CISO Alliances

Gauteng Chapter

1st September 2022

Results

ALLIANCE Media Group

Alliance - ‘A union formed for mutual benefit’

Community – ‘1: a unified body of individuals: such as. A: the people with common interests living in a particular area broadly: the area itself the problems of a large community’

Foreword

Leigh Thomas
Director & Founder

We are a team of ambitious and passionate executives with a desire for achieving the ideal.

We have experience in numerous industries in building and participating in C-level communities across the globe in Oil & Gas, Mining, Power & Enterprise IT, Info and Cyber Security, across multiple divisions across the business.

The core values of the Alliances Community were born along with Alliance Media Group appropriately put by the Collins dictionary definition - Alliance - 'A union formed for mutual benefit'. Everyone must feel like there is success and progression. This is only achieved with selflessness in sharing and candid feedback from all that we commit our time to.

We, as a group, no longer view this industry as B2B but P2P (Person to Person). Our intentions are to, and since August 2016 have been to create a trusted platform for people who are executives combating similar business objectives to leverage their collective experience to help one and other, debate opinions candidly for industry progression and professional growth and to benchmark strategies against one and other. This is the CISO Alliances community. Built by the community for the community.

Whilst understanding that every business will need to drive commercials to become sustainable in the modern world. We believe 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 where ego is the drive and industry professional growth. The industry was born off the back of 'Everybody wants to learn' and we 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.

2020 and the Digital environment has been forced for a remote workforce with limited human interaction due to the Coronavirus pandemic since March 2020. From this, our community representative have been relied upon even more for business enablement. From the event space environment, even more events companies have found an overnight solution of plaguing diaries with event upon event, with revenue driven activities. As an organisation, we will shy away from this and only invite the community to engage when justified. We will also, not be looking for time commitments of more than an hour or two as we understand that life is continued, in the remote style of operating business currently. With every hope that we can safely run physical chapters as soon as possible.

Overview

Date: Thursday, 1st September 2022

Time: 8:00am – 14:30pm

Venue: Verona 1, The Pivot

Location: Montecasino Boulevard, Fourways, Johannesburg, 2055, South Africa

The Alliances chapter is a gathering consists of business risk, information and cyber security leaders who have been highlighted as being able to offer value in terms of content and influence. It is designed to form alliances and to drive progressive change in the business world and beyond.

The content and format is designed to talk together, learn better and experience more.

Format: Up to 40 Leaders debating pertinent, real life issues through the form of open forums, workshops and Panels.

Outcomes:

1. Depth achieved around business objectives where the opportunity of experience within the attendees is leveraged
2. Benchmarking and verification of thought processes outside of existing networks i.e. the broader CISO Alliances community
3. Industry progression and unity in impacting the challenges of the common business objectives
4. Not corporate flag waiving or sales pitches. We insist, do that elsewhere.

Themes:

Understand the purpose of the day, order of the day and your role throughout the day
Third Party Risk for a connected ecosystem
Data Security: Understanding the Threat within
Mind the Gap – impacting the skills gap quicker
What do Boards want to see?
Any other business and carrying on the conversation to the post-alliances

08:00
Registration

08:40
Welcome Remarks & House Keeping
Leigh Thomas, Director – CISO Alliances
Session Outcome: Understand the purpose of the day, order of the day and your role throughout the day

8:45
The Warm Up Quiz
Short Quiz on the Recent Breaches which we Should have Learnt from
Jaco Swanepoel, Senior Cyber Response Analyst – Absa Group Ltd
CISO Alliances Quiz Master

9:00
Session 1 - Workshop
Third Party Risk for a connected ecosystem
Session Leader: Robin Barnwell
Session Builders: Nadia Veeren-Patel, Oscar Stark, Steve Jump.

10:30 **Networking Break**

10:50
Session 2 - Customer Insights
Data Security: Understanding the Threat within
Martin Nortje, Fallon Steyn, Chris Denbigh-White

11:35
Session 3 - Workshop
Mind the Gap – impacting the skills gap quicker
Oscar Stark, Zakiyya Cassimjee

12.30 **Networking Lunch**

13:15
The Warm Up Quiz
Short Quiz on the Recent Breaches which we Should have Learnt from
Jaco Swanepoel, Senior Cyber Response Analyst – Absa Group Ltd

13:30
Session 4 - Open Forum
What do Boards want to see?
Oscar Stark, Zakiyya Cassimjee

CISO Alliances

Gauteng Chapter
September 2022

Use Case Partner

Qush

Networking Partner

CYBER 1

Community Attendees

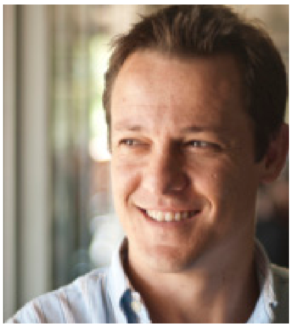
Jaco Swanepoel
Senior Cyber Repsonse Analyst
ABSA

Colin van Niekerk
Head: Cyber Security Operations Centre
ABSA

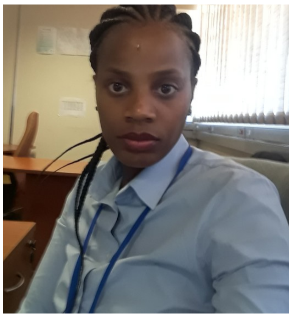
Louise Van Der Bank
CIO
Afrisam

Zakiyya Cassimjee
CIO
Astute Financial Services Exchange

Stephen Mark
CSO/ CIO
Bankx



Lloyd Vassard
CIO
Barrows



Nozipho Morajane
IT Risk & Information Security Officer
Bayport Financial Services

Paul Kankwende
Group Head of Infromation Security
Bayport Financial Services

Fundile Ntuli
Regional Director: Botswana, Mauritius, Namibia, Zambia & Zimbabwe - CISO Alliances

Steve Jump
Executive Director
Custodiet

Jayson O'Reilly
Cyber Security Risk Officer
Cyber One Solutions South Africa

Tendai Chinhamo
IAM Analyst
DeBeers Group

Mineshree Narsai
Security Officer
Discovery

Abdul Baba
CTIO
Infrstructure South Africa

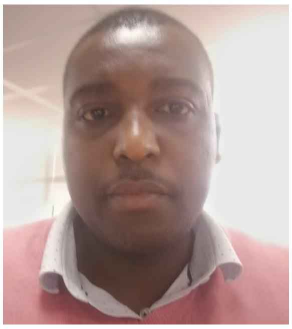
Martin Nortje
Information Security Engineer
Investec

