spiralling into a dark tunnel of an industry where money is the leader and not the value of time. The industry was born off the back of 'Everybody wants to learn' and Leigh Thomas has created the Alliances to ensure that the end user driven meets, are purely focused around the educational needs of everyone involved and around their business objectives. Zoning in on the best practices in overcoming the common business objectives that motivate activity within each of the end user firms and not simply global trends and themes to generate revenue.

Leigh Thomas
Director & Founder

08:00 – 08:30

Registration

08:30 – 08:45

Housekeeping, purpose driver and format reminder

Leigh Thomas –Director & Founder - CISO Alliances

08:45 - 09:45

Session 1 - Workshop

Christine Fahlberg – IT Security Manager – Truworths

Problem Statement: How to gain influence and buy-in for Security investment from the Board?

09:45 - 10:30

Session 2 - Open Forum

Ravindra Jugdav – Information Security Manager Africa, Middle East, Baltics, Nordics & Caribbean – Rentokil-Initial

Cloud Security – The Facts: Customer Responsibilities for Security in Cloud Computing

10:30 - 10:45

Networking Break

10:45 - 1200

Session 3 - Scenario Overview & Open Forum

Suren Naidoo – CISO – The Foschini GroupSession

Threat Intelligence Cyber crime is a global issue and everyone is exposed to it in some shape or form.

12:00 - 12:45

Session 4 - Community Survey

Charlie Hinde – Senior Manager Information Security – The Foschini Group

Socialising InfoSec Policy

12:45 - 13:45

Networking Lunch

13:45 - 15:00

Session 5 - Scenario Overview & Open Forum

Michelle Barnett – IT Risk, Governance and Compliance Manager – Cape Union Mart (Pty) Ltd

3rd Party Risk Management

15:00

Closing Remarks & the Next Steps

Clint Abels

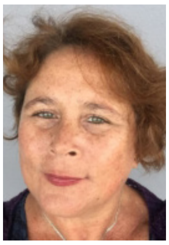
IT Risk, Security & Compliance Manager

Distell

Michelle Barnett

IT Risk, Governance and Compliance Manager

Cape Union Mart (Pty)



Sylvia Brouwer

Freelancer

Marc Dotan

Security Engineer

EOH/ITCS

Faseeg Osman

Information Security Manager

TFG

Christine Fahlberg

IT Security Manager

TRUWORTHS

Ebrahim Makda

ICT Operations Manager

Van Schaik Bookstore

Gail Francke

IT GRC Analyst

Curo Fund Services

Roshan Harneker

Senior Manager: Info and Cybersecurity Services

University of Cape Town

Lulamela Qoma

Information Security Analyst

The Foschini Group

Sue Gordon

Operations and Client Security Relations Executive

EOH/ITCS

Charlie Hinde

Senior Manager: Information Security

The Foschini Group (Pty) Ltd

Renaldo Jack

Head of Cybersecurity

Engen

Grant Hughes

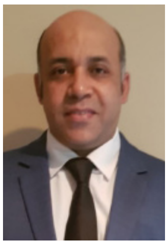
Cybersecurity Intelligence Centre Manager

TFG

Akash Srikewal

Modern Workplace Solutions Specialist

Microsoft



Sodick Jacobs

Technical Cyber Threat Intelligence Analyst

South African Reserve Bank

Andre Matthee

Head of IT

HomeChoice

Ravindra Jugdav

Information Security Manager

Rentokil Initial

Andrew Meyer

Head of IT Group Security, Risk and Governance

Woolworths

Deon White

CIO

Allan Gray Orbis Foundation

Suren Naidoo

CISO

TFG

Martin Potgieter

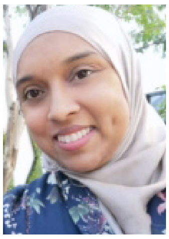
Technical Director

Nclose

Johannes Steyn

Snr Info Security Architect

The Foschini Group



Kerissa Varma

Risk Executive

Old Mutual

Arlene - Lynn Volmink

President SA

ISACA

Yashin Raghavjee

IT Manager SAA
(Interim HoIT)

