CISO Alliances

Johannesburg Chapter

12th March 2020

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

Varonis Executive Exchanges

08:30 – 09:00

Registration

09:00 – 09:15

Housekeeping, purpose driver and format reminder

Leigh Thomas – Director & Founder - CISO Alliances

09:15 - 10:00

Session 1 - Open Forum - Cyber Risk Ontology

Steve Jump – Head: Corporate Information Security Governance, Telkom

10:00 - 10:30

Session 2 - KnowBe4 - Security Awareness – Best Practices

Anna Collard – Managing Director Popcorn Training

Liza Weschta – Head of Sales and Marketing: Africa

10:30 - 11:00

Networking Break

11:00 - 11:45

Session 3 - Open Forum - Trust Experience – who do you really trust?

Oscar Stark – Chief Specialist: Strategic Architecture, Liberty

11:45 - 12:15

Session 4 - Microsoft - Intel being collated to build

Colin Erasmus

Johannes Kanis

12:15 - 13:00

Networking Lunch

13:00 - 14:00

Session 5 - Cloud Security Workshop

Justin Williams – Executive: Group Information Security, MTN Group

14:00 - 14:30

Session 6 - Security Analytics Open Forum

Pragasen Pather – GM: Governance Risk and Security, Sun International

Closing Remarks & the Next Steps

CISO Alliances

Johannesburg Chapter
12th March 2020

Networking Partner

VARONIS

Networking Partner

KnowBe4
Human error. Conquered.
Formerly known as Popcorn Training

Networking Partner

Microsoft

Thank you for supporting the Alliances, SS Consulting & T-Systems.

Attendees

Mia Andric	Director	Infosec Live
Mark Baatjes	Regional Sales Manager	BeyondTrust
Nelesh Baichan	Cyber Security Management	Tiger Brands
Nomaphelo Baloyi		Mastercard
Sheldon Bennett	Managing Execuitve: Cyber Security	Vodacom
Anna Collard	MD Popcorn Training	KnowBe 4, Formerly Popcorn Training
Yolanda Cornelius	Security Governance Officer	Discovery
Gerhard Cronje	Head of Cyber Information Security Unit	SOUTH AFRICAN RESERVE BANK SARB
Jashwin Dayaram	Head of Enterprise Architecture and Planning	Liberty Holdings
Louis De Kock	South Africa - Country Business Development	Varonis
Emmerentia du Plooy	Head of Information Risk Government	Standard Bank Group
Nastassja Finnegan	Cyber Security Officer	FIRST RAND GROUP
Andrew Ford	Senior Systems Engineer	Varonis
Doc Gule IT	Security Officer	MINTEK
Sheldon Hand	BU Leader	IBM Security SA
Rashid Ishmail	Head of Security Strategy	Liberty
Steve Jump	Head of Information Security Governance	TELKOM/BCX
Johannes Kannis	Cloud and Enterprise Business Leader	Microsoft
Ian Keller	CSO	SBV
Thelma Kganakga	CISO	MTN
Shalendra Kundalram	Global Business Services Exectuve	Adcorp Holdings
Charles Sello Kungwane	Chief IT Security Officer	IMPERIAL AUTO PARTS DIVISION/MOTUS
Jacques Lourens	CISO	Nedbank
Xolani Lukhele	Principal Specialist Security Risk & Compliance	AcelorMittal SA
Mafaiti Maclaud	CISO	SA POST OFFICE LTD
Funzani Madi	CISO	JSE
Itumeleng Makgati Group	CISO	Sasol
Celia Mantshiyane	CISO	Coca-cola Beverages Africa
Simphiwe Mayisela	MD	SS-Consulting
Jenny Mohanlall	Group Chief Information And Security Officer	Sturrock And Robson Industries
Tebogo Mokoena	Head of Information Security	Bayport Finance
Russell Nel	Independent Privacy & Data Protection Consultant	Privacyconsulting
Pragasen Pather	GM: Governance Risk and Security	Sun International
Garith Peck	Director - Regional Sales and Key Accounts Africa	BeyondTrust
Susan Potgieter	Head: Strategic Services	SABRIC
Oscar Stark	Divisional Director Technology Centre of Excellence	Liberty
Mosa Tladi	Information Security Manager	Luxaviation
Sam van der Westhuizen	Business Development Manager	KnowBe 4, Formerly Popcorn Training
Nadia Veeran-Patel	Cyber Resilience Advisory Manager	Applied Cyber Defense Systems
Justin Williams	Executive: Group Information Security	MTN Group
Colin Erasmus	BG Lead M&O WWL	==Microsoft

Apologies from

Robin Barnwell	Head: Security Strategy	Standard Bank Group
Noleen Ilunga-Muleya	Head of Digital (Consulting)	SA Government
Paul Kankwende	GM/Head IT Infrastructure and Security	Motus Financial Services
Hetisani Maringa	IT Risk and Compliance Manager	ubank
Zaine Miller	CIO	Sun International
Dudley Petersen	CIO	Department of Cooperative Governance & Department of Tradition Affairs
Dr. Kiru Pillay	Chief Director: Cybersecurity Operation	South African Department of Telecommunications and Postal Services (DTPS)
Arashad Samuels	Secops Africa	Cisco
Reander Botha	Cyber Security Manager	OUTsurance
Sandro Bucchianeri	Group Chief Security Officer	ABSA
Ian de Klerk	ACD & Network Security Specialist	T-Systems South Africa
Corjee Du Plessis	Senior Manager: Global Operations, Security & Architecture	Nampak
Dario Fachin	Head of IM, Global Information Security	DeBeers Group
Jacques Fouche	Senior Specialist: Information Security Analyst	TELKOM/BCX
Selvan Govender	Security Operations Manager	T-Systems South Africa
Dr Denisha Jairam-Owthar	CIO	City of Johannesburg Metropolitan Municipality
Loritta Kudumba	Head of IT GRC	Barloworld Equipment
Vickus Meyer	Divisional Technology Officer	NEDBANK
Maphelo Mpofu	Security Operations Manager	FIRST RAND GROUP
Fundile Ntuli	CIO	ubank
Lushen Padayachi	Group Information Security	Massmart
Julian Ramiah	Group CISO	Alexander Forbes
Gadija Ryklief	Divisional Executive Information Security	Edcon
Zunaid Vanker	CISO	Standard Bank Group
Kevin Wilson	GM Group IT	Stefanutti Stocks Holdings

Remember why you are here and thank you for being part of the build.