Oscar Stark
Divisional Director Technology Centre of Excellence
Liberty Holdings

Community Attendees

Rashid Ishmail
Head of Security Strategy
Liberty Holdings

Nadia Veeran-Patel
ISO
LRMG



Nhlanhla Xaba
Information Manager
Mediclinic Southern Africa

Doc Gule
IT Security Officer
MINTEK

Terence Fogarthy
Opco Ops: Security Head
MTN Group

Fayyaadh Adams
Campaign Specialist
Old Mutual

Allen De Klerk
Head IT Security
Postbank

Chris Denbigh-White
Global Director of Customer Success
Qush Security

Fallon Steyn
Regional Sales Manager - MEA
Qush Security

Ishaaq Jacobs
Chief Cyber Security Officer (CISO)
Sasol

Patrick Devine
Sales Director
Solid8 International

Alan Visser
Group Executive Media Technology Infrastructure
South African Broadcasting Corporation

Tapiwa Mandividza
Senior IT Manager: IT Governance, Information Security, Risk & Compliance
Right to Care

Miyoba FaithSichimwi
IT Security Officer
South African National Accreditation System (SANAS)

Olwethu Sinxoto
Head: Information Security
Standard Bank Group

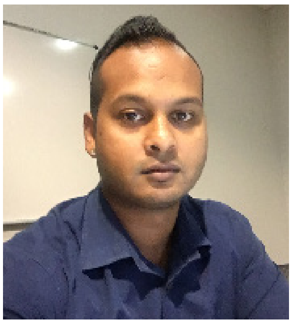
Robin Barnwell
Head: Security Strategy
Standard Bank Group

Community Attendees

Kevin Wilson
GM Group IT
Stefanutti Stocks Holdings

Reg Green
Senior Manager Information Assuarance
Telesure

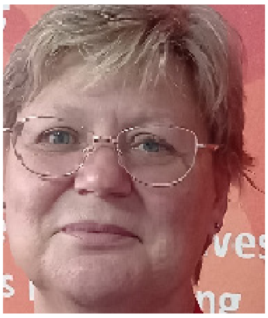
Joseph Stokes
Cyber Security Operations Manager
Telesure



Nelesh Baichan
Cyber Security Management
Tiger Brands

Xolani Lukhele
General Manager: ICT Governance, Risk & Security
Transnet SOC

Deeren Vallabh
Senior Manager: Data and Information Governance
Universal Healthcare



Stefnie Viljoen
ISO
Universal Healthcare

Darshan Lakha
Head of Cyber Security SA
Vodafone Africa

Johan Taute
Manager Cyber Defence
Vodafone Africa

Test Your Knowledge

08.45 - The Warm Up Quiz

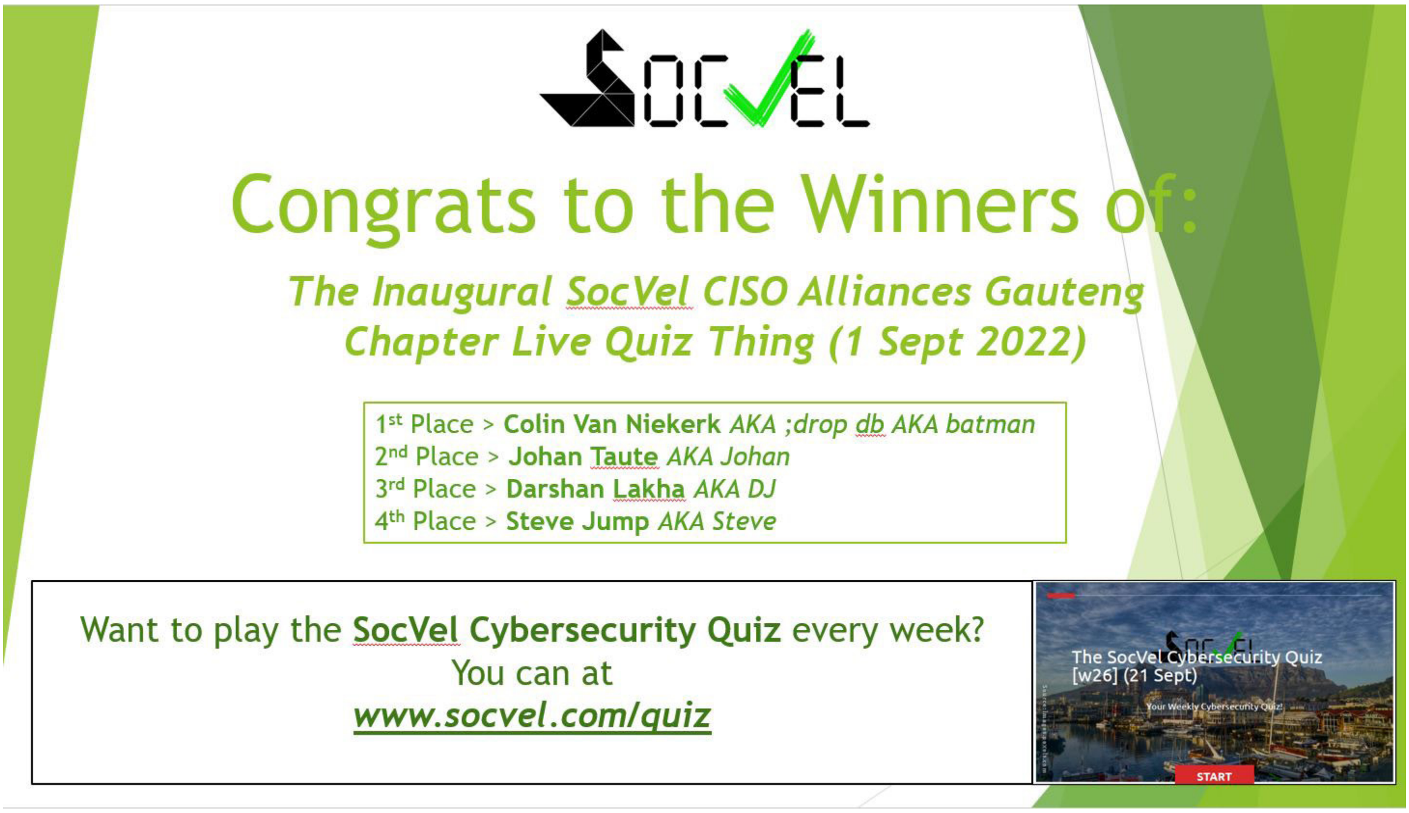
Short Quiz on the Recent Breaches which we Should have Learnt from