British American Tobacco

Samantha Rule

Group Information Security, Risk and Governance Head

Maitland Group

Vikesh Ramdayal

Infosec Programme Manager

TFG

Duncan Rae

Infrastructure and Security Architect

Pick n Pay

Sizwe Zikhali

Technology Solutions Professional

Microsoft

Janine Van Niekerk

Lead IT Specialist

Old Mutual

Bernard van der Merwe

Information Security Officer

HomeChoice

Brian Mkaza

CIO

Stellenbosch Municipality

Celeste Rogers

Group CIO

MTO Group

Workshop

Christine Fahlberg

IT Security Manager

TRUWORTHS

Session 1

Session Leader: **Christine Fahlberg – IT Security Manager – Truworths**

Problem Statement: **How to gain influence and buy-in for Security investment from the Board?**

Abstract: Cybersecurity attacks and data breaches continue to make headlines as businesses fall victim to compromised corporate networks and information theft.

However, some organisations are reluctant to buy-in to security investment plans to build or improve their security posture. Cybersecurity becomes more expensive, Gartner reports that average annual security spending per employee doubled, from $584 in 2012 to $1,178 in 2018. Often an intense debate arises whether the cost of a breach justifies the investment cost of such preventative programs. So how do you justify your investment plan? The challenge is that information security costs are often not explicit. High security standards may arise in higher procurement costs, as the cheapest supplier does not provide the right security capabilities or it increases training costs as regular and updated security awareness training is required in addition to the existing training program. Given these challenges it is important to address the financials but it might not be the right strategy to start off your investment argument with the numbers game. Ever asked yourself why do people buy? Why not turn your board into your customers and align your security investment plan to the buying process?

3 Key Questions:

- How to make Information Security stick (and not get lost in technicalities)?
- How to turn the decision makers into ambassadors?
- How to demonstrate that Information Security plays a vital role in business growth?

Tools used during the (interactive) session:

- Start with Why (Simon Sinek)
- Business Model Canvas (Osterwalder, Pigneur & al. 2010)
- Risk Management (isaca.org)

Materials to Support:

How to gain influence and buy-in for Security investment from the Board?

Session 2

Ravindra Jugdav

Information Security Manager

Rentokil Initial

Session Leader: **Ravindra Jugdav**
Information Security Manager Africa, Middle East, Baltics, Nordics & Caribbean – Rentokil-Initial

Session Title: **Cloud Security – The Facts: Customer Responsibilities for Security in Cloud Computing**

The majority of businesses in South African have a focus on cloud strategies to enable their business availability for the customer and workforce. From a Security perspective there is a common concern around the clarity of roles and responsibilities of the end user when it comes to the areas bullet pointed below.

Provider Competencies
Contracting provider
Disaster recovery
Guidance and assurance whilst migration is taking place (on-premise into the cloud)

Desired Outcomes for:

What are the key challenges and issues in cloud from a security standpoint?
How long is data is stored, encrypted and transmitted?
Data privacy policy

- Where is the data stored?
- Who is responsible for data compliance?

Where is your product closing the gap from a security perspective?

- Where are the cloud provider partners covering the unsolved areas?

Materials to Support:

Customer Responsibilities for Cloud Security

CSA – SecaaS Cat 5 Security Assessments Implementation Guidance

OWASP – Secure Medical Devices Deployment Standard 7.18.18

CSA – Top Threats to Cloud Computing Deep Dive

Open Forum & Scenario Overview

Suren Naidoo

CISO

TFG

Session 3

Session Leader: **Suren Naidoo – CISO – The Foschini GroupSession**

Session Title: **Threat Intelligence Cyber crime is a global issue and everyone is exposed to it in some shape or form.**

As a community, we represent some of the leading organisations in South Africa, with a common interest of "protecting our brands" as well as protecting our business stakeholders and communities at large.

"Doing good never goes out of fashion"

One of the ways in-order for us to deal with our common enemies, is to utilise cyber threat intelligence to better "protect our houses" and communities.

"Are you willing to be part of a cyber threat intelligence sharing network?"