Open Forum

Session 1

Steve Jump

Head: Corporate Information Security Governance

Telkom

Session Title: Cyber Risk Ontology

Session Leader: Steve Jump – Head: Corporate Information Security Governance, Telkom

To establish an unambiguous terminology to communicate actual cyber risk across business groups and management levels. From technical attack level through to strategic risk. Allowing effective value based actions to be both taken and funded.

Materials to Support: Cyber Risk Ontology

Steve Jump – Cyber Risk Ontology - Session 1 Feedback

I found Steve Jump's presentation to be the most interesting. I was very valuable indeed.

Brilliant exercise to get people out of their comfort zone

What Jumps to mind :) Great presentation with great lessons learned

Great exercise. Look forward to seeing the outcomes. Could be packaged to use internally in my organization.

Interesting activity which confirmed what I've assumed for a while: we don't know how to communicate between levels of an organisation and there are often no standards within organisations. An exercise to replicate within my own teams / client environments.

Excellent workshop, shows the real problem you would have getting a problem through to the board

The format was good and demonstrated the challenge of communicating security at different levels in the organisation. I was hoping to get more ideas on how this can be resolve

Good practical exercise. Might be good to create a training manual around it

Yes, this was a valuable exercise on how quickly the wrong message can go up to board level.

Communication is key and this was very well articulated how different audiences communicate. expectations are very important and often IT staff forget that

Good ice breaker it really did highlight the broken telephone phenomenon. Proper communication is vital to ensure that all stakeholder have a similar view to the issues at hand.

Great session, the workshop bit really got the discussions going in all different directions.

Great session and brilliant methodology used for discussing the session

Excellent perspective on how communication up and down the hierarchy of organisations should be approached. Very relevant for security given the urgent need to raise awareness at an executive level.

Valuable session that gave me opportunity to connect all levels of professions when incident of occurs . It challenged me to think what message and how to present certain information at different levels.

Open Forum

Steve Jump

Head: Corporate Information Security Governance

Telkom

Captured Comments

The results of the exercise however are very interesting. Without a doubt they show that cross-level communication is almost non-existent.

So far that is the easy part.

What seems obvious from these comments is that each layer of reporting is only aware of its own context. So although this is a very limited scope test at first glance it appears to prove our original hypothesis.

The initial conclusion is that we really do need to teach each level how to report their situation and its meaning in the context of their adjacent reporting structures

It is very easy to laugh at some of the assumptions came out of the exercise but I think we will agree that we have encountered exactly this in a real business environment.

Given that our team members where multidisciplinary there appears to be very little insight from this mix. Again confirmation that attitude and amplitude rule in a business context.

This is nice data, but too small a set to be of any statistical significance, so we really need to run this again across multiple groups, perhaps I might ask your indulgence to use CISO alliances as a platform for this?

How we do this in the time of coronavirus might prove interesting, but an online collaborative exercise seems plausible, if quite hard to engineer.

	Operational Management Technical, Operational, Network, IT Logistics, Engineering, Manufacturing **Reports to Tactical>**	**Tactical Management** Product, Sales, Service Delivery, Store, Systems, Warehouse, Factory, Retail **<Instructs Operations – Reports to Business>**	**Business Management** Sales, Finance, HR, Procurement, Regional, IT, Business support systems, Legal **<Instructs Tactical – Reports to Exco>**	**Exco – Strategic Management** Board & Strategy, C-Level Management, Shareholder, CEO, CFO, CIO, CxO **< Instructs Business**
1				
2				
3				

	Operational Management Technical, Operational, Network, IT Logistics, Engineering, Manufacturing **Reports to Tactical>**	**Tactical Management** Product, Sales, Service Delivery, Store, Systems, Warehouse, Factory, Retail **<Instructs Operations – Reports to Business>**	**Business Management** Sales, Finance, HR, Procurement, Regional, IT, Business support systems, Legal **<Instructs Tactical – Reports to Exco>**	**Exco – Strategic Management** Board & Strategy, C-Level Management, Shareholder, CEO, CFO, CIO, CxO **< Instructs Business**
1				
2				
3				

Operational Management Technical, Operational, Network, IT Logistics, Engineering, Manufacturing **Reports to Tactical>**	**Tactical Management** Product, Sales, Service Delivery, Store, Systems, Warehouse, Factory, Retail **<Instructs Operations – Reports to Business>**	**Business Management** Sales, Finance, HR, Procurement, Regional, IT, Business support systems, Legal **<Instructs Tactical – Reports to Exco>**	**Exco – Strategic Management** Board & Strategy, C-Level Management, Shareholder, CEO, CFO, CIO, CxO **< Instructs Business**
3	1	6	5
Firewall stats on an incline	We are experiencing a high volume of activity on our security technology	Is this normal? Which security technology? (contact Is this out of the ordinary for this time of month?	COME TO MY OFFICE
Someone deleted active directory	Users are unable authenticate to their computers	Why? How can service be restored	Don't ask me!!
Outbound traffic to suspicious IP	There is a potential breach that is being investigated	What's the impact? What symptoms are being observed	Don't ask me!!
Potential zero day exploit	We have a potential vulnerability	Patch it! Why can't it be patched?	Don't ask me!!
5	3	2	1
Discovered a new malware suspected ransomware	Antivirus update System patched Were suspicious activities noticed?	Investigate forensics on suspicious Infected servers to be reported on next month	Digital forensic investigation in progress Report due next month / next board meeting
Spyware on the CEOs laptop	Targeted attack	20% of Exec dashboard training	More training required for Exco
DDos on the perimeter network	Business system not available?	Productivity Down Days of service down Cost of business lost R2 million Critical business system	Critical business system outage Impacting productivity Financial loss of R2m
Spearphishing on the CFOs laptop	Check validity of email from the CFO	CFO email spoofed Monthly investigation Need stricter payment controls	Users receiving emails purporting to be from CFO Investigation in progress. Controls being improved.
1	2	5	4
Microsoft SMB– V3 Vulnerability announced without patch	Zero day apply mitigating controls Affects 20% environment No patch	Network/system isolation Validation of sensitive information being compromised Risk/issue identified which affects 20% of the environment CSIRT activated	CSIRT activated Dealing with information breach affecting 20% of environment; Potential reputational impact for PR to deal with.
Hard drive failure on MS– exchange server	Critical failure–Email to be restored from DR	Provide updates Clarify issue	No details on the issue
User clicked on a fishing link–PA of CEO	Ransomware exposed region affected through fishing	Execute incident response Impact? Regional office– incident response activated	Region off-line, Incident response is broken, Considering invoking BCP to minimize business impact
2	6	4	3
DC– shut down one client Multiple sites affected	Invoke incident management root cause investigation service restoration stop the bleeding	Incident process invoked for three incidents Awaiting details managing impact	No message for EXCO
Phishing attack:$500,000 Payment made	Invoke incident management root cause investigation service restoration stop the bleeding	Incident process invoked for three incidents Awaiting details managing impact	
DataBreach: 10,000 records leaked to Dark web	Invoke incident management root cause investigation service restoration stop the bleeding	Incident process invoked for three incidents Awaiting details managing impact	
6	4	1	2
Online banking is down	Customer service will be impacted for online banking platforms CallCenter volumes will be impacted	Online banking is down affecting CallCenter volumes	Invoke PR – calls alternate banking Temp staff to handle influx Vendor management third-party investigation
CEOs payslip found on the network printer	CEOs PII contained on payslip potentially exposed to some staff members. Potential PR/ID theft reputational impact	Potential leakage of CEOs personal information to internal staff member	HR involvement and containment. To deal with the employer

