CISO Alliances

Johannesburg Chapter

14th March 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 - 09:00

Reflective Session

Session 1

09:00 - 09:30 - Scenario Overview 09:30 - 10:30 - Open Forum

Cyber Awareness - Let's do this

Yolanda Cornelius - Cyber Awareness Manager - Discovery

Leigh Thomas - Director - Alliances

10:30 - 10:50

Networking Break

Session 2

10:55 - 11:10 - Scenario Overview 11:10 - 11:40 - Open Forum

Framework / Best Practices for Incident Response Orchestration and Automation

Amr Awad - MEA Regional Technical Leader - Resilient - IBM

Session 3

11:40 - 11:55 - Scenario Overview 11:55 - 12:25 - Open Forum

Prioritization - *the fact or condition of being regarded or treated as more important than others.*

Robin Barnwell - Head: Security Strategy Enablement - Standard Bank Group

12:25 - 13:15

Networking Lunch

Session 4

13:15 - 13:30 - Scenario Overview 13:30 - 14:00 - Open Forum

How Security is Changing in a Digital World?

Oscar Stark - Divisional Director - Technology Operational Excellence - Liberty Group

Session 5

14:00 - 14:15 - Scenario Overview 14:15 - 15:00 - Workshop

We know the buzz but, what's does 'The Buzz' mean?

Gerhard Cronje - Head of Cyber Information Security Unit - South African Reserve Bank (SARB)

Closing Remarks & the Next Steps

CISO Alliances

Johannesburg Chapter March 2019

Use Case Partner

IBM

Networking Partner

Qualys.

Networking Partner

VARONIS

Networking Partner

Popcorn Training

a KnowBe4 company

InfosecLive
cyber security news

Mia Andric
Director
Infosec Live

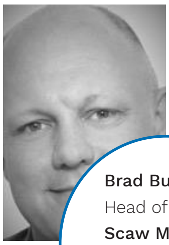
Rishard Baderoon
Country Manager: Africa
Qualys

Nelesh Baichan
Technical Security Lead
Tiger Brands

Nomaphelo Baloyi
Information Security
Mastercard

Robin Barnwell
Head: Security Strategy Enablement
Standard Bank

Sheldon Bennett
Head of Cyber Security
Standard Bank Group

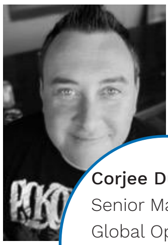


Brad Buttle
Head of IM
Scaw Metals Group

Yolanda Cornelius
Security Governance Officer
Discovery

Gerhard Cronje
Head of Cyber Information Security Unit
South African Reserve Bank

Louis de Kock
South Africa Country Business Development
Varonis Systems

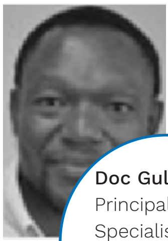


Corjee Du Plessis
Senior Manager: Global Operations, Security & Architecture
Nampak

John Farebrother
Managing Director - EMEA
Qualys

Andrew Ford
Security Consultant
Varonis

Renelle Govender
Information Security Project Manager
Discovery



Doc Gule
Principal ICT Specialist: Security, Telephony & User Support
Mintek

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

Deeren Vallabh
Senior Manager: IT GRC
Barloworld Automotive

Amr Awad
MEA IBM Technical Consultant: Incident Response
IBM

Angela Henry
B_ISO
Rand Merchant Bank

Ian Keller
Head: Technology Security, Information Officer
SBV

Steve Jump
Head: Corporate Information Security Governance
Telkom Group

Thelma Kganakga
CISO
RMB

Loritta Kudumba
Head of IT Governance, Risk and Compliance
Barloworld Equipment

Shalendra Kundalram
CIO & Shared Services Executive
Consumer Goods Council of South Africa

Ntuthuzelo Mgole
Information Security Manager
Dimension Data MEA

Jenny Mohanlall
Chief Information & Security Officer
T-Systems South Africa

Caryn Morgan
Governance, Risk & Compliance Manager
Nampak

Theven Naicker
Head of Information Technology
Scania Southern Africa

Mineshree Narsai
Executive : Information Security Privacy & BCM
BCX

Ronald Mulder
IT Security & Risk Manager
Coca-Cola Beverages Africa

Venisha Nayagar
Director
CryptIT

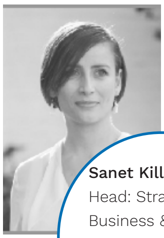
Martin Nortje
Senior Information Security Manager
Eurasian Resources Group Africa

Caston Nyabadza
IT Risk Manager
FNB

Lushen Padayachi
Group Information Security Executive
Massmart

Pragasen Pather
IT Security, Risk and Governance Director
Tiger Brands

Julian Ramiah
Group Chief Information Security Officer
Liberty Holdings Limited



Sanet Killian
Head: Strategic Business & Product Development
Popcorn Training, a KnowBe4 Company

Liza Weschta
Head of Sales & Marketing
Popcorn Training, a KnowBe4 Company

Sithembile Songo
Information Security Officer
Internet Solutions a **Division of Dimension Data**

Oscar Stark
Divisional Director: Technology Centre of Excellence
Liberty Group Limited

Grant Thompson
General Manager Group Security Operations (Cyber Defense)
MTN

Thembi Tshangela
ICT and Risk Management
Tshwane Municipality

Justin Williams
Executive: Group Information Security
MTN

Workshop

Leigh Thomas
Director
Alliances

Yolanda Cornelius
Security Governance Officer
Discovery

Session 1

Presentation

9:00 - 9:30 - Scenario Overview

9:30 - 10:30 - Open Forum

Session Title: Cyber Awareness - Let's do this

Description:

Initial objectives of CAT & did we achieve

- Educate user base
- Regulatory Requirement
- Secure Data & Infrastructure

How do we measure success?

- Measured by how many completed training?
- How many modules you rolled out
- Measured by phishing simulations
- Measured by pass rate?

How do we stack up with real attack?

- SA attacks in 2017-2018
- User behavior hasn't changed

New Cyber Awareness Objective

- What behavior needs to change
- What drives Behavior change
- Identifying channels to facilitate remediation
- Carrot/stick approach outdated why?

Food for Thought

27 Continuous Examples of User Awareness Training

- Gamification
    - Board Games
    - Competition over a sustained period
- Prizes and Rewards
- Collaboration Platforms to deliver the message
- Include user awareness in the user groups (Managers)
- Set KPIs
- Board level support of the user awareness training initiatives
- Integrate into inductions
- Annual attestation
- Ongoing phishing/ online training
- Incident based ongoing messaging
- Sustainability requires a role that is accountable
- Screensavers with awareness
- Weekly communications
- Explicitly identify high risk users
    - Make sure they know they are the HRU
    - Regularly remind them
    - Drive program around them
- Identify a user risk
    - Respected security individuals spoke to the very small target group of leaders in the area. Followed by very targeted training campaigns and supported by communications elements and scheduled (process)
    - Scheduled a reduction in % of the identified risk & supported by continued comms & feedback
    - Key points
        - One risk identified
        - Target audience touched where they were ready and open for the message
        - Support with extra channels
        - Ongoing touchpoints
        - Continuous feedback
- Consistency around campaigns
- Make awareness practical for the day to day life
- Ensure the content is driven by the consumer
- Consequence management and rewards
- Profile based training builds training campaign specific for each user
- Regular snap shots ensure continuity
- Conducting security awareness in a more interactive/ personal and fun way
- Sustain
    - Must be hinged/ linked on a wider change plan
    - Lever/ link to other similar campaigns e.g. POPI, FIC
    - Reward instead of only driving compliance/ punitive
    - Content needs to be fun/ gamified/ innovative/ colourful
- Repetitive phishing simulations on all levels of staff to assess points of compromise in the real environment. Then target specific training campaigns to these individuals. Character models seem to work best to help people relate to a brand
- Make Cyber Security part of the strategy
- Continuous awareness through Popcorn, Screen server & induction
- In the absence of personalised training on a digital platform, face-to-face training remains very effective (though often not practical in very large organisations) so that users can ask questions relevant to their own specific context and have these addressed by the trainer/ facilitator

Outcomes:

How are we measuring effectiveness of the training? Behaviour changed? –
What have we not tried?

- Approach

  Resource, Video, Culture
- External ‘Events’ changing behaviour? (Note SABC to assist in)

  Enough?
  Effectiveness of news of ‘Event’

Community Workshop focus

- Leveraging the Social Media Impact (Does/ Could it work)
- Quantifying Risk
- Differing our Approach
- Content Development
- Consequences of Cyber Awareness (+/-)
- Aligned/ Appropriate Data to Measure Impact

Future topics derived from workshop

- Insurance – what’s the point?
- Training targeted approach
- Incentives
- Utilising new S.A platforms
- Working on good examples. Who can improve and wants to?