CISO Alliances Quiz Master

Jaco Swanepoel, Senior Cyber Response Analyst – Absa Group Ltd

Session Overview and Synopsis:

- Identify the most powerful CISO Alliances Member Quiz Mind



SocVel

Congrats to the Winners of:

The Inaugural SocVel CISO Alliances Gauteng Chapter Live Quiz Thing (1 Sept 2022)

1st Place > **Colin Van Niekerk** *AKA ;drop db AKA batman*
2nd Place > **Johan Taute** *AKA Johan*
3rd Place > **Darshan Lakha** *AKA DJ*
4th Place > **Steve Jump** *AKA Steve*

Want to play the **SocVel Cybersecurity Quiz** every week? You can at *www.socvel.com/quiz*

The SocVel Cybersecurity Quiz [w26] (21 Sept)

Your Weekly Cybersecurity Quiz!

1st

Colin van Niekerk

2nd

Johan Taute

3rd

Darshan Lakha

4th

Steve Jump

Workshop

Standard Bank

9.00 - Session 1

Third Party Risk for a connected ecosystem

Session Leader

Robin Barnwell

Session Builders

Nadia Veeren-Patel

Oscar Stark

Steve Jump

Session Overview and Synopsis:

Businesses are becoming more connected and dependent on 3rd parties.
This interconnected ecosystem means that 3rd party risk management has to evolve.

- Have point-in-time risk assessments evolved to assess the changing ecosystem risks?
- Have legal / regulatory obligations improved the quality of risk assessments?
- How do you scale 3rd party risk management in smaller organisations?

Session Outcomes and Takeaways:

This open discussion will pose these questions and more and leave the audience with some practical approaches on how to start or mature their 3rd party risk programme.

CISO Alliances

Johannesburg Chapter

Workshop Unpacking

Third Party Risk for a connected ecosystem

www.alliances.global

September 1st 2022

SESSION LEADERS

ROBIN BARNWELL

STEVE JUMP

NADIA VEERAN-PATEL

OSCAR STARK

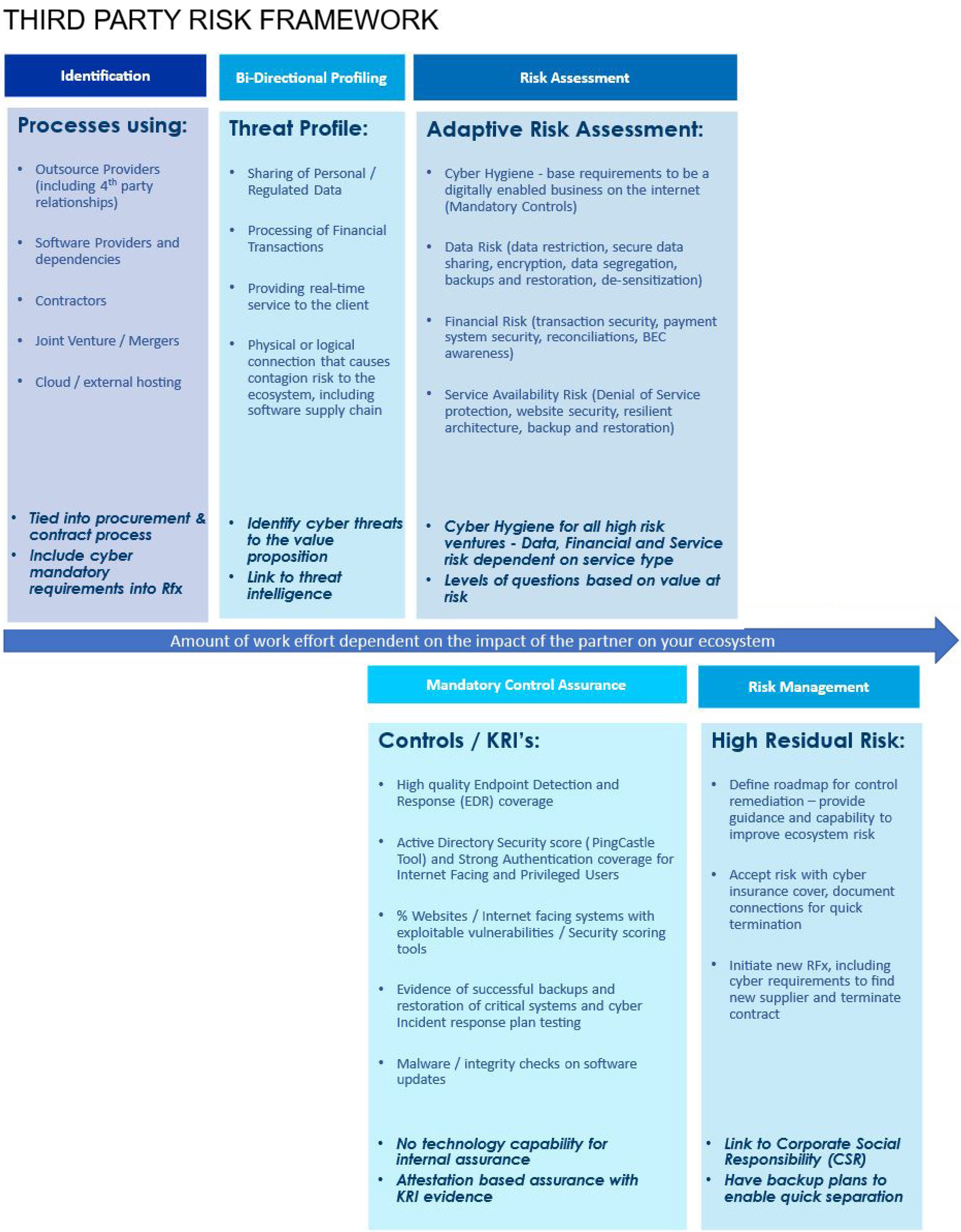
Takeaways

THIRD PARTY RISK FOR THE CONNECTED ECOSYSTEM

Businesses are becoming more connected and dependent on 3rd parties/partners/joint ventures to provide value to clients and shareholders. This interconnected ecosystem, facilitate by interwoven processed and technology, means that traditional 3rd party risk management has to mature and evolve to:

- Have cyber requirements as a quality metric in RFx process and contract, not just price and SLA;
- Be adaptable depending on the type of relationship:
  - Public cloud providers - shared responsibility risk model
  - Technology / software suppliers – dependent of supplier's internal quality control
  - Outsource providers - dependent on client security requirements
  - Partners and M&A - shared value and risk model
- Be scalable by having early warning triggers to ensure the work effort is focussed on high risk ventures;
- Be bi-directional - cyber risk has to be assessed and assured in both directions of the relationship;
- Develop Key Risk Indicators (KRI's) that allow the move from point-in-time risk assessments to continuous assurance; and
- Meet a changing and evolving threat landscape
- Validation of information provided in risk assessment (as opposed to a check box exercise)
- Bigger organisations to provide smaller organisations in their ecosystem with assistance to become more secure

Takeaways



THIRD PARTY RISK FRAMEWORK

Identification

Processes using:

- Outsource Providers (including 4th party relationships)
- Software Providers and dependencies
- Contractors
- Joint Venture / Mergers
- Cloud / external hosting

- ***Tied into procurement & contract process***
- ***Include cyber mandatory requirements into Rfx***

Bi-Directional Profiling

Threat Profile:

- Sharing of Personal / Regulated Data
- Processing of Financial Transactions
- Providing real-time service to the client
- Physical or logical connection that causes contagion risk to the ecosystem, including software supply chain

- ***Identify cyber threats to the value proposition***
- ***Link to threat intelligence***

Risk Assessment

Adaptive Risk Assessment:

- Cyber Hygiene - base requirements to be a digitally enabled business on the internet (Mandatory Controls)
- Data Risk (data restriction, secure data sharing, encryption, data segregation, backups and restoration, de-sensitization)
- Financial Risk (transaction security, payment system security, reconciliations, BEC awareness)
- Service Availability Risk (Denial of Service protection, website security, resilient architecture, backup and restoration)

- ***Cyber Hygiene for all high risk ventures - Data, Financial and Service risk dependent on service type***
- ***Levels of questions based on value at risk***

Amount of work effort dependent on the impact of the partner on your ecosystem

Mandatory Control Assurance

Controls / KRI's:

- High quality Endpoint Detection and Response (EDR) coverage
- Active Directory Security score (PingCastle Tool) and Strong Authentication coverage for Internet Facing and Privileged Users
- % Websites / Internet facing systems with exploitable vulnerabilities / Security scoring tools
- Evidence of successful backups and restoration of critical systems and cyber Incident response plan testing
- Malware / integrity checks on software updates

- ***No technology capability for internal assurance***
- ***Attestation based assurance with KRI evidence***

Risk Management

High Residual Risk:

- Define roadmap for control remediation – provide guidance and capability to improve ecosystem risk
- Accept risk with cyber insurance cover, document connections for quick termination
- Initiate new RFx, including cyber requirements to find new supplier and terminate contract

- ***Link to Corporate Social Responsibility (CSR)***
- ***Have backup plans to enable quick separation***

Customer Insights

10.50 - Session 2

Data Security: Understanding the Threat within

Session Leaders

Martin Nortje

Fallon Steyn

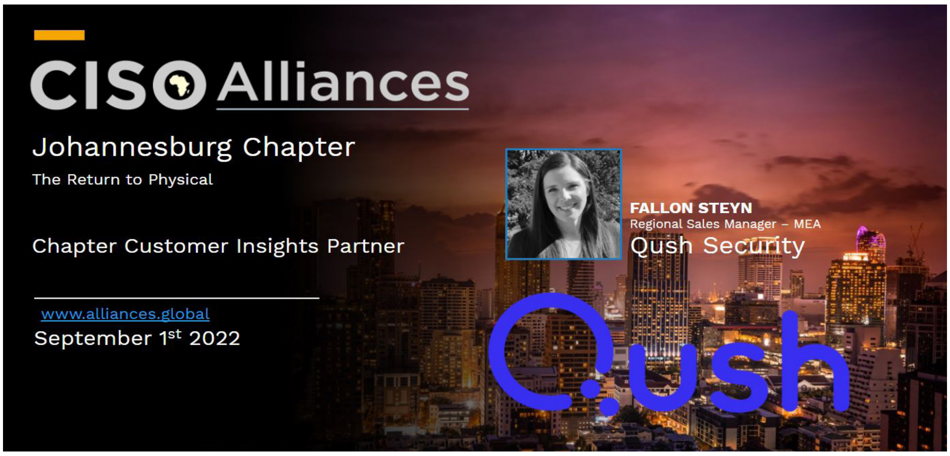
Chris Denbigh-White

Some insight into Qush Security –
https://techcentral.co.za/qush-infosec-prevention-always-better-than-cure-qusprom/214118/

Qush

A MESSAGE FROM THE CHAPTER PARTNER

FALLON STEYN



CISO Alliances

Johannesburg Chapter

The Return to Physical

Chapter Customer Insights Partner

www.alliances.global

September 1st 2022

FALLON STEYN

Regional Sales Manager – MEA

Qush Security

Qush

I was given the opportunity to bring Qush into the MEA region and coming from a reseller/partner background I wanted to take a different approach to our market. I wanted to be able to stand out and target the right audience. Making a noise amongst thousands of other vendors is a challenge on its own, now bringing something fresh and sexy to this region and disrupting the DLP and Insider Risk narrative, it was crucial and it was needed to take a different approach.

I spoke to several CISO's in my network and the CISO Alliances kept coming up as the one community whereby I had the chance of making the impact we needed to make. When I met with Leigh in person we got along well, and we have similar goals on how to work together in fighting cyber security but also how do we help our CISO's protect and keep their jobs and organisations safe.