Materials to Support:

Microsoft Security Intelligence Report – Volume 23

Proposed Threat Intelligence Sharing Framework – Workshop

Community Survey

Session 4

Charlie Hinde

Senior Manager:
Information Security

The Foschini Group

Session Title: **Socialising InfoSec Policy**

Session Leader: **Charlie Hinde – Senior Manager Information Security – The Foschini Group**

Materials to Support:

InfoSec Local Findings – CISO Alliances Cape Town Chapter

Scenario Overview & Open Forum

Michelle Barnett

IT Risk, Governance and Compliance Manager

Cape Union Mart (Pty)

Session 5

Session Leader: **Michelle Barnett – IT Risk, Governance and Compliance Manager – Cape Union Mart (Pty) Ltd**

Session Title: **3rd Party Risk Management**

Synopsis:

A third party data breach is a nightmare in the making for any organisation, the consequences of such potentially include financial loss, reputational damage as well as penalties and operating restrictions that regulators might impose.

Organisations deploy a number of different approaches to third party risk management; some effective, others less so. For those that develop the most effective response there is significant opportunity. Gaining holistic visibility of the risks that third parties bring to organisations enables us to exploit, to the full, the opportunities that third parties' services bring to the table whilst mitigating the risk.

However, when a breach occurs it is essential that a plan is in place for dealing with third party data breaches before they happen. Breaches require immediate attention and valuable time can be saved by plotting out a response ahead of time.

Materials to Support:

Third Party Risk Management

CISO Alliances Testimonials & Feedback

- Session Leader: Christine Fahlberg – IT Security Manager – Truworths: both informative, interesting and practical. Combined knowledge experiences and insight with examples of practical insights.

- Suren Naidoo: Threat Intelligence. Although the external speaker was a let-down; Suren provided some good insight and feedback and I feel we made some progress here. I hope you can organize an online session with the actual external speaker.

- Christine's session provided great insight and I feel many info sec leaders can learn from her approach.

- Threat Intel sharing session was good but I feel our community particularly in Cape Town need more education around threat intel and we need to explore the basics first.

- 3rd party risk session by Michelle is very on topic, I do however feel the workshop component needed more structure. It did however get discussion going which is important.

- Influencing & Buy-in for Security investment from the Board – Christine did a great job. I thought the content was very well structured and relatable and found all the tips and debates very useful. It was very practical insights into an important topic.

- I also thoroughly enjoyed Suren's session on Cyber Intel. It was engaging and led to good debate. Again, practical discussion not just theory or best practice stuff that don't work in practice. It highlighted the issues with collaboration and culture and legal responsibility to your company.

- The reserve bank input highlighted the need to structure objectives of a session clearly to the people providing input. I felt a bit bad for him – as it looked like he was thrown in at the deep end with no prep or context to the topic or his role in it – but Leigh I think rescued that session well – by summarising it and identifying clear next steps.

- Information Security Policy topic ran out of time – and I'm not sure if Charlie felt cheated from meeting his objectives for that session. Maybe that topic can be raised again.

- The session on Influencing & Buy-in for Security investment from the Board. Very topical.

- Finally, a platform that is content driven and not vendor driven. Due to its clear vision this format has the potential to become the key information security group to provide its members with the necessary ideas to drive competitive advantage.

H2 Alliances Activities

Executive Business Exchange

NORDICS
EASTERN EUROPE
BENELUX

Executive Business Exchange

NORTH AMERICA

CISO Alliances

LAGOS CHAPTER

Executive Business Exchange

SOUTH AMERICA

CXO Alliances

WINDHOEK CHAPTER

CXO Alliances

CAPE TOWN CHAPTER

Executive Business Exchange

Asia Middle East

CXO Alliances

Nairobi Chapter

CXO Alliances

Johannesburg Chapter

CISO Alliances

Durban Chapter

Executive Business Exchange

Australia

Alliance Chapters

Each taking place every six months
EBE formed as part of your
planning cycles

CXO Alliances
Business Transformation

Cape Town
Johannesburg
Nairobi

CXO Alliances
Securing the Business

Cape Town
Johannesburg
Nairobi

CISO Alliances

Lagos
Durban
Windhoek

Executive Business Exchange

Stockholm
Amsterdam
Oslo
London
Paris