CFO approved urgent funds transfer request	Funds transfer approved not through normal channels by CFO; Explore change management process	Finance governance process bypassed on approval of fund transfer	Review process Automate process for stricter control Recover funds
4	5	3	6
AD. admins excessive privileges	Review of AD. admin access in line of policy Remediate Potential system or data compromise	We have compromise Need forensic investigation Need HR and legal Initiate incident	Who is involved? How much have we lost? Who needs to be notified? (Comms, Public comms, statutory reporting)
Coronavirus found on server (CTC)	Hand sanitizer deployed BCM deployed	Awareness – Impact customers – Remote working – What to communicate?	Invoke BCP DR etc
External mail compromise;	Block and purge emails	– Delay communication via email Platform – Alternative communications - ETA What's operational costs using other comms channel	Incident plan(BCP) Switch off emailFix it Communicate via social media and SMS

Six Teams were self selected based on location in conference area.
Each Team was given a blank template and asked to complete column one as Operations (5 minutes were allowed)
After the time elapsed each template was handed to next team, who were asked to complete their response as Tactical management (5 minutes were allowed)
The first column was folded behind the form and the next team was asked to complete the management column only using the 'report' from the previous team (6 minutes were allo
The second column was folded behind the form and the next team was asked to complete the Exco column only using the 'report' from the previous team (6 minutes were allowed)

Form distribution was arranged to ensure 4 different teams for each form

Teams were asked to complete only first three rows due to time constraint.

Thanks to Emmerentia du Plooy and Russell Nel for form co-ordination and general team wrangling

Steve Jump
+27813520045

Know Be4

Anna Collard

Managing Director

KnowBe4 Africa

Session 2

Session Leaders: Anna Collard – Managing Director Popcorn Training

Organisation: KnowBe4 Africa, Formerly Popcorn Training

Session Title: KnowBe4 Security Awareness – Best Practices

Focus of the Session:

Security Awareness – best practices

- Incentives, yes or no?
- Keeping engagement
- Showing Return of Investment/metrics
- What's coming soon

Takeaways:

- Social engineering is #1 attack vector
- Sharing what works and what doesn't work
- People can transform to become our strongest security assets – we just have to enable them.

Materials to Support:

African Cybersecurity Research Report
CLTRe-The7DimensionsSecurityCulture-ResearchPaper
Slides
KnowBe4

KnowBe4 - From a South African content perspective, is there any specific content that you would like to educate your users on?	KnowBe4 - What would it take for you to recommend KnowBe4 to one of your peers?	KnowBe4 - Would you be interested in sharing your experience with KnowBe4 as a case study?
Yes, Business Email Compromise	I can recommend KnowBe4 to my peers anytime	Yes
N/A	Getting through procurement	Depends, would consider it
Informative but more interactive would have been great	Yes, I would	Not at the moment
Love the product love the message. For people not using the product...well they are missing out	Not much....all they need to do is ask	Sure
Useful insights into running awareness campaigns in Africa and hearing how approaches have changed over time.	A great Organisation. Would recommend.	N/A
Thanks for the idea of getting “victims” to present back their own story - in essence turning them into champions for the cause: a cautionary tale - don’t let this happen to you. Otherwise general security awareness, tailored and practical and not too overwhelming - reinforcement and repetition of messages that have been provided for ages.	One of my clients already uses the platform - so with firsthand exposure to it, I can honestly say I love it! Just need to get their approach right (with the right buy-in, frequency, etc.)	Sure! Any time!
Glad to hear that there is free personal training available to anyone	personal training	N/A
Security for industrial control systems	A referral from a peer works mostly, that proves that there is value in the service.	N/A
Not specific	Nothing, have done so in the past	No thanks
Currently used in our environment lent New functionality	Yes	Yes, once we have matured
lack of corporate emails on public forums.		yes, always do.
Need to show more instances of cyber crime. Users don't "see" enough cyber crime reported on I'd like more content stories showing what could go wrong	I already to ☺	Already on board
Yes, communication to key and we need to look at awareness more in light with nudging end users to good behaviour instead of punishing bad behaviour.	Already starting the engagement with KnowBe4	Already starting the engagement with KnowBe4
N/A	I think that their approach is very valuable, and it is something worth mentioning to my peers.	Was very informative - especially looking at awareness through a lense of what you SHOULD NOT do.
Good content, well prepared	Happy to recommend them, well known in the market, feedback from our customer base is that they are reputable	Will not be relevant as our Security team in State runs with it
Great	Yes	Of course, yes
Sophisticated phishing including spear and whale phishing and how social engineering is used.	Better understanding of the offering and pricing	Have not used KnowBe4
Not at the moment.	They have good content I would .	No

Open Forum

Session 3

Oscar Stark

Chief Specialist: Strategic Architecture

Liberty

Session Leader: Oscar Stark – Chief Specialist: Strategic Architecture, Liberty

Session Title: Trust Experience – who do you really trust?