When we reached out to one of our flagship clients, they were more than happy to speak to the community and give their reasons behind the choice to go move forward with Qush.

When we reached out to one of our flagship clients, they were more than happy to speak to the community and give their reasons behind the choice to go move forward with Qush. Martin told his story beautifully, his analogy around the castle resonated with everyone in the room which was appreciated.

After the CISO Alliances Chapter, it has exceeding mine and my colleague's expectations. It's great to see there is a platform where professionals can meet and discuss and collaborate on how they can work together to improve their day-to-day jobs. A CISO needs to have broad shoulders as the weight of their responsibility is a heavy one, I am grateful to each person at this Chapter affording us the opportunity to take part. Listening to their worries and challenges, aligning and working together with them meanwhile leveraging off the Qush technology I believe will help take a little weight off their shoulders.

Thank you for the warmth during and after the chapter. It's been great getting to know you.

Workshop

11.35 - Session 3

Mind the Gap – impacting the skills gap quicker

Session Leader

Oscar Stark

Zakiyya Cassimjee

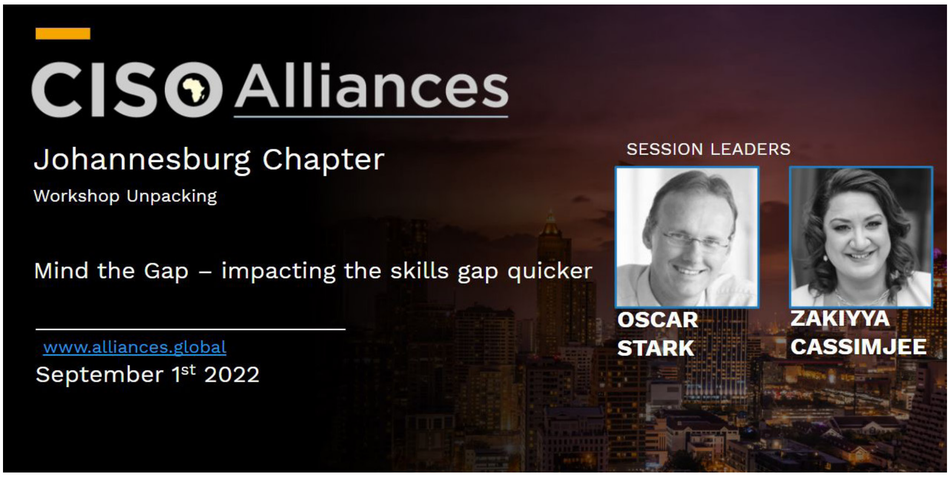
Session Overview and Synopsis:

Very few people share a common career journey, but most share common learnings. How can one draw on these common learnings to help enrich the CISO Alliances community, but in a way that it can be setup to be reused.

Session Outcomes and Takeaways:

1. Deep insight into common career lessons learnt by Security Professionals
2. A measurement framework for skills development
3. Actionable takeaways to deal with the skills gap

CAUSE OF SESSION 3



CISO Alliances

Johannesburg Chapter

Workshop Unpacking

Mind the Gap – impacting the skills gap quicker

www.alliances.global

September 1st 2022

SESSION LEADERS

OSCAR STARK

ZAKIYYA CASSIMJEE

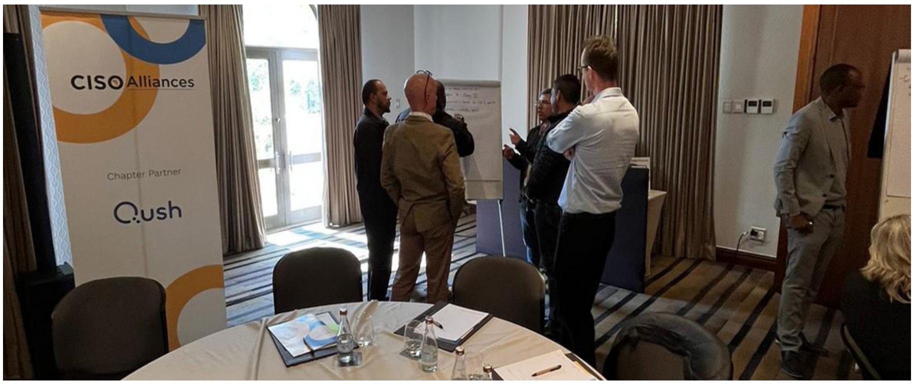
Very few people share a common career journey, but most share common learnings. It is these learnings which can serve to help address the growing Cybersecurity skills gap, and support individuals in their professional development.

Cybersecurity continues to be a significant threat to governments, businesses and individuals around the world. Worldwide, around 80% of organizations suffered one or more breaches that they could attribute to a lack of cybersecurity skills and/ or awareness. These cybersecurity challenges are compounded by a workforce shortage; there simply aren't enough people with the required Cybersecurity skills needed to fill open jobs.

The nature of this problem is global. It estimated that by 2025, there will be [3.5 million cybersecurity jobs open globally](), representing a 350% increase over an eight-year period, according to Cybersecurity Ventures Magazine.

In addressing this growing concern that organisations invest in the Cybersecurity workforce to ensure there are enough people with the skills needed to deal the growing risk of attacks and protect the digital ecosystems they operate in, but it is also critical that Cybersecurity professionals step in to help solve the skills requirements as they are often on the receiving end of it.

The multi-dimensional nature of the skills required to operate in the Cybersecurity environment, asks of all who practise in it to become lifelong learners. It is upon the leanring community represented in the CISO Alliances to leverage off each other to help close the gap on Cybersecurity skills.