Workshop community input around:

1. Social Media Impact - Does work (Could work) –
Use social media to message e.g. fake/real news
Bleed into customers/ external
Avoid Failed projects, social media (internal)
Not even HR gets it done – multi-divisional approach
Approves campaign – or more organic
Avoid old intranet
History click rate – measure
Don't treat all users the same, swift admin, sit down, intel. customised response > intel-based awareness red teaming / big brother > recon scam on CEO / risk splash page
Ownership and Accountability of SM approaches
Was with social media trolls etc.
Abuse like video feedback. Real hack (red teaming)
Corporate rooms can't compete with social media > Popcorn is spray and pay
Social media – intranet – intel based (website / external) awareness (awareness red teaming) (personal targeting)
Target users
Abuse platforms? – int – etc.
Targeted – CEO – system admin, typically don't care (not training) > repeat offenders > web behaviour - target based on AD
Scare the users (behavioural)
Profile users
Do high risk, know they are high risk?
Used repetitive behaviour > intense auditing e.g.

2. Quantifying risk
Challenge to overcome, and quickly - Articulating the risk to return on investment to C-Level executives

- Practical demonstration – hack – motivation for budget
- Security is a grudge purchase – paying insurance**** CISO Alliances note for future topic
- C-Level executive speak a different language to security heads
- Change our language
- Influence and credibility
- Good governance structure
- Security topical on the agenda
- Don't waste a good crisis, if hacked
- Cyber insurance, in the event of a security incident – is there a company that actually pays out?
- Measuring of security posture
- Accountability and positioning of security in the organisation
- Making Security a board-level agenda item

3. Different approaches

- Online training
  - Name and Shame or Name and Encourage?
- Top > down – they must own it
  - Not an option? > compliance
- Warning as a consequence
- Gamification
- Communication – create and type
- Personal implication > targeted approach, divisional. With budget constraints, can we leverage leaders in the workforce to drive and create a ripple/ domino effect into the masses?

4. Content

- Tailored to audience (easily understandable) – Are we overcomplicating due to our understanding of Cyber Risk Landscape and its potential/ real impact?
- Relevant to environment > topical threats > industry > geography
- Relate to content to the "individual"
- Realisation to the impact of an individual > consequence > also to organisation
  - tools to make practical for individuals (non tech)
- Content linked to gamification
- Content needs to be dynamic and reviewed, therefore owned
- Report a breach (content to indicate "how to"). Encourage the opportunity to learn from a mistake and the learning can be widespread.

5. Consequences

- Societal problem – no consequences
- General population don't care about impact at corporate level
- Buttons
  - personal (segment of 1)
  - emotional connection
  - context (my buddy sharing)
- Build internal consequence

6. Appropriate (aligned data) (intelligence)

- Point in time training: password change!
- ID. Targeted > awareness
  - Split > training
- What's in it for me?
  - brand 4@me? Make it personal
    - Work / Parents/ Home/ Kids
- Regular snapshots > review
- Point system: risk profile
- Measurement
- KISS

Feedback

- Yolanda Cornelius gave a good presentation and she touched on some important points which I will talk about below:

- Threat Landscape:
- Monitoring is key in ensuring the management of a cyber-threat. As Ms Cornelius pointed, it is key to measure the current cyber awareness maturity.

- User Behaviour:
- We should make use of our user community as the human security layer by introducing, amongst other things, a behavioural change as well as habit change.

- Clear and precise. A very good re-look at an area that everyone should know, but often passes by. I especially like idea of working out what heathy behaviour looks like before trying to encourage it. Relevant and thought provoking. New ideas shared around a common problem.

- Well Presented, good content in presentation, and openness on what was shared on wins and failures around security awareness

- I believe the transparency that was shared from Yolanda set the stage for the audience to interact,

- Yola landed her "problem statement" well. Relevant and Yola spoke to the masses

- It raised some interesting thought on the sustainability of cyber awareness within organisations.

- A good choice of topic and it is well Thomas: presented. I like the fact that this was an interactive session because it allows everyone to put their ideas forward. Introverts and Extroverts ;-) The content was good (I especially loved the video chosen - The coffee Shop scenario) .... I do think that if we make our content more aligned to South Africa, we could get a richer experience.

- Yolanda - good presenter, slightly nervous but picked up well in her session. Leigh - behaved well

- Good content in presentation. Example of real problems that professionals deal with.

- Pity that the lady from the blog sitting in the session did not have some comments in this regard

Open Forum

Session 2

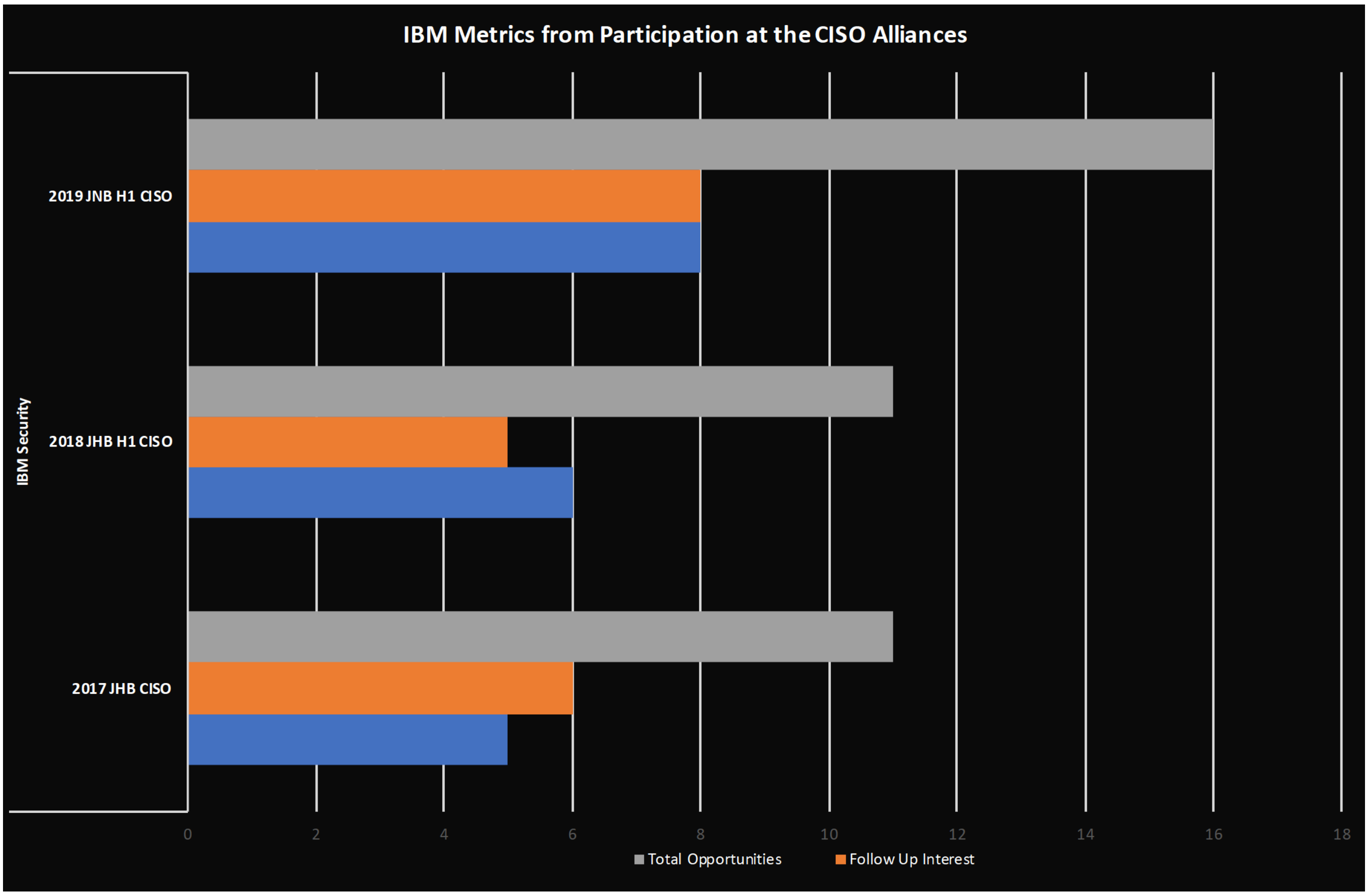
Amr Awad
MEA IBM Technical Consultant: Incident Response
IBM

Presentation

10:55 - 11:10 - Scenario Overview

11:10 - 11:40 - Open Forum

Session Title: Framework / Best Practices for Incident Response Orchestration and Automation



Alliance - *'A union formed for mutual benefit'*

Food for Thought

1. **What consumes most of your security operations resources?**
    a. New IT Implementations driven by the business keeping changing the security posture. Not being able to mature the current security posture, means that security is always playing catch-up.
    b. Most of the time is spent MANAGING Security tooling versus DOING Security. Too much time is spent installing, configuring, patching and maintaining security toolsets rather than focusing on patterns, trends, analysis and preparing to respond effectively to security incidents.
    c. Having to work with and maintain old obsolete technology.
    d. Constantly having to re-act to unplanned external factors such as regulatory and legislative changes
    e. Responding to consumers of the business services who have been hacked. Thus doing investigations and providing support etc.
    f. Investigating UNKNOWN attacks. It takes days to understand and formulate a response.