So your organisation is going digital, transforming the business and implementing technologies like Artificial Intelligence and Blockchain. And now you are bombarded with acronyms like customer experience (CX), and user experience (UX). But have you thought of the trust experience (TX)? Trust serves as fundamental anchor to enable transactions and lives in the fabric of the organisation. Trust is however not considered when building out experiences for customers to engage with the organisation or how new technologies implemented would impact it. What is more alarming, is when people assume that the security mechanisms they implement will naturally instil trust, but actually has the converse impact. This generally unowned territory of trust gets associated with information security and cyber, but what can professionals do to make trust a deliberate outcome?

This talk will delve into:

- What trust experience (TX) is;
- How one can be deliberate in designing trust into your engagement with customers;
- How trust experience relates to threat modelling, and
- How trust will serve as a business differentiator going forward

Some discussions points:

- Does your organisation even consider the customers trust experience and expectations?
- If you where to tackle this topic, who would you partner with in your organisation?
- What measures would you use to check that you are making an impact?
- Do you think the topic is even relevant?

Materials to Support:

Who do you TRUST?

Oscar Stark - Trust Experience – who do you really trust? - Session 3 Feedback

Great presentation. However, the question about 3rd Party opinion was not well addressed

Interesting view

Again great content, valuable info taken from the session

Good thought-provoking discussion. Aligns to thinking that building trust should be core to our mission and doesn't happen accidentally.

As always, a thought-provoking presentation. With the right level of drama and confusion building at the beginning but culminating in a very pertinent point. Thank you!

Great topic, I learned a lot and it is something I will explore more
I have zero trust, so the question is what is scarier, zero trust or blind trust

Interesting positioning but really a complex topic.

A new dimension to consider

Thank you Oscar I loved your segment
I know it was built for the techies BUT I will use it for Cyber awareness

Cyber awareness will only thrive where Trust has been built. and IT people don't really care about Trust because its fluffy

Trust is not a control. Trust is an enabler to ensure a long-term relationship between stakeholders. We need to be cognisant of our actions/processes which might affect the trust our various stakeholders have in us.

I trust Stark

Great content

Very lively discussion

Great and on point! No further comments.

Great perspective to Information Security . Important learning on how to understand and have expectation of trust from users in the organisation .

Microsoft

Session 4

Session Leaders: Johannes Kanis

Organisations: Microsoft

Session Title: Let Microsoft Security and AI Help Protect Your Business with Intelligent Security

Synopsis:

With more than 3,500 global security experts and $1B invested annually in research and development, we are making AI and automation work for our customers. Our business ready security solutions reduce noise by 90 percent, eliminate time-consuming tasks, and automatically remediate 97 percent of end-point threats. To help customers with these challenges, we recently released Microsoft Azure Sentinel which is a cloud-native security information and event manager (SIEM) solution that provides limitless cloud speed and scale, integration with existing tools and data sources, and faster threat protection with AI by your side.

Links:

https://www.microsoft.com/mea/security/

https://www.microsoft.com/en-za/trust-center

Slides

Microsoft

Microsoft - Session 4 Feedback

Good

No really, I think we all are aware of the what they offer
Nice tools if you have the budget

Would have been good to hear more around the ai ml capability of the product and less about generic information around it.

Thank you for answering questions candidly and for providing insight into the new tools, approaches and activities that Microsoft is investing in. Also for “sticking to the script” and not being too sales-driven.

It wasn’t informative enough on statistics

Nice high-level view of an available capabilities

Informative

Found a new functionality
session approach was great. Transparency and ongoing conversation is great.

Good presentation - didn’t really resonate with me

The new capabilities of the Azure cloud (Sentinel) are interesting and can add a lot of value to organisations.

Was good to know that MS is looking at investing in security and their cloud presence in SA

Was good to see how MS portfolio advanced

Great session

Microsoft products speak for themselves , great to know more products availability .

Cloud Security Workshop

Justin Williams

Executive: Group Information Security

MTN Group

Session 5

Session Leader: Justin Williams – Executive: Group Information Security, MTN Group

Session Title: Unpacking Cloud Security As a Community

Contextualised overview:

The Cloud is here whether you like it or not. Increased pressure from internal organisational customers and external solution providers is forcing organisations to progress on the cloud journey regardless of reservations.

There are several key components to security in any infrastructure—and the cloud is no exception. What is different about security in the cloud is where the responsibility for managing different security components lies.

With an on-premises solution, your organization is solely responsible for all aspects of security. In the cloud, a cloud service provider (CSP) may take responsibility for certain components of their infrastructure. Here's a table showing the typical allocation of responsibility for different IT security components for specific types of cloud services: See graph.

Source - www.compuquip.com/blog/cloud-security-challenges-and-risks

It's important to note that this table only represents a typical allocation of responsibility. Cloud service providers may have different allocations of responsibility outlined in their service agreements. The complexity only grows where application and service providers are introduced who are providing services built on top of the cloud provider as the responsibilities marked as CSP may now be distributed between multiple parties and tends to be even more vague.

Given this complexity, let us use the power of our community to further explore the key risks and challenges, share some of our experiences and challenges and possible solutions.

6 Subsections (and related questions)

- Lack of transparency, visibility and control
- Vendor lock-in
- Application of the Lockheed Martin Cyber Kill Chain in the cloud
- Cloud as an opportunity to optimise limited security budget
- Technical compliance challenges
- Legal, regulatory and governance compliance challenges

Expected outcomes and action areas (tangible returns)

- Possible solutions, successes and failures
- Sources of useful references material in relation to the section
- Recommendations for tools and services which organisations have successfully used in addressing the challenges