An Enterprise Framework for Managing Cyber Risk
Cyber Measurement and Reporting

TAKEAWAYS

Drawing on the CISO Alliance community the following common learnings where shared to serve as reference to closing the skills gap. They are categorised as follow:

- How to address the problem:
  - The nature of the skills gap problem requires a multi prong approach, recognising that organisational and personal dynamics differ – once size does not fit all.
  - There is an opportunity to create common solutions to solving skills, like common training content, which can be used to help drive more consistent resolution to the skills gap problem.
- Awareness:
  - Establishing awareness around the Cybersecurity skills gap is critical to help mobilise resolution.
  - There are three common levels at which it is suggested awareness is driven:
    - Society at large - Helping to educate the population as to why Cybersecurity is important, how it impacts them, and how they can help promote the importance of it.
    - Corporates – The role of Cybersecurity to help sustain the business activities, and how that draws on a plethora of different skills.
    - Education institutions - In this regard, specific emphasis is placed on education institutions to influence students. The view is that the earlier one can engage with children, preferably at school level, the sooner they can appreciate the opportunity. Tertiary academic institutions would in turn then serve as grounds to ensure industry relevant skills are developed, fed from the schooling systems interest.
- Skills pipeline:
  - Deciding how to build and establish the subsequent skills pipeline is critical.
  - Recognising that there is limited individuals in the market that carry extensive experience, skills and certifications - don't expect that all your talent will reach this level in the short-term. Rather focus on building basic skills base, and allow people to grow their abilities over time.
  - Establish corporate mobility for people who want to move into Cybersecurity. Often the organisation treats experienced senior talent as juniors when they want to change their careers.
  - Partner with other companies or suppliers to help develop talent. Create exchange programmes which allow people to more rapidly grow their scope of exposure, between organisations.
  - Run an intern program to build a pipeline of future capacity. This point was commonly highlighted by attendees, delving into some handy details to consider:
    - First establish that the organisation wants to utilise the intern model to grow skills. Typically the Human Resources department has a valuable role to play in this regard.
    - Establish where to recruit candidates from. In this regard, what basic academic acumen is required, and what relevant traits are you looking for. Attitude in this regard, quite often trumps qualifications.
    - Setup a program to drive the development of the interns, supported by structured education, hands-on problem solving and constructive guidance. In this regard, interns that have already completed their internship, can serve as great guides to new mentees, if properly incentivised.
    - An often overlook opportunity is leveraging tax incentives to offset intern remuneration against.
    - Most intern programmes will result in some interns who complete their internship to leave the organisation. This attrition should be seen as a success, as oppose to failure, as these ex-interns are helping to build a larger community of Cybersecurity practitioners. At the end of the day you are training people for a career.

Open Forum

13.20 - Session 4

What do Boards want to see?

Session Leader

Oscar Stark

Zakiyya Cassimjee

Session Overview and Synopsis:

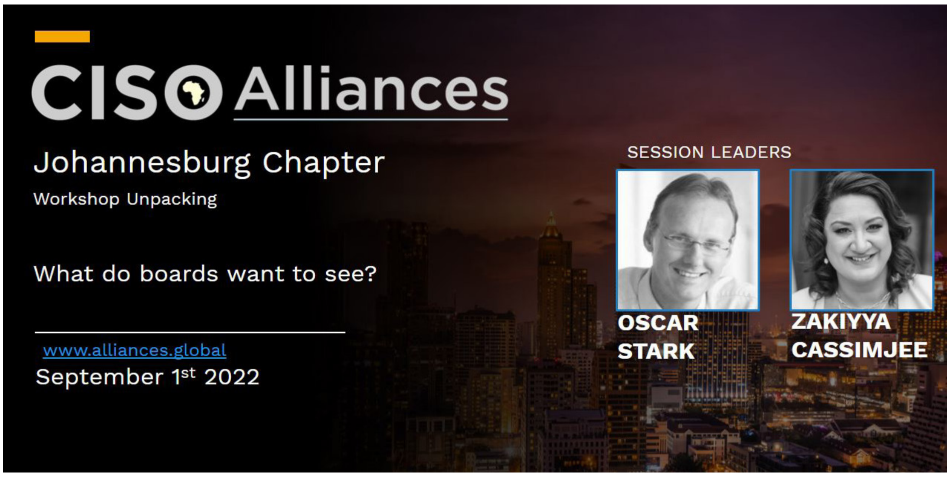
Conversation at Board level often deal with various dynamics. Regularly the CISO is prepared to account for how the risk landscape is changing > how the Information Security and Cyber strategy is designed to address it > what actions are underway to reduce risk in the environment > to how well the controls are performing. But these might not be adequate to deal with some of the more probing realities that the board wants to understand.

In this session we will draw on the collectives experience to help frame what are some of the less appreciated aspects to cover in a board engagement, and help make the information security and cyber conversation more relatable to business.

Session Outcomes and Takeaways:

1. Shared experiences around what boards are looking
2. Distilled guiding framework for approaching board engagement

CYBER SECURITY BOARD COMMUNICATION



CISO Alliances

Johannesburg Chapter

Workshop Unpacking

What do boards want to see?

www.alliances.global

September 1st 2022

SESSION LEADERS

OSCAR STARK

ZAKIYYA CASSIMJEE

The engagement at a Board level is critical for any Chief Information Security Officer (CISO) to establish the required support, but also help provide assurance that adequate efforts are underway to manage the risk exposure of the organisation, as an ever evolving risk category due to the nature of business (This well stated in the King IV guidance to Boards). Drawing on the collective understanding of the CISO Alliances members the following key points where highlighted as being involved in the Board engagement:

- All Boards are not the same, but have to operate in complement to the enterprise risk framework of an organisation. Here it is not just about IT risks, but the business as a whole, and serves as the backdrop to contextualise the conversation in. Framing the Cybersecurity strategy and the plan to execute against it, needs to play out against this backdrop. It is vital to help convey the strategic risk posed by Cybersecurity focusing on effect of it in context to risk impact, organisations reputation or brand, and cost to the organisation.
- Boards carry legal responsibilities expedited as oversight, and helping them understand the legal and compliance implications of Cybersecurity is critical to their role in helping to sustain the organisation. In this regard, ensuring that the matter of Cybersecurity is adequately represented on the Board agenda is vital. It can further be enhanced by helping the Board gain access to Cybersecurity expertise, on the Board, to support the management of the risk.
- Frame the conversation to help carry across how risks are addressed by controls, and how these are providing adequate or inadequate coverage for the organisation. This level of detail may vary from one Board to another, but typically lies at the heart of the plan in play. This is also to appreciate that within large organisations their might be different Boards that carry specific focus areas that you have to relay your message to complement their optic on the matter.
- When Boards need to judge performance, it is always good to have some benchmarking data that can be used as a yardstick. This context helps broaden the appreciation of the topic, as the realities of the organisation are not insular in nature, and can be compared to similar industry players or conditions in active market environments. Auditors, being internal or external, have a similar role to play in providing opinion of effectiveness of Cybersecurity efforts.
- Some valuable precursors to the board engagement is to keep the language simple so that they can understand – no acronyms or jargon. Leverage the strength of visuals. Risk conversations are often best understood with some colour notation, where red could represent it needs attention and green is, it is in hand.