2. **After a Cyber Incident, how can you apply lessons learnt:**
    a. Perform a GAP Analysis – review the current internal processes , and if there is a performance gap, how can those process be enhanced / matured to be more effective next time.
    b. Questions to be asked in the GAP Analysis:
        i. What did we do well?
        ii. Where can we improve?
        iii. What is the corrective action?
        iv. What resources (people, process, technology) do we need to ensure that this does not occur again.
    c. Put a RASCI Matrix together- used to assign and display responsibilities of individuals or jobs (people) in a task (project, service or process) in the organization.
    d. Institute an assurance (governance) process in place to ensure the newly implemented controls (after the cyber incident) are being effective.
    e. Do we have a plan to secure other possible resources to assist with the remediation. Maybe a retainer contract with 3rd party suppliers specializing in Cyber Incident Response

3. **What are the Business Benefits of Effective Incident Response?**
    a. Being able to sustain business operations
    b. Being able to protect the business reputation with it's constituents (staff, shareholders, regulators, customers, board, executives, etc.)
    c. To eliminate, or at the very least minimize the financial impact to the organization
    d. Having a planned, effective, well-rehearsed Incident Response capability leverages all the available resources to mitigate or reduce the impact of a cyber incident.
    e. Applying lessons learnt always provides an opportunity to refine and improve the security posture

4. **For HIGH Business Impacting, LOW Volume Cyber Incidents, how can you orchestrate the Cyber Response more effectively?**

a. Have an Incident Response Plan. Understand the plan. Mature the plan.
b. Ensure Effective Communication
c. Understand who the incident is impacting, communicate effectively to that audience. Is it affecting just the organization or potentially customers ?
d. Understand who all the role players are in needed in the response. Pre-define CERT team members from both IT and the business
e. Implement AI Technology:

i. Use Security Technology Platforms to Orchestrate , Automate, Remediate such as SOAR (Security Orchestration Automation Response)
ii. Humans take too long to remediate alone, you need to augment with technology

f. Perform Cyber Threat Specific Simulations (not just BCP/DR tests)

5. **For LOW Business Impacting, High Volume Cyber Incidents, how can you orchestrate the Cyber Response more effectively?**

a. Categorize the incidents – Low / Medium / High Impact
b. Define a incident response baseline (Review and Build on)
c. Review the current incident response process – Determine how to deal with exceptions
d. Identify Security Incidents for Automation – quick wins, low hanging fruit, low risk, high volume
e. Integrate Monitoring capabilities

6. **What other use cases could be addressed using a SOAR platform (Security Orchestration Automation Response) ?**

a. Monitoring and Escalation
b. Identification and Enrichment
c. Containment, Response and Recovery
d. Communication and Co-ordination

Feedback

- Mr Amr Awad's presentation was highly informative.

- Good and clear presentation. Explained the points that need focus.

- Nice one Amr - you kept the presentation technology agnostic until the end. this is a very good way to convey the actual concept that links back to business value.

- Responding to a security incident: - This is one of the critical points that I learnt from Mr Awad's presentation that an organisation may suffer a cyber-attack however; its security plan would be judged based on how quick it responds to an incident.

- I was impressed by the Gartner Security Operations & Response Model.

- Very Familiar, and very appropriate. Not oversold.

- We already use several of the major IBM components in our current architecture

- Nice to see a presentation from vendor - that is just not another product push

- The interactive-ness helped the audience to better relate

- The content was well prepared.

- Content was excellent and very relevant to most people in the audience.

- The workshop session should have been planned much better (not that it was bad); but it is encouraging to see that IBM has recognized that this is an ideal way to generate insights from the consumer to help improve on technology and services on offer.

- Very informative practical and useful esp. at this day and age where CISOs or organisations are measured by how quick they respond to incidents.

- Glad to see them exploring concepts and sharing some thought leadership

Open Forum

Robin Barnwell
Head: Security
Strategy Enablement
Standard Bank

Session 3

Presentation

11:40 - 11:55 - Scenario Overview

11:55 - 12:25 - Open Forum

Session Title: Prioritization - the fact or condition of being regarded or treated as more important than others.

- Is infosec identifying the business objectives?
- Is infosec justifying ROI in the wrong areas?
- How is infosec prioritising the risks that the business faces? Where is the line?

Food for Thought

Quantifying reputation risk
Measure threat impact
Internal vs external breach
Quantum of risk

- Paradigm shift in board sell
- Is there an impact regardless?

Don’t get breached
Secure your ‘cheese’

Liberty – 10% dip in share price
2 days to recovery

Brand reputation science
What is the science behind the impact on ‘reputation’?

Prioritization conversations - get to the point
-how do we avoid damage to the brand
What is the value proposition to your board?

Feedback

- Mr Robin Barnwell's presentation was impressive. It exceeded my expectations.

- Very thought provoking - a subtly different, and very appropriate view on the complexities of getting it right.

- Robin did an absolute fabulous job in landing his intended message and I think that this is the sort of thought leadership that is required within SA.

- Very good. A very effective and intelligent way of driving a security strategy that enables business by managing business risks and demonstrating ROI. Business hardly derives value from a compliance driven strategy because it is always perceived as a tick-box exercise

- Mr Barnwell of Standard Bank highlighted the fact that there have created their own security framework which looks at the Risk => Impact => financial loss.

- I was particularly impressed by the intelligence-led Cyber Strategy of Standard Bank:

- The Impact looks at the affected business areas; - Readiness to respond is key in dealing with a cyber incident;

- Gaining visibility in the assets that are being protected;

- Protecting the common points that would otherwise harm the business;
- Looking at the selective use of controls; and
- Continuous testing and monitoring of the controls.

- A primer for anyone looking at Cyber strategy. Unpacking the concept behind "What does a bad for your business really look like" offers a perspective that made the entire day worthwhile

- Good Content, as per Yolanda session, makes a big difference when organisations are willing to share on what works and best practices and also fails

- Must share more openly without compromise. More practical details missing

- A very interesting view on how to prioritise security initiatives within an organisation.

- Excellent content. Well done to Robin and team from SBSA

- Good content and highlights the importance of how security needs to understand what drives business.

- Enjoyed the session. Although you didn't speak to Cyber Awareness - i did take away some of the concepts you raised and plan to use in Cyber Awareness to Exco.

Thank you

Open Forum

Oscar Stark
Divisional Director: Technology Centre of Excellence
Liberty Group Limited

Session 4

Presentation

13:15 - 13:30 - Scenario Overview

13:30 - 14:00 - Open Forum

Session Title: How Security is Changing in a Digital World?

Synopsis

Business models are rapidly evolving from what was the status quo for many years, to ones which are operating with higher levels of interconnectedness. This is resulting in changing trust models and leveraging of capabilities which execute in large collaborative environments. How does this backdrop influence the security practitioners life?

Takeaways

What are the prevailing business models?

Some of the realities at play shaping the world

Changes in security thinking to remain relevant

Food for Thought

1 value chain – controls (less breaks in the monitoring)

3rd party (partner & supplies)

- Consolidate (when international)
- Contract with security processes
- ISO27001 – compliance
- Having the right to audit
- Threat exposure

- Enforcing when others impact
- 3rd party role in process
- Legally compliant (across the board/business divisions)

People and process of security in digital transformation

Educate why – build trust

(biometrics example)

Business to trust security

Security look outbound

Fail friendly as target as opposed to self -healing.....>busy protecting your money

Consistent experience on elastic infrastructure

Trust in distributed development

(across partners /sites) – consistency

KPI – improve trust on digital platform

-comms and underlying actions

Security more visible to business

Feedback

- Mr Oscar Stark gave an impressive and practical presentation for CISOs.

- As always Mr Stark's thinking is at a different level. He is a real thought leader and always sees the bigger picture. Mr Stark just needs to get some easier to understand examples and/or analogies to help convey his message :-)

- Great style and very stimulating discussion. "Its all about Trust", and "Fail Friendly" enjoyed the content, and the challenge to think broader

- Mr Stark's presentation was useful to me as we are currently going through the review of the organisation strategy and he gave me some excellent pointers as to how I should align the ICT Security Strategy with the business strategy regarding whichever business model the organisation is taking as per the following:
  - Omni Channel
  - Supplier
  - Ecosystem Driver – Modular Producer

- The other key point that Mr Stark raised was the impact on trust as regards to:
  - Trust => centralised or distributed;
  - Decision making => hierarchical (self directing);
  - Think Process => non-integrated (systematic);
  - Capacity => defined (demand).

- An engaging speaker. Some good thoughts put forward.