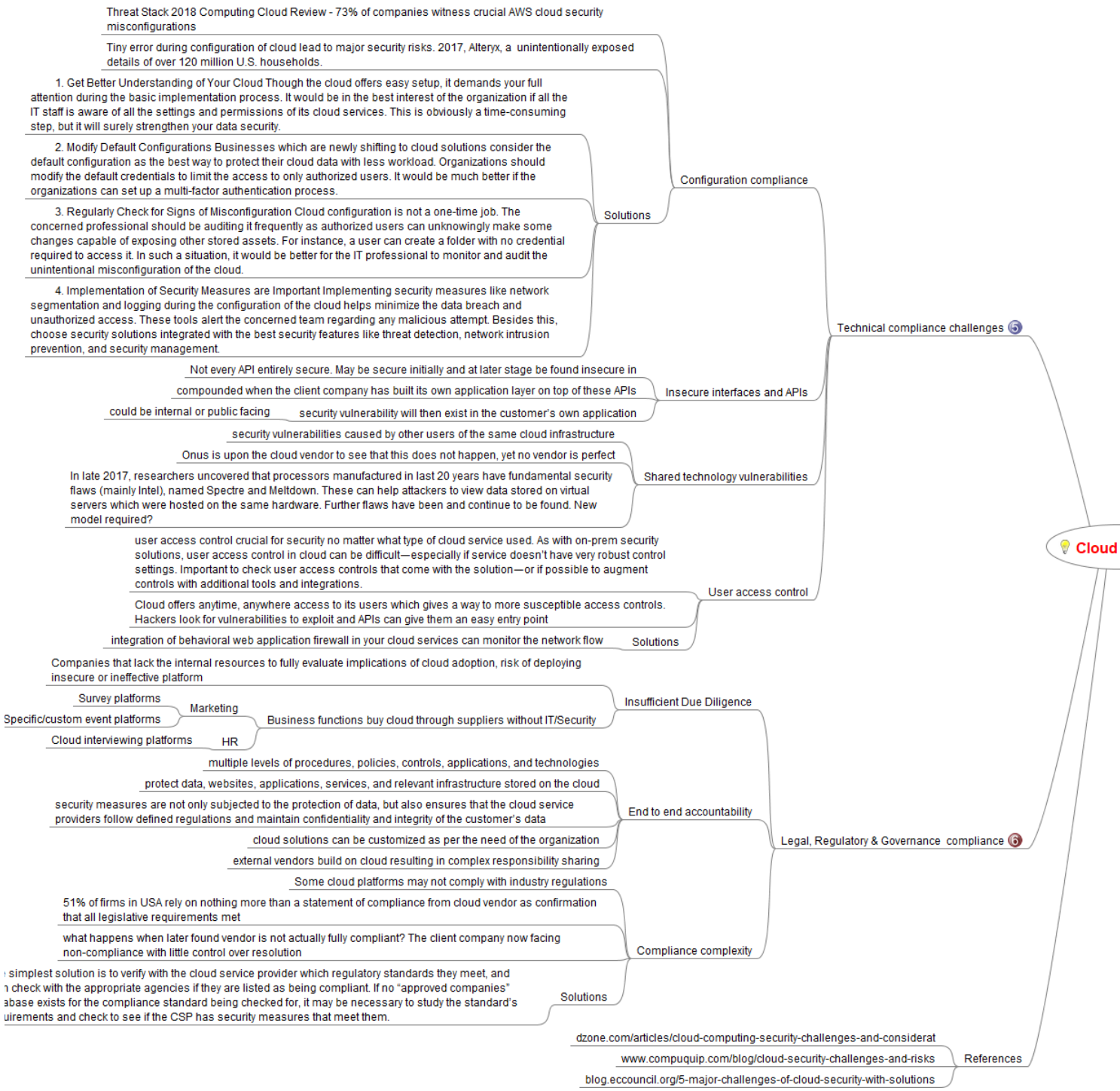
Cloud Security Slides

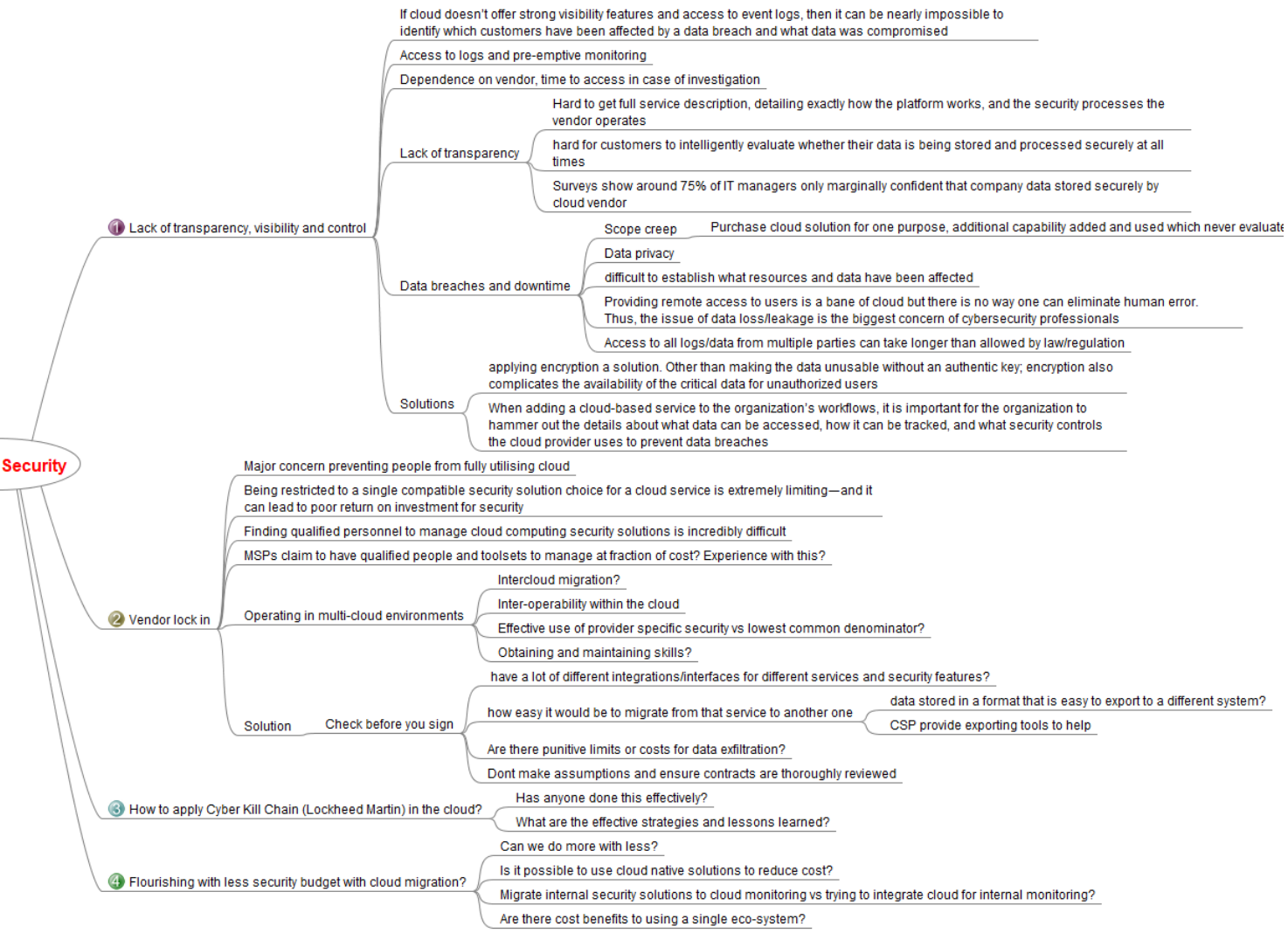
Cloud Workshop

Responsibility for Key Security Components in the Cloud			
IT Security Component	IaaS	PaaS	SaaS
User Access	You	You	You
Data	You	You	You
Applications	You	You	CSP
Operating System (OS)	You	CSP	CSP
Network Traffic	You	CSP	CSP
Hypervisor	CSP	CSP	CSP
Infrastructure	CSP	CSP	CSP
Physical	CSP	CSP	CSP

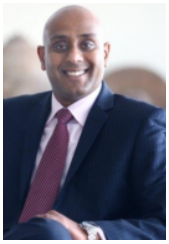
Cloud Security Workshop

Session 5




Security
1 Lack of transparency, visibility and control
If cloud doesn't offer strong visibility features and access to event logs, then it can be nearly impossible to identify which customers have been affected by a data breach and what data was compromised
Access to logs and pre-emptive monitoring
Dependence on vendor, time to access in case of investigation
Lack of transparency
Hard to get full service description, detailing exactly how the platform works, and the security processes the vendor operates
hard for customers to intelligently evaluate whether their data is being stored and processed securely at all times
Surveys show around 75% of IT managers only marginally confident that company data stored securely by cloud vendor
Data breaches and downtime
Scope creep
Purchase cloud solution for one purpose, additional capability added and used which never evaluate
Data privacy
difficult to establish what resources and data have been affected
Providing remote access to users is a bane of cloud but there is no way one can eliminate human error. Thus, the issue of data loss/leakage is the biggest concern of cybersecurity professionals
Access to all logs/data from multiple parties can take longer than allowed by law/regulation
Solutions
applying encryption a solution. Other than making the data unusable without an authentic key; encryption also complicates the availability of the critical data for unauthorized users
When adding a cloud-based service to the organization's workflows, it is important for the organization to hammer out the details about what data can be accessed, how it can be tracked, and what security controls the cloud provider uses to prevent data breaches
2 Vendor lock in
Major concern preventing people from fully utilising cloud
Being restricted to a single compatible security solution choice for a cloud service is extremely limiting—and it can lead to poor return on investment for security
Finding qualified personnel to manage cloud computing security solutions is incredibly difficult
MSPs claim to have qualified people and toolsets to manage at fraction of cost? Experience with this?
Operating in multi-cloud environments
Intercloud migration?