With all this in mind one needs to remember that when engaging with your Board one needs to manage a conversation, in which you might be asking for something, or wanting to convey a specific point. Make it easy for the Board to recognise it, as your success depends on it.

Recommendations from the community

- None. Great format
- No suggestion. Liked the format.
- None, I liked this format
- Representation from all the local Banks
- Collaboration
- More ‘encouraged participation’ from attendees
- More sessions :)
- More quizzes!
- Run the sessions for the full day to enable more in depth discussions
- Happy with the current format aligns nicely
- More time to debate the topics before feedback, just as we were getting up to speed, the time was out
- Keep it up, nothing needed to improve
- It was my first Alliances Chapter attendance and cannot comment on anything, everyone that was there wanted to be there and they believe in this Chapter.
- None specifically, but keep it up!
- Really isn’t much to add here. One tiny thing is that I needed power to charge my laptop and that was a bit tricky as there were no power ports, but obviously when encouraging people to be interactive this isn’t really a factor. Also something like recording the sessions would be difficult and not allow people to open about their thoughts.

Food for thought

4.8
out of
5

Chapter Content Scored by the community

4.8
out of
5

Chapter Format Scored by the community

Qush Content Score by the community

4.2
out of
5

Qush Format Score by the community

4.3
out of
5

Chapters Best Sessions as voted for by the community

1

Session 1
Third Party Risk for a connected ecosystem

2

Session 4
What do Boards want to see?

3

Session 2
Data Security: Understanding the Threat within

Testimonials

Reg Green

Very helpful forum where we brush shoulders with like minded industry peers to collaboratively address and resolve issues

Stefnie Viljoen

Sharing and brainstorming important ISO matters

Stephen Mark

A great place to learn and occasionally share

Olwethu Sinxoto

Growth. Networking. Collaboratation.

Allen De Klerk

Valuable resource for like minded professionals to network

Steve Jump

An opportunity to meet peers, and to payback shared learnings into the group

Zakiyya Cassimjee

An amazing community of people willing to share, learn and teach at the drop of a hat. A whole tribe !

Jaco Swanepoel

First time attending a CISO Alliances session. It's still weird how surprisingly engaging the session were, and how 'friendly' and inviting the participants were.

Deeren Vallabh

A well formatted workshop to bring the information security community together to collaborate, network and bring thought leadership to challenges faced by all.

Louise van der Bank

The CISO Alliance in my view provides a great platform for Information Security executives and professionals to connect and engage. It provides the opportunity for all participants to share and to gain relevant knowledge.

Joseph Stokes

A dynamic environment where ideas flow freely and challenges are raised within a community of like-minded professionals to solve together.

Testimonials

Jayson Thomas O'Reilly

It allows me to understand what South African CISO's are facing and their varying levels of maturity and acknowledge that many are engaged at a highly operational level and sometime and not aways understand the strategic value they fulfil

Nadia Veeran-Patel

An opportunity to share, collaborate and debate issues and thoughts about different strategies to achieve our goals. We all have the same problems, just different ways to tackle them

Kevin Wilson

As a dual hat CIO / CISO I am getting to learn from the crowd. This is not my primary role, and my sector is not leading or very good at putting focus on security. This helps me see where I should be aiming my efforts, and to learn from mistakes of others.

Ishaaq Jacobs

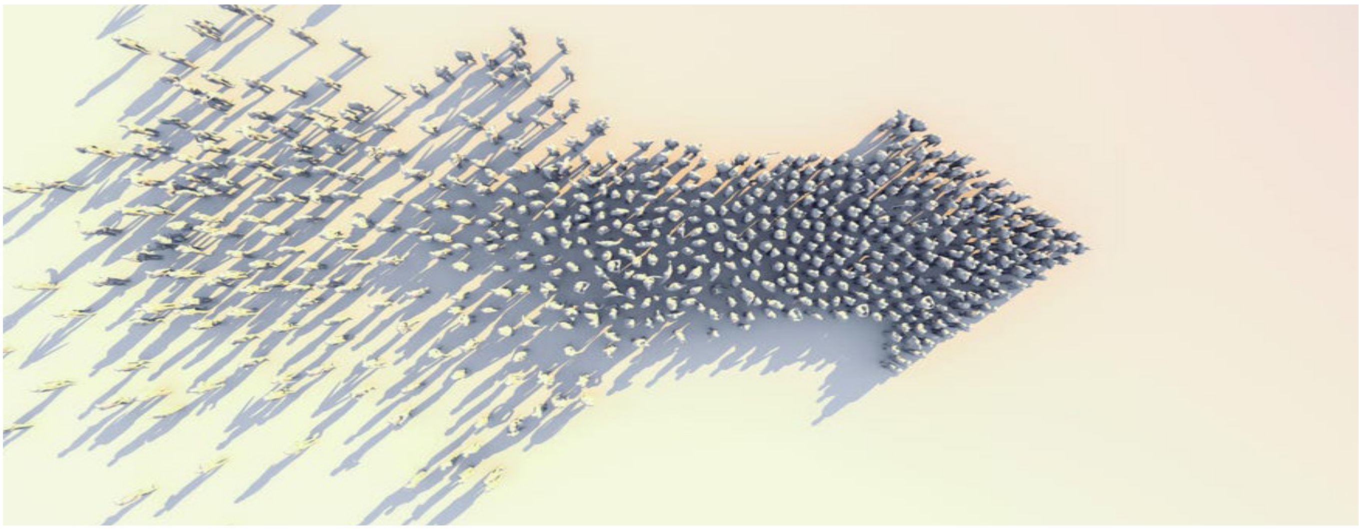
Advise, mentorship and guidance from experts who care.

Terence Fogarty

CISO Alliances offers a great way to share information amongst like-minded senior managers in Information Security. It provides a constructive method to collaborate on these ideas and challenges faced at different companies.