Workshop

Gerhard Cronje
Head of Cyber Information Security Unit
South African Reserve Bank

Session 5

14:00 - 14:15 - Scenario Overview

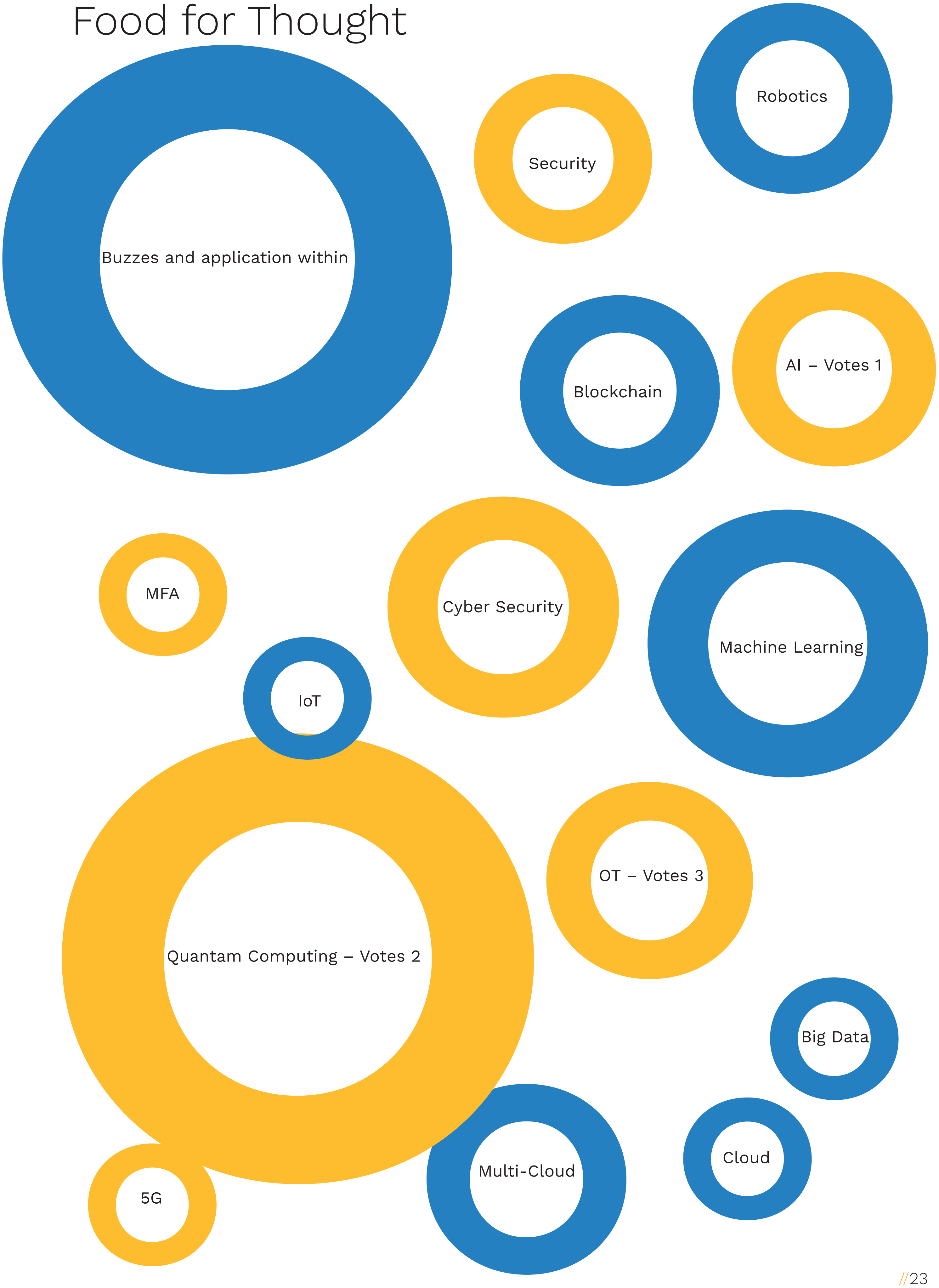
14:15 - 15:00 - Workshop

Session Title: We know the buzz but, what's does 'The Buzz' mean?

- Security Automation
- AI
- Behavioural Analysis
- Blockchain

Practically what does that mean for us in our role?

Food for Thought



Buzzes and application within

Security

Robotics

Blockchain

AI – Votes 1

MFA

Cyber Security

Machine Learning

IoT

Quantam Computing – Votes 2

OT – Votes 3

Big Data

Multi-Cloud

Cloud

5G

AI

Many local examples of ‘AI’ implementations or mathematical algorithms but, how do we vouch it is still functioning? Should AI be auditing another AI function? Will there be a ‘bias’ on standards of the audit?

Security Models on AI?

AI in our Job?

  - Learning like a human

How to interface – natural language interface for all. The language is a security understanding including cross learning.

5G – The value proposition is a distributed environment – timeline is 24 months for Africa

- Connectivity globally and anywhere
- Security has a consideration but not core, so how will we secure 5G? Blockchain?
- Identified and authorised everything. Could this be a privacy issue?
  - Self-protecting environment
  - Industry defined policy GSM.A
- Who is accountable? Similar to data in the cloud.

Quantum

- Unrestricted processing ability
- Will it change how to run crypto currencies?
- Good practice: design with an exit strategy (Rip & Replace)
- What about the technology barrier between backups?
- It is like that the Crypto Paradigm will change

OT

- Industry Control Systems (ICS) – commodity hardware with applications running on top (proprietory)
  - Engineering and cybersecurity don’t understand each other
- OT & IoT are starting to merge: opening up data interchange
  - Where they traditionally don’t care about security
- Digitising OT systems/ factories – challenge to connect to enterprise systems (proprietory protocols, etc.)
- (1) Skills & (2) technology to bridge the gap
  1. Scarce
  2. Expensive
- Find ways to discover and react to events in plants/ factories/ OT Systems

Feedback

- Mr Gerhard Cronje's presentation was impressive! It highlighted the fact that we need to be familiar with the new terms and trends.

- The future is coming fast, and it has new Buzzwords on a daily basis. Brilliant topic. Well handled.

- Most people failed to understand the question

- These sorts of sessions are an absolute must with regard to how we need to think as professionals. As the CISO alliance (SA Chapter) we can start generating some good content from topics like these.

- The content was very much relevant, and I liked examples that were provided to add some colour to the content.

- The urgent future technologies that will disrupt the industry that we need to understand its impact on cybersecurity are 5G technology and Quantum Computing in terms of encryption. I will be doing more research as regard to these two critical future disruptors.

- The examples from the audience helped

- The meaning of these "buzz" words seem to have a different interpretation within different organisations. An interesting topic would be how 5G connectivity would change the business landscape from a connectivity and bandwidth perspective, and how security practitioners would need to deal with this.

- Good topic, but it would have been better to have something down to provide a view before we went into deeper conversations. As an Enterprise Architect (myself) I constantly have to work with buzz words and align it back to the thinking of the organization. I generally conduct light research to help expedite the thinking.

- I liked Gerhard's different approach. It was very engaging, interactive and very suitable for the afternoon session.

- Brave approach, but the session worked out well with some good discussion

- Very Educational Session. Thoroughly enjoyed and learned alot. I hope this is a permanent feature

CISO Alliance Testimonials

- It was my first CISO event and it was informative and great for networking. – **Doc Gule –** Principal ICT Specialist: Security, Telephony & User Support **– Mintek**

- Effortless brilliance ;) – **Steve Jump –** Head: Corporate Information Security Governance – **Telkom Group**