Inter-operability within the cloud
Effective use of provider specific security vs lowest common denominator?
Obtaining and maintaining skills?
Solution
Check before you sign
have a lot of different integrations/interfaces for different services and security features?
how easy it would be to migrate from that service to another one
data stored in a format that is easy to export to a different system?
CSP provide exporting tools to help
Are there punitive limits or costs for data exfiltration?
Dont make assumptions and ensure contracts are thoroughly reviewed
3 How to apply Cyber Kill Chain (Lockheed Martin) in the cloud?
Has anyone done this effectively?
What are the effective strategies and lessons learned?
4 Flourishing with less security budget with cloud migration?
Can we do more with less?
Is it possible to use cloud native solutions to reduce cost?
Migrate internal security solutions to cloud monitoring vs trying to integrate cloud for internal monitoring?
Are there cost benefits to using a single eco-system?

Security Analytics Open Forum



Pragasen Pather

GM: Governance Risk and Security

Sun International

Session 6

Session Leader: Pragasen Pather – GM: Governance Risk and Security, Sun International

Session Title: Security Analytics

Session Synopsis:

Not all organisations have extensive experience of Security Analytics in the region but the adoption is inevitable.

This session will provide those who have, an opportunity to benchmark, those who are tasting, some insight into lessons learnt from those who have and the rest, the benefit of both.

Slides: Security Analytics

Pragasen Pather - Security Analytics - Session 6 Feedback

Good session. Asked a few interesting questions. Good conversation. VODACOM guy a bit of a loud mouth.

Time to invest in a security analytical tool

Great topic and inline with my findings. The journey is one you should be taking some time with

Interesting practical discussion. Enjoyed this.

It's clear that there is not a single tool or approach to this, so opening up the discussion for us to learn from what others have experienced was particularly interesting. Loved the concept of an Enterprise Immune System! Thank you!

Informative on the discussion session

Shared interesting insight, would like to continue the conversation with Pragasen.

Good discussion

Confirming current AI deployment

this was a great session. it was good to understand the same pain points i have, is had by all...but perhaps how do we know resolve this.

Analytics, need to extend to Awareness.

Great Presentation though. enjoyed the discourse

Interesting conversation. We need a holistic view when adopting the security analytics tools.