THE NEW CISO

ARE YOUR PERCEPTIONS ALIGNED? CISO REPORT

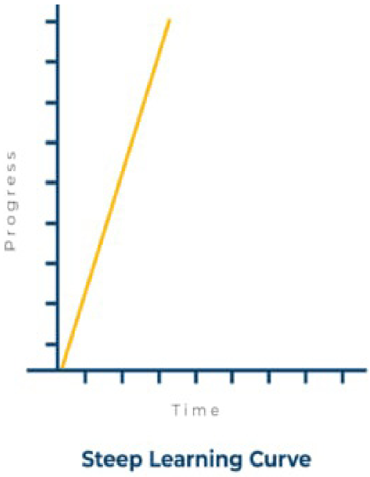


Chief Information Security Officers (CISO's) often get stuck in the operational aspects of their jobs due to talent shortages and fall short to expand their roles to play across multiple dimensions of the organization. This challenge is compounded by major talent shortages in the Cyber Security landscape that makes finding & keeping cyber specialists challenging, let alone grooming them into a future CISO. Reflecting the mirror back at the CISO, it is also worth appreciating that the demand that the organisation is placing on them is changing, moving from a more basement engagement (dealing technical issues) to where they are called on to support boardroom (strategic direction setting and execution) discussions.

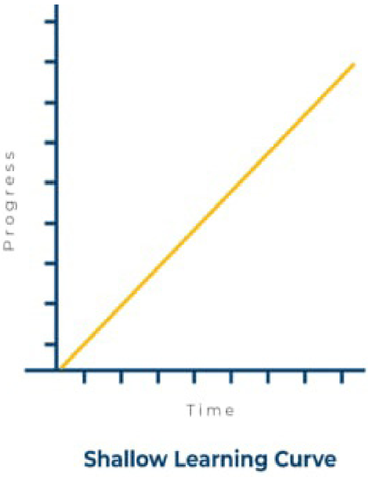
These realities are not always well expressed by organisations, and might contrast or conflict with individuals personal aspiration for growth and development of their respective careers. This reality was highlighted through survey results by a significant CISO sample pool, where, although more than 50% of CISO's who started their career in the Technology field, envision their future role to transition operating at an Executive or Board level role.

Only 12,5% of respondents believe that their current and future role will be similar. This data correlates with industry statistics, which indicate more than 50% of people are not happy with their careers, and 76% of people in companies are looking for growth opportunities.

This brings into sharp focus the urgency in which organisations will



Steep Learning Curve



Shallow Learning Curve

have to build mechanisms to accelerate upskilling, certification and internal mobility to enable Cyber and Information Security (Cybersecurity) professionals to meet the future demands of their ever evolving roles. As the average global tenure for a CISO in a role is now 3.2 years, CISO's will need to not only leave a legacy but also a viable successor or two in the wings who have been ramped up through a steep learning curve. With this backdrop, hardliners might feel that if people ship off to greener pastures you can just hire an alternative. The realities are however that globally there is a 3,5 million Cybersecurity Workforce shortage, with organisations on average expanding their Cybersecurity teams by 15%.

This sketches a picture, that even if you wanted to, "outhiring" for skills shortage is not plausible. There are however options to tackle this situation, from being deliberate around career path development, focusing on closing skills gaps, grooming successors or running talent development pipelines. The process to leverage one or more of the options, rooted in a simple yet effective deliberately driven engagement comprising out of the following steps:

- Skills audit – understand if the existing skills in play are sufficient to meet current and future objectives.
- Skills gap – identify your teams technical bench strength to meet your technology and business strategy, and how the existing skills stack up against known industry benchmarks.
- Build customized learning paths leveraging of recognised learning platforms to support the individual in their learning journey.
- Change manage to drive outcomes – ensure that the development efforts are incorporated into the work effort, to ensure value from applying new found knowledge, through the aid of personal development plans.
- Skills at hand when you need it – incentivise staff to stay committed to the company as their skills grow to ensure that the skills are accessible to the organisation over the long-run.

The majority of respondents (78%) would suggest that that the largest impact on their career will be a result of personal and industry influences. Organizational influence is not seen as a majorly impactful factor in the life of a CISO. A reality that is collaborated by the fact that 74% of organisations have no formal knowledge transfer, and the average global tenure of a CISO is 26 months. This pressure cooker situation is not stacked in favour of the organisation, especially if one appreciates that the future earning expectation of most responders in the survey are pegged in the R2m plus per annum salary bracket. Not an unrealistic number if compared to what can be obtained as a remote worker in this skillset.

Reflecting on the data, and the realities experienced in industry, there is a strategic imperative for each organization to enable and speed their CISO's efforts and investment in growing and securing their successors. This would also allow current CISO's to pursue their own growth paths. The demands of the organisation on a CISO to know the business from basement to boardroom, and play across the technology to business continuum creates great opportunity, but if unsupported by the organisation in their growth aspirations, will most likely be supported by another organisation.

Authors; Oscar Stark - Chief Strategic Enterprise Architect for the Liberty Group, MCom, CISSP, ACE(MIT) and Eugene Brockman - Manager of Tech Talent Solutions for Capitec, B.Com, MIT Cert in Org Design for Digital Transformation

WHAT TO EXPECT

CISO Alliances

Alliances - A union formed for mutual benefit
Everyone is expected to contribute

Access to a community of peers to benchmark, support and debate

Non-discriminatory community on race, gender, age, vertical experience

Community First,
Commercials Last

An opportunity to engage on the Chat forum, Digital Alliances Chapter and Physical Chapters

WHAT WE EXPECT

This is a supportive environment for progression and growth

You do not directly benefit from topics being raised but, have experience within the topic:
1 - Share your knowledge
2 - Bring forward themes / topics that matter to you and your business objectives

Suggest and recommend peers to broaden the perspectives within the group

Constructive comments rather than opinionated are provided. Back up your opinion

If there is a potential eventuality of commercial gain for the organisation you work for, you will be expected to pay to play to help sustain the Alliances and their activities.

THANK YOU
WE HOPE YOU ARE ENJOYING THE JOURNEY

CISO Alliances

Gauteng Chapter
September 1st 2022

www.alliances.global