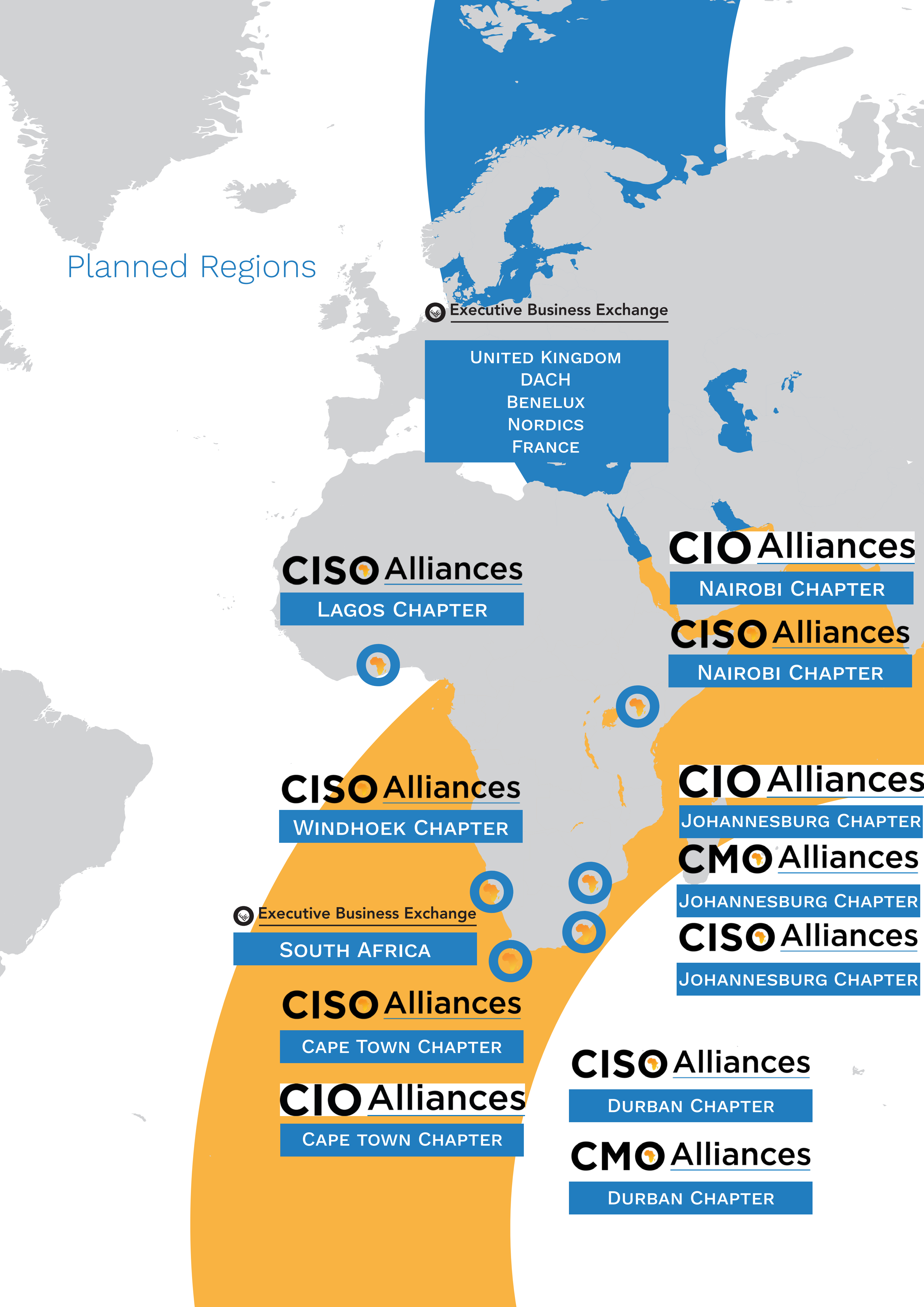
- Platform must be a trusted 1 to allow for open sharing – **Julian Ramiah –** Group Chief Information Security Officer **– Liberty Holdings Limited**

- I am a firm believer that everyone has value to add, and as such, the workshop way of running the sessions, is an absolute must going forward. Again, well done on a very successful session. - **Jashwin Dayaram** – Enterprise Architecture – **Liberty Holdings Limited**

- I appreciate Leigh's awesome initiative in helping us to collaborate and sharing useful insights that will help us to improve the overall cybersecurity posture in our community. **- Sithembile Songo** – Information Security Officer Internet Solutions – **Division of Dimension Data**

- The CISO Alliance has become the foundational engagement platform for security professionals who are dealing with the real-world problems. It is truly a meeting place of great security minds. - **Oscar Stark –** Divisional Director: Technology Centre of Excellence –**Liberty Group Limited**

Planned Regions



Executive Business Exchange

United Kingdom
DACH
Benelux
Nordics
France

CISO Alliances

Lagos Chapter

CIO Alliances

Nairobi Chapter

CISO Alliances

Nairobi Chapter

CISO Alliances

Windhoek Chapter

Executive Business Exchange

South Africa

CISO Alliances

Cape Town Chapter

CIO Alliances

Cape town Chapter

CIO Alliances

Johannesburg Chapter

CMO Alliances

Johannesburg Chapter

CISO Alliances

Johannesburg Chapter

CISO Alliances

Durban Chapter

CMO Alliances

Durban Chapter

CISO Alliances

SYDNEY CHAPTER

CIO Alliances

SYDNEY CHAPTER

CISO Alliances

MELBOURNE CHAPTER

CIO Alliances

MELBOURNE CHAPTER

Focus on the topics you care about most

Smarter Business Showcase

Put smart to work for your enterprise with guidance from top experts and industry-leading **service** solutions.

Data & AI Campus

Unlock the value of your data and put smart to work with AI.

Cloud & Infrastructure Campus

Optimize your **infrastructure** with faster, smarter **platforms** and services.

Security & Resiliency Campus

Build **trust and resiliency** with the biggest advances in cybersecurity at work.

think Summit

IBM

12 June 2019
Kyalami Grand Prix Circuit | International Convention Centre

Think Summit Johannesburg is the most celebrated gathering of visionaries, technologists and innovators. Where the curious convene and foremost business leaders connect to inspire and learn.

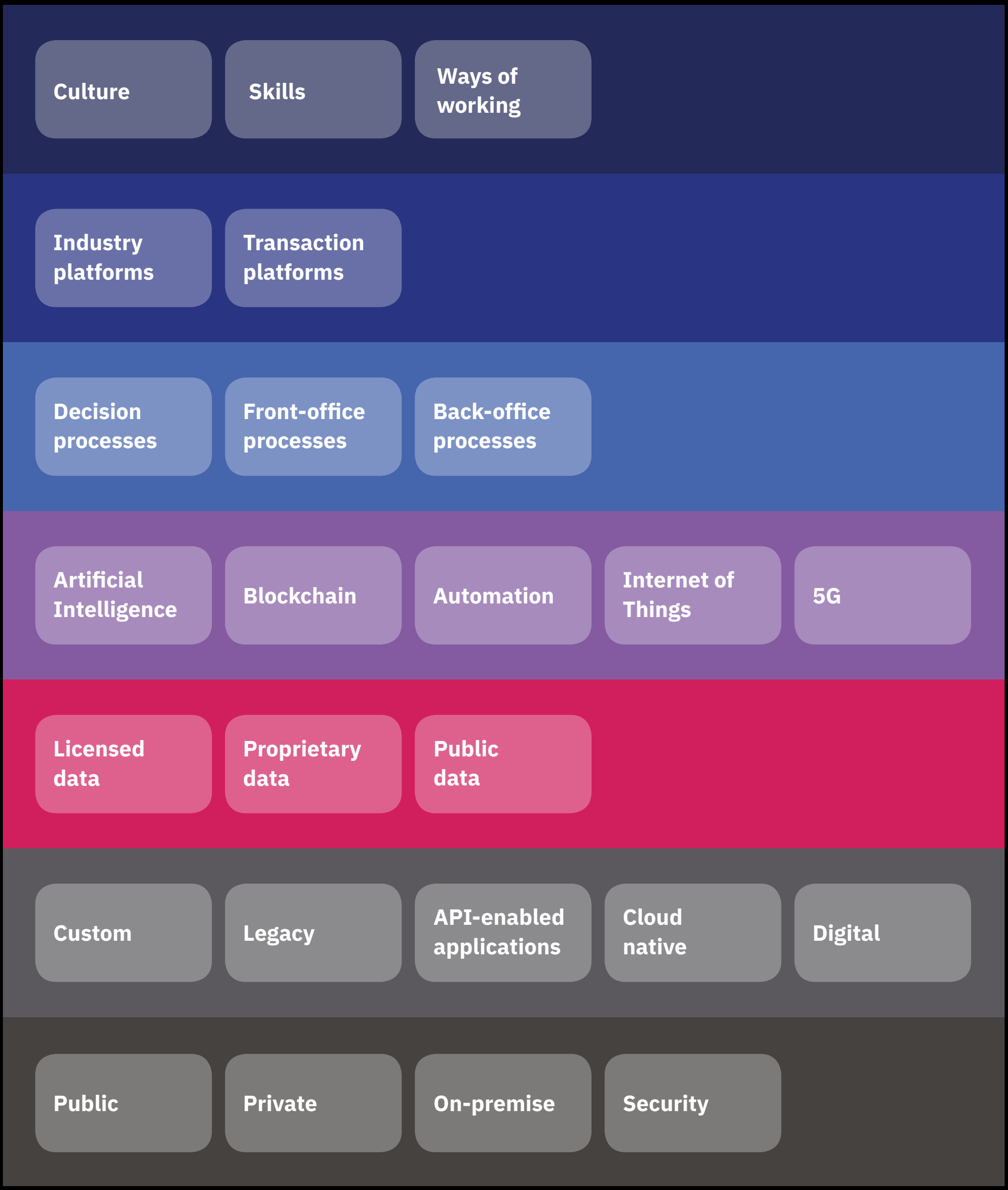
Join us to create in the Cloud, innovate with IoT, break down barriers with Blockchain, and solve the unsolvable with Quantum. Learn how to get more value from AI and your Data - train it, trust it and make your business more efficient and Secure. See how the newest technology paired with our industry expertise can reinvent your business and industry, your school and store, your farm and pharmacology, your bank and energy grid, regulations and workflows.

At Think Summit Johannesburg you will find the way forward through deep interactions with brilliant minds and industry experts. Change the way the world works by putting smart to work.

We invite you to come together and think on
12 June at Kyalami Grand Prix Circuit |
International Convention Centre.
http://www-05.ibm.com/za/think-johannesburg/

Join us to learn how IBM is re-inventing, not only i
smarter business and change the way we work.