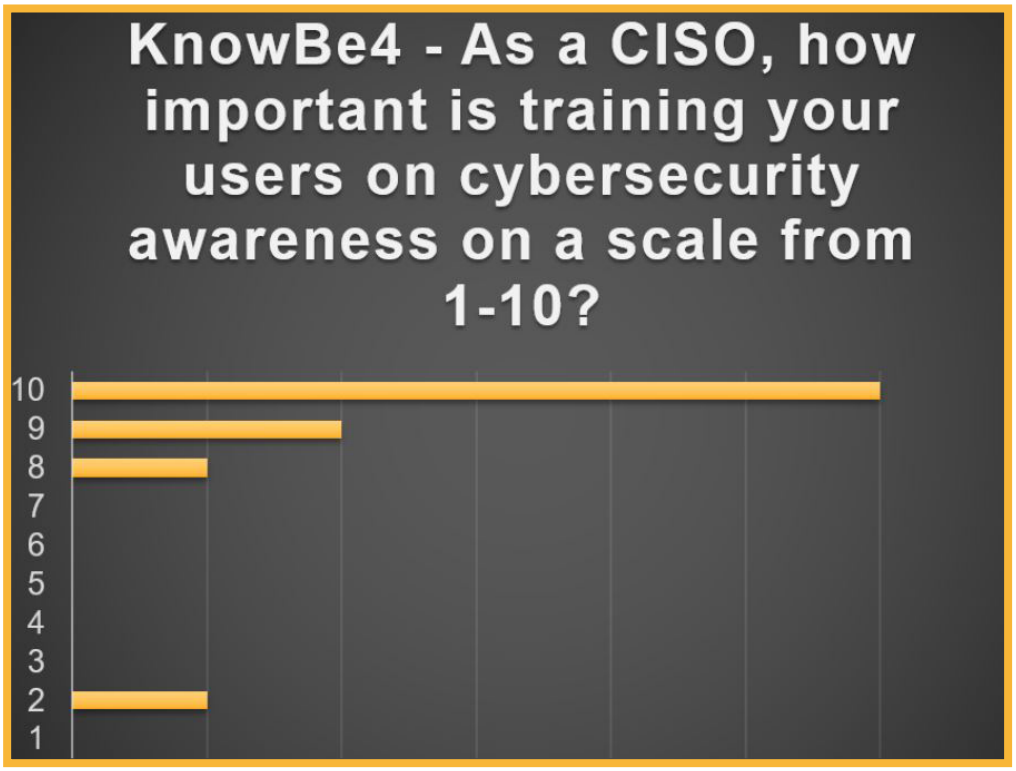
Great analogy USED to unpack analytics and AI.AI is here to stay, but use it within the constraints of your current business, and allow it to learn gracefully

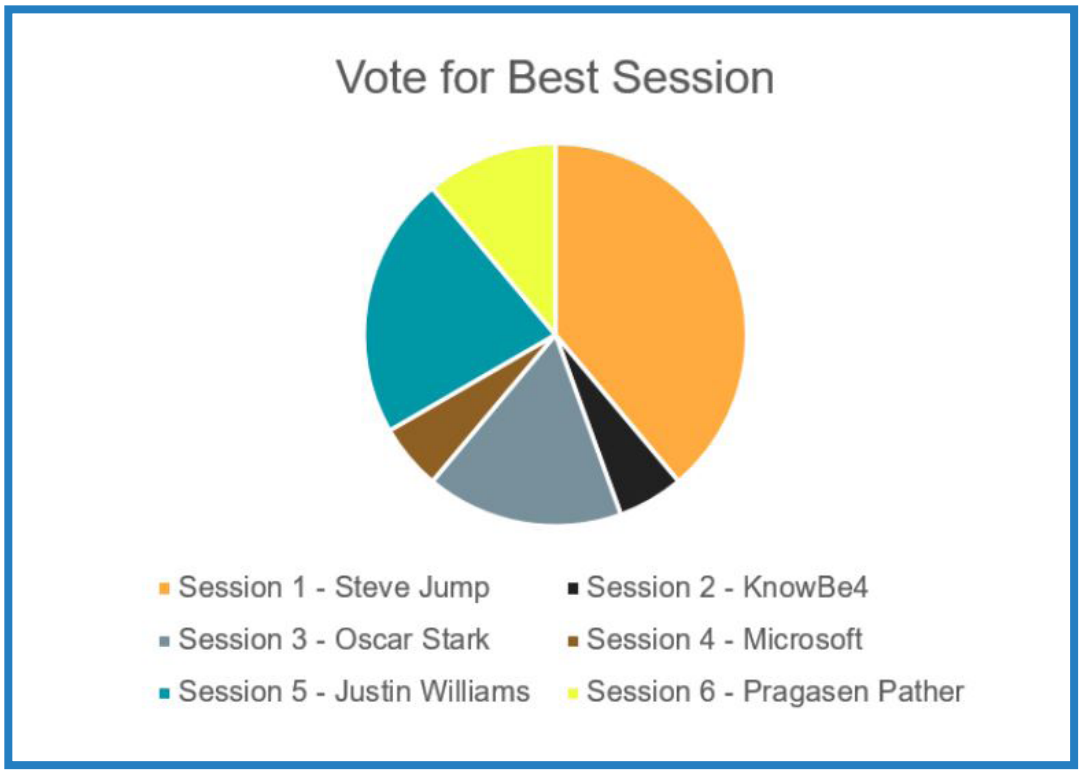
Nice to see how companies start to open around their experience, challenges and viewpoints