1 Questions: How do you transform across multiple business
and common capability layers, to enable a smarter business?



Culture	Skills	Ways of working			Culture of agile inn
Industry platforms	Transaction platforms				...powered by an e business platform
Decision processes	Front-office processes	Back-office processes			...activated by cog enterprise workflo
Artificial Intelligence	Blockchain	Automation	Internet of Things	5G	...made possible w technologies
Licensed data	Proprietary data	Public data			...that are fuelled b
Custom	Legacy	API-enabled applications	Cloud native	Digital	...using next-gener
Public	Private	On-premise	Security		...on a secure hybr infrastructure

1 Day **1200 Attendees** **5 Th**

tself, but its clients to build

platforms

2 Focus areas

novation

cosystem of
s

nitive-enabled
ws

ith exponential

oy data

ration applications

id multi-cloud

Transform the customer experience through "outside-in" digital reinvention

Make the most of your data and unleash the full potential of AI-enabled workflows

Co-create your business platforms with our industry and technology know-how

neatres **28 Sessions** **26 Demos**

KnowBe4
Human error. Conquered.

WHITEPAPER
How to Transform Employee Worst Practices Into Enterprise Best Practices

WHITEPAPER: How to Transform Employee Worst Practices Into Enterprise Best Practic

Preventing your worst data breach nightmare with New School Security Awareness Training

Executive Summary

The press can't get enough of corporate data breaches. They delight in showcasing the latest horror story about a business that lost massive amounts of private records or millions in revenue to the latest hack. You could be next.

Despite all the funds you may have spent on state-of-the-art security software, the bad guys are just one gullible user click away from staging an all-out invasion. To make matters worse, that user might well be you! Recent surveys show that executives can be some of the biggest culprits when it comes to clicking on phishing links and opening malicious email attachments.

Yet by far the most effective strategy in combatting these attacks is also one of the most poorly implemented – security awareness training. The long list of "worst practices" for user education is almost endless – break room briefings while people eat lunch and catch up on email; short instructional videos that provide no more than superficial understanding; and the time-honored practice of hoping for the best and doing nothing.

Find out what the true best practices are for security awareness training – those that establish a human firewall to effectively block hackers and criminals, and keep you out of the headlines.

This whitepaper provides clear direction on how to go about improving your organization's security posture by "inoculating" employees who fall for social engineering attacks. Such incidents are far from uncommon. According to a recent study by Osterman Research, email is the most prevalent channel of infiltration into the enterprise.

> **"The adage is true that the security systems have to win every time, the attacker only has to win once."**
>
> —Dustin Dykes, CISSP
> Founder Wirefall Consulting

Key Points

- A summary of the main email-based attack vectors into organizations such as phishing, spear-phishing, executive "whaling", and "CEO fraud".
- What organizations are doing about it and why this isn't enough.
- What is wrong with most current security awareness training programs. This includes a list of "worst practices" along with why they don't work.
- The proven best practices for security awareness training that reinforce existing defenses by erecting a human firewall.
- How to combine security awareness training with simulated phishing attacks to keep employees on their toes with security top of mind.
- How to devise a valid KPI for the effectiveness of that training to showcase its return on investment.

Understanding the Threat

According to a recent study by Osterman Research, email is the top attack vector into organizations. Web-based attacks used to predominate which is why their prevention appears to receive more funding. Yet email attacks were never far away from first place and are now once again in the lead. Osterman places email in the lead with malware infections impacting 67% of organizations, with web-based attacks in second place at 63%.

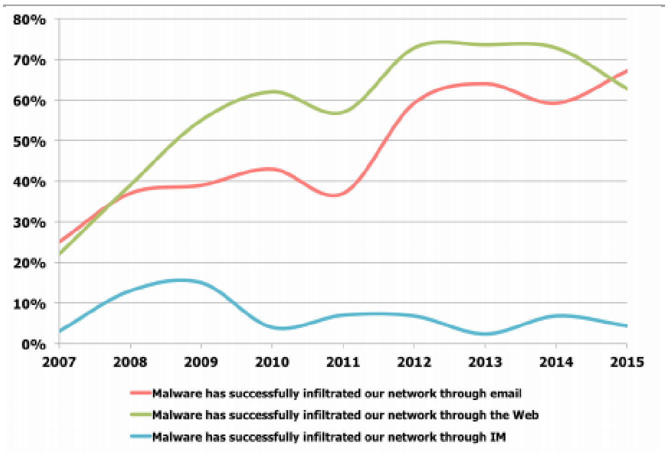
In third place is a category of attack of uncertain origin. Those attacks may well have come via email but the source has never been detected. 23% of organizations marked this category over the past year, and the true number is probably much higher.

Why can't these companies identify some of the avenues of security compromise? Cybercriminals are becoming more effective. Verizon numbers indicate that 80,000 security incidents were reported by 70 organizations contributing to the survey and over 2,000 breaches occurred in one year.

Here is a summary of the primary email-based attack vectors into organizations:

Phishing: You've all seen examples of phishing emails. They are sent to large numbers of users simultaneously and attempt to "fish" sensitive information from unsuspecting users by posing as reputable sources. This includes banks, credit card providers, delivery firms and law enforcement. Their ploy is to trick the user into either clicking on a link to infect the PC, open an infected attachment or go to a fake website to enter login credentials, financial information, social security data or credit card details. But any data entered is likely to be used maliciously to steal money or an identity, or infiltrate a network. According to the Verizon 2015 Data Breach Investigations Report, 23% of recipients open phishing messages. Another 11% click on attachments. Unfortunately, nearly half open these emails and click on links within an hour of receiving them. Some respond within a minute of receipt. In other words, security teams have a tiny window in which to note the presence of such an attack and take adequate precautions to cleanse it. Clearly, a purely defensive posture is doomed to failure.

Malware Infiltrations for the Period 2007 to 2015



Source: Osterman Research, Inc.

Spear-phishing: This malicious strategy takes phishing to a different level. Phishing is spray and pray in that it involves the transmission of one email to a large list, many of whom don't even use that bank, credit card or service. Spear-phishing, on the other hand, is targeted at specific individuals or a small group. The cybercriminal has either studied up on the company or group, or has gleaned data from social media sites in order to gain enough data to con users. The originators craft their messages to make them more believable and increase the likelihood of success. It isn't difficult for the bad guys to find out basic data about employees from the web, Facebook, Twitter, LinkedIn and other similar venues. This can include travel plans, family details, employment history, various affiliations and more. Thus the open rate for spear-phishing is far higher than that of phishing.

Executive Whaling: This practice is becoming increasingly common. The term comes from the Vegas gambling moniker "whale" which means a high roller who is going to lay down some serious money in the casino. After all, the higher up the command chain you go, the more likely you are to find valuable information from your phishing efforts. So cybercriminals are increasingly targeting executive whales. To make matters worse, C-level executives have been found to be some of the biggest culprits when it comes to opening suspicious emails. Perhaps due to their hefty volume of traffic, they don't have the time to look closely before they click. Whatever the reason, whaling is causing some serious breaches inside major corporations.

CEO Fraud: Known variously as the "CEO fraud," or the "business email compromise," highly sophisticated cyber criminals try to social engineer businesses that work with foreign suppliers. This swindle is increasingly common and targets businesses that regularly perform (foreign) wire transfer payments. In January 2015, the FBI warned that cyber thieves stole nearly $215 million from businesses in the previous 14 months through such scams, which start when crooks spoof or hijack the email accounts of business executives or employees. The CEO's email gets spoofed while the CEO is travelling and employees are tasked to transfer large amounts of money out of the country.

> "Passive security practices like setting and maintaining defensive security perimeters simply don't work against highly aggressive and adaptable threat sources, including criminal organizations and rogue states."
>
> —Charles King, Analyst
> Pund-It

Old School Defenses Are Inadequate

Organizations can't be accused of ignoring the problem. Their budgets reflect that these threats are considered high risk. Money is being spent to upgrade or add new antivirus (AV) software, anti-malware systems, IDS, firewalls, spam filters, security analytics and more. While all of these actions are definitely necessary, they aren't bringing about any marked improvement.

Osterman Research revealed that about half of all organizations feel they made no progress in the past year in combatting phishing efforts and 21% felt they were actually backsliding. This is easy to understand when you consider that the sophistication of malware is growing and the bad guys are far more organized than ever.

Take the case of sandboxing – the practice of placing a potential threat into a system that is isolated from the main network so it can be examined and neutralized. Some malware has appeared that can detect when it has been placed in a sandbox and will remain dormant during that time so as not to alert security personnel of its harmful nature. Other pieces of malware quietly infiltrate a network and are seemingly innocuous. But they are designed to only operate in tandem with other elements. Only when all are present will actual harm result. This strain can be very hard to detect until it is too late.

Verizon notes that phishing is increasingly employed to gain access and then quietly set up camp inside the corporate network. Thus phishing does not always lead to an immediate data breach. Increasingly sophisticated attacks may take their time learning passwords, security defenses and account numbers then stage a sudden attack which transfers millions before being spotted. Alternatively, some hackers have quietly siphoned off small amounts from multiple accounts over many years. Tens of millions disappeared before being detected.

The biggest indictment of traditional security defenses, though, concerns (antivirus) AV software. Still considered the primary defense against malicious programs, the sheer volume of threats is making it impossible for AV to keep up. At the time of this writing, about two million malicious programs are detected every week, according to Virus Total, which provides total malware submissions weekly. It is important to note, though, that AV does not spot all threats. Estimates of AV effectiveness vary from 60 to 98 percent. So at the very least, a few percent of attacks will be missed by AV.

Further, as most AV tools mainly use signature files to detect viruses, new threats are only added to these lists once they are detected. They may have gotten much faster at finding new strains and adding them to their virus signatures – an average of six hours in some cases. But that still leaves a large enough invasion window for the cybercriminals to exploit and cause damage. Time to compromise among Verizon customers was often less than a day once a breach occurred, whereas time to discover the breach was much slower.

Charles King, an analyst at Pund-IT puts it plainly. "It is abundantly clear that traditional security solutions are increasingly ineffectual and that vendors' assurances are often empty promises," says King.

Professional teams of Eastern European cyber mafias exist, for example, that actively hire the best talent in order to innovate new malware strains at a furious pace. This gives them the capability of quickly posting a malicious website, staging an attack on a corporate network and disappearing within a few hours, well before AV companies have had time to update their malware definitions, if the malicious code is spotted at all.

NYSE Governance Services asked top executives just how confident they were that their companies were properly secured against cyberattacks. Only 33% expressed confidence. The same survey found that 81% of executives discussed cybersecurity in most if not all meetings.

This doesn't mean that traditional defenses like AV should be discarded. They all play their part and make it harder for the bad guys to succeed. But they are no longer enough.

What it takes is using any and all of the aforementioned security technologies and strategies as part of a robust and layered defense in depth. But they must be augmented by what Osterman Research considers the "first line of defense in any security infrastructure" – the users themselves. Aberdeen Group called user behavior the "critical last mile" of reducing risks on the prevention side of the security risk equation. In spite of all the technical controls designed to prevent an occurrence, incidents still occur. The root cause for most of these incidents is the action of users. Aberdeen Group concluded that investment in effective security awareness training reduces risk from the financial impact of phishing by 60%.

To some, the concept of a human firewall may appear naive. After all, survey after survey reveals just how gullible users can be. Out of 100 engineering and science majors, for example, one in six fell victim to obvious phishing scams. Another survey showed that 96% of executives failed to tell the difference between a real email and a phishing email.

This is why top executives have become prime targets for whaling attacks. According to research from the SANS Institute, 95% of all attacks on the enterprise network are the result of successful spear-phishing. These attacks no longer only target large companies. They can have dangerous ramifications to any business, regardless of size.

Clearly, modern executives and employees are a ticking time bomb of gullibility ready to explode any organization into the headlines when they fall victim to a clever or even a not-so-clever attack. Steps must be taken to plug this gaping hole. Done correctly, however, these same employees can be molded into an effective human firewall via new school security awareness training. Unfortunately, training efforts of the past have only been marginally effective. Let's take a look at why this is by examining what passes for security training in the ever-evolving world of cyberthreats.

Your Worst Practice Guide to Security Training

It's easy to dismiss security awareness training as unworkable. After all, its results are poor in most organizations. Osterman surveys show that less than a quarter of executives consider it effective. With an IT department continually having to put out fires due to the latest employee or senior executive being tricked into handing over sensitive information, it is understandable that they have little faith in attempts to educate users on phishing and its various schemes.

But the problem is not with the concept of user training itself but rather with the way it is being executed. Here are some of the ways it is traditionally carried out.

Worst Practice #1: Do Nothing and Hope for the Best

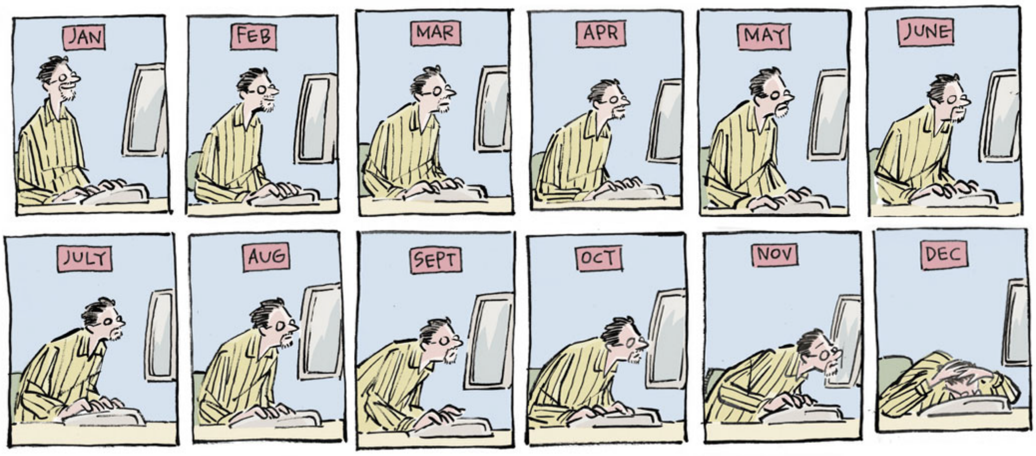
Only about one in five organizations admit to this as their "strategy" against the rise of phishing. But the actual number is probably much higher. The logic goes, "We haven't had a company-threatening data breach to date, and we can live with these minor outbreaks which keep IT busy. So let's hope 'the big one' doesn't happen to us." Aberdeen Group put a hefty price tag on reliance on this strategy. The analyst firm said that there is an 80% likelihood that infections from users will result in total costs of more than $2.5 million per year.

Worst Practice #2: Break Room Training

About 30% of organizations favor the break room approach. They gather as many employees as they can in the break room, provide lunch and have someone from IT or a security expert lecture on topics such as phishing, spear-phishing and whaling. This is certainly better than nothing, but often attendance is low and most of the audience looks upon the event as a time to make some headway on their email backlog. And the results speak for themselves. Measures of the effectiveness of phishing show little change after such briefings.

Worst Practice #3: Monthly Security Videos

This can be done informally with videos made available via email or placed on the website for employees to view, or formally via mandatory classes. These short clips educate users on the perils of promiscuous clicking and on the many snares used by phishers to reel in unsuspecting employees. About one in four organizations gravitate towards this method. At best, this can be categorized as being little more than a superficial training program. On its own, it can't be expected to do much to diminish the risk of data breach. It also causes training fragmentation because important topics are covered months too late.



Worst Practice #4: Phishing Tests

This approach pre-selects high-risk employees only and sends them simulated phishing emails to see how many fall victim to the attack. This is typically paired with some kind of educational module such as links to training modules for offenders as well as short videos to view to increase awareness. The plus on this method is that it offers some kind of metric about phishing. The minus is that employees soon get wise to it and "prairie dogging" begins to happen – an employee sees a phishing test email and pops his or her head up above the cubicle to let the others know to watch out for it. This approach, then, is both limited and too simplistic.

These Worst Practices are the reason why some IT managers struggle to obtain budget approval for more effective security training measures as they struggle to win the fight against phishing. Unaware of the shallowness of their ongoing efforts to proof up staff against attack, executives redline training expenses as "we are already doing that" and buy into vendor hype by throwing money at new technology to deal with latest threat vector. Alternatively, they disapprove security training as the do-nothing approach appears to be working.

Now let's review what the actual best practices are and how to implement them in your organization.

Best Practices for New School Security Awareness Training

The proven best practices for New School Security Awareness Training are designed to add a layer on top of existing firewalls. The goal is to establish an effective human firewall of informed, educated and phish-savvy employees. According to Lance Spitzer, Training Director at the SANS Institute, "One of the most effective ways you can minimize the phishing threat is through awareness and training. You create a network of human sensors that are more effective at detecting phishing than almost any technology."

Best Practice #1: Comprehensive Programs Work

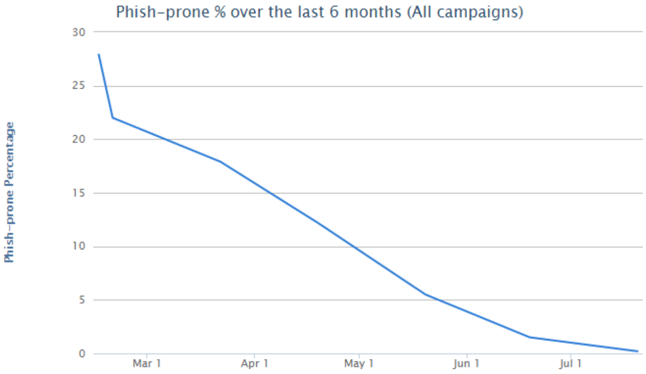
Most security awareness programs are superficial at best. They may include some sensible actions, but they don't dovetail into a coordinated and comprehensive program. What is missing is an appreciation of the adversary being faced and the degree of commitment an organization has to have to stave off attacks. It is vital that the C-suite comes to terms with the extent of the threat and the sheer weight of resources the enemy is bringing to bear against naive employees. Only by doing so is it possible for C-level executives to comprehend the measures that must be taken to secure the enterprise and the vital necessity of erecting a human firewall of informed and ever-vigilant users. The crux of this best practice is having an awareness of the scale of the problem and the resources necessary to defend against it.