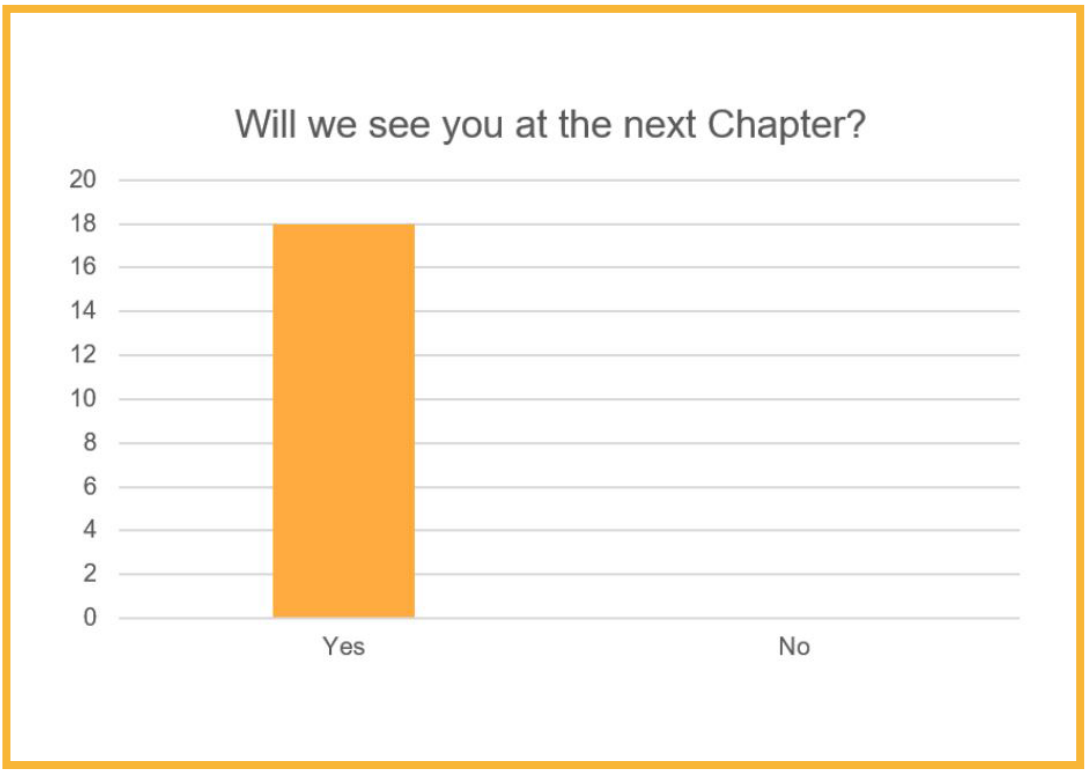
Great session

Very relevant - with threats increasing in frequency AI is critical

Great case study kind of session . Engaging and provided lesson to optimize what you have as a security professional


KnowBe4 - As a CISO, how important is training your users on cybersecurity awareness on a scale from 1-10?
10
9
8
7
6
5
4
3
2
1


Vote for Best Session
Session 1 - Steve Jump
Session 2 - KnowBe4
Session 3 - Oscar Stark
Session 4 - Microsoft
Session 5 - Justin Williams
Session 6 - Pragasen Pather


Will we see you at the next Chapter?
20
18
16
14
12
10
8
6
4
2
0
Yes
No

TESTIMONIALS

Simphiwe Mayisela

Excellent

Jenny Mohanlall

The Alliance Group is great networking and informative to hear what others are experiencing and sharing

Ian Keller

The best CISO event / group south of the North Pole

Justin Williams

A great day to share and engage with peers and benefit from their learnings.

Nadia Veeren-Patel

I loved it, thank you Leigh, you promised me s omething and finally someone has delivered on their promise

Oscar Stark

CISO Alliance still remains the best platform for real security discussions by security professionals for security professionals

Nelesh Baichan

If you spend more on coffee than Cyber security...You will be hacked

Yolanda Cornelius

Great platform that encourages safe sharing.
One can learn and take away from your peers without feeling that you will be in the press the next morning

Maclaud Mafaiti

This is a great opportunity for information sharing

Lukas van der Merwe

Engaging with and collaborating with industry peer in an open and authentic way is incredibly valuable. There needs to be much more platforms of open collaboration regarding cyber security to improve resilience. Very valuable and insightful!

Nomaphelo Baloyi

Best community , growing strong in SA .

Johannesburg Chapter 12th March 2020

Thank you to all our partners.

Thank you to all community members for their loyalty in creating an environment for themselves.

KnowBe4
Human error. Conquered.

Security Awareness Training and Simulated Phishing Platform

Helps you manage the ongoing problem of **social engineering**

KnowBe4 Security Awareness Training

Old-school security awareness training doesn't hack it anymore. Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks.

Baseline Testing

We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.

Train Your Users

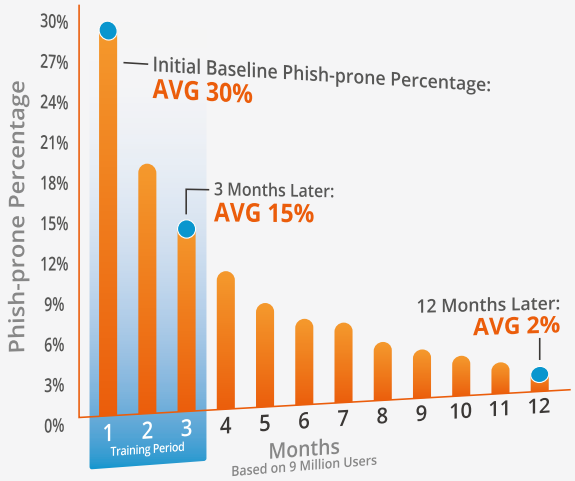
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users

Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

See the Results

Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!



The System Really Works

With KnowBe4's massive database, we analysed nearly 9 million users over the course of 12 months, and our 2019 research uncovered surprising results. The overall industry initial Phish-prone percentage benchmark turned out to be a troubling 30%.

Fortunately, the data showed that this 30% can be brought down more than half to just 15% in only 90 days by deploying new-school security awareness training. The 365-day results show that by following these best practices, the final Phish-prone percentage can be minimized to 2% on average.

See how your company's phish-prone percentage compares to your peers! The **Industry Benchmarking** feature is included with your subscription.

Did you know that 91% of successful data breaches started with a spear phishing attack?

Get your free phishing security test and f ind out what percentage of your employees are Phish-prone

www.KnowBe4.com/PST

KnowBe4 | The Planet Art, 32 Jamieson St, Cape Town, 8001, South Africa | Tel: +27 21 300 8457 | www.KnowBe4.com | Email: Sales@KnowBe4.com

Today's **Threat Landscape**

Today's cybersecurity threat landscape is everchanging. Long gone are the days where companies operated solely within their own four walls and could be protected by perimeter-based security. As business has moved to the cloud, the concept of a "secure perimeter" has become a thing of the past.

The question is not **"if"** an attacker will get in, but **"when."**

Zero Trust is a security strategy developed by industry analysts at Forrester Research who recognized the shortcomings of perimeter-based security and argue instead that organizations should design their security controls to be data-centric. Understanding what's happening to your data— knowing whether it's sensitive or confidential, over-exposed, or under attack—is a more effective approach for protecting data proactively then relying in perimeter-based security alone.

Organizations should assume hackers will be able to penetrate their network. The question is not "if" an attacker will get in, but "when." All it takes to compromise a network is a subtle misconfiguration or stolen credentials to give bad actors the entry point they need. And, once they're in, it's often not hard for them to gain access to the valuable data they're after, especially on infrastructure that doesn't adhere to a Zero Trust, least privilege model.

To limit the potential damage bad actors can do once inside and proactively detect suspicious activity by insiders or malware, organizations should focus first on defending their data—the asset hackers are ultimately after. Varonis is a pioneer in data security whose capabilities can help organizations implement data security in line with Zero Trust.

Looking forward to our chapters and roadshows in H2 2020

CISO Alliances

CHRO Alliances

CMO Alliances

CDO Alliances

CXO Alliances

DPO Alliances

Women In Tech

Executive Business Exchange