Best Practice #2: Develop a Coordinated Campaign that Combines Training and Phishing Simulation

Training on its own, typically once a year, isn't enough. Simulated phishing of personnel on its own doesn't work. But together, they can be combined to greatly increase effectiveness. An important best practice is to intelligently integrate these components into an overall campaign. This is best accomplished by finding a platform that integrates simulated phishing and security awareness training.

Best Practice #3: Baseline Phishing Susceptibility

Security awareness training can be undermined due to difficulty in measuring its impact. How exactly are you supposed to prove that it obtains results? All it takes is one fresh outbreak and someone in authority can point to the event as evidence that such training dollars would be better spent elsewhere.



This is where the baseline comes into play. It is vital to establish a baseline on phishing click-through rates so you know the percentage of users who open malicious emails prior to awareness training campaign commencement. This is easily accomplished. Send out a simulated phishing email to a random sample of personnel to find out the number that are tricked into opening an attachment, click on a link or enter sensitive information. This is your baseline phish-prone percentage. This metric can be later used to determine how effective the campaign is. Further, it provides specific numbers that can prove useful during the purchase order approval process.

Best Practice #4: Gain Executive and IT Buy In

To be effective, top executives and IT managers must be onboard. Thus extensive briefings before and during a training program is a must. Briefings are needed in advance to accomplish finance approval, but it should never end there. Prior to beginning a phishing simulation project, communicate to executives and iron out all political or sensitivity issues in advance.

This should include HR, Legal and union representatives where applicable. Otherwise, such campaigns may be unjustly accused of targeting specific employees, undermining morale or discriminating against certain groups. Only by keeping all interested parties involved, listening to their concerns and addressing their needs can the campaign hope to succeed. In some organizations, there may be pressure to inform employees that a simulated phishing campaign is about to be launched. In those cases, where staff are forewarned, the effectiveness of the campaign is significantly reduced.

Another aspect of this best practice is to inform executives about baseline phishing numbers so they are more aware of the extent of the problem and the uphill task facing the organization. Return to this baseline again and again as a means of monitoring results. Showcase all drops in phishing effectiveness as a way to demonstrate the value of the program.

Best Practice #5: Conduct Random-Random Phishing Attacks

Earlier, we mentioned prairie dogging where an employee notices a simulated phishing email and warns the others in the office about it. This phenomenon can even bring about an apparent drop in phishing susceptibility in tests that doesn't translate into the real world. Employees get used to the simulated actions of the campaign, learn to watch out for them every Monday morning and thereafter continue as normal. What you end up with is a simulated phishing initiative that has little or no impact on employee gullibility.

This is particularly important when you consider the findings from a study by Proofpoint. It found that no company had a zero click rate from phishing attacks. While repeat clickers account for the majority of clicks on malicious links, 40% of clicks are typically one-off clickers. In other words, even the best and the brightest can be caught unawares and will click on something malicious from time to time. Prairie dogging might allow these rare but occasional phishing victims to develop complacency.

The way to guard against this is to use what are termed random-random simulated phishing attacks. This New School Security Awareness Training practice entails the selection of random groups, random schedules, and random phishing templates to gain a more accurate estimate of an organization's likelihood to fall victim to phishing. Instead of sending out the same phishing emails every Monday morning to accounting, every Tuesday at lunch to sales and every Friday evening to manufacturing, switch the tactics and schedules around by varying the groups and schedules randomly. This eliminates prairie dogging and provides the organization with a real metric they can use to determine effectiveness.

Best Practice #6 Personalize Emails

Personalized emails are more believable. In some cases, this can be as simple as adding the employee's first name. But in large organizations, personalization must be taken further. For example, obtain from payroll the names of the banks used by employees for direct deposit and use that bank name in a phishing campaign. Another tactic is to split phishing email into groups such as by departments, or to tie phishing emails into topical or popular events.

> **"Verizon notes that phishing is increasingly employed to gain access and then quietly set up camp inside the corporate network."**
>
> —Osterman Research

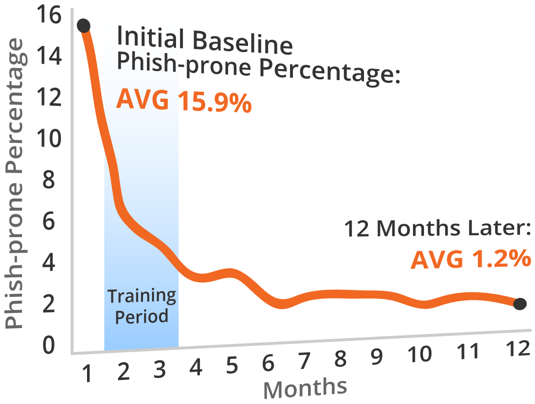
Best Practice #7: Don't Expect Miracles

The results from New School Security Awareness Training are excellent. But they fall short of the miraculous. By that, we mean phishing victimization rates generally fall from the 10-25% range to about 2%. It appears that getting below that point is extremely difficult. But continuation of the campaign can keep results at or below that level, which will have a significant impact on the organization. With malware infections caused by phishing minimized, IT finds itself able to contain remaining outbreaks more effectively as there are far less of them.

Due to the dramatic drop in infections, other security measures have a greater chance of success. IT finds itself moving from constant troubleshooting mode to being able to move forward with projects that provide greater strategic value to the organization.

Best Practice #8: Avoid Witch Hunts

A common concern about simulated phishing is that the results could be used in witch hunts. Therefore, don't ever use results in this way or bring them up in annual reviews. It is best to keep results general and use them to correct and train the organization as a whole as opposed to singling out specific individuals.



The exception to this comes once the coordinated campaign of training and phishing simulation has brought about marked results. After a prolonged series of simulations and training steps, and once the numbers have bottomed out, companies are likely to find the same small group of repeat offenders. Proofpoint noted that less than 10% of users are responsible for almost all clicks on any given wave of malicious attacks. While New School Security Awareness Training can push that number down far lower, there will remain a handful of individuals who continue to click despite being given every opportunity to reform.

By this point, they will have attended several training classes, and received a thorough education on how phishing can fool them. Yet they go on being fooled no matter what remedial steps are taken. Now is the time to involve HR to take up findings with repeat offenders who show no improvement despite several attempts at retraining. To take any possible negative connotation away from 'flunking' simulated phishing tests, it sometimes works to incentivize departments to encourage their staff to complete training or retraining in an effort to achieve a 0% click rate. Those doing so, or scoring below a particular level can be awarded with gift cards or other inducements.

Best Practice #9: Continue to Test Employees Regularly

Even when testing confirms that phishing susceptibility has fallen to nominal levels, continue to test employees frequently to determine if anti-phishing training remains effective. The bad guys are always changing the rules, adjusting their tactics and upgrading their technologies. Therefore, training reinforcement must remain a part of the organizational security arsenal in order to keep pace with constantly evolving threats.

Best Practice #10: Provide Thorough Security Training

Old school security training favored a lecture or video approach. The problem with this type of training is that it can rapidly become outdated – the security landscape of one year ago is very different from that of today. It also focuses too much on theory and isn't balanced by practical application. New School Security Awareness Training is interactive, balances theory and application, is continually updated, and is based upon thorough insight of how cybercriminals operate. Ideally, it will incorporate the services of an expert hacker who knows all the ways of entering an organization and all the tricks of the phishing trade. It should make sure employees understand the mechanisms of spam, phishing, spear-phishing, malware, ransomware and social engineering, and are able to apply this knowledge in their day-to-day jobs.

Conclusion

It is obvious that IT security must be significantly improved on all fronts. Organizations must seek out and adopt the latest methods available in order to keep one step ahead of ever more resourceful organized cybercrime. However, many of the budget dollars spent on such programs will be wasted unless this technology is supported by New School Security Awareness Training programs reinforced by frequent simulated, randomized phishing attacks. The consequences of failing to do so go well beyond bad headlines. The estimated financial loss from 700 million compromised financial records in 2015 was $400 million, according to Verizon. One well-publicized data breach can lead to lost jobs (including that of the CEO, CIO and CISO), rising legal costs, non-compliance penalties, loss of brand reputation, customer churn, and a major hit on the bottom line.

About KnowBe4

KnowBe4 is the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created by two of the best known names in cybersecurity, Kevin Mitnick (the World's Most Famous Hacker) and Inc. 500 alum serial security entrepreneur Stu Sjouwerman, to help organizations manage the problem of social engineering tactics through new school security awareness training.

More than 1,700 organizations use KnowBe4's platform to keep employees on their toes with security top of mind. KnowBe4 is used across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance.

- KnowBe4 wrote the book on cyber security (8 books and counting between Mitnick and Sjouwerman).

- KnowBe4 is the only set-it-and-forget-it security awareness training platform "by admins for admins" with minimum time spent by IT to get and keep it up and running.

- The platform includes a large library of known-to-work phishing templates.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

What Constitutes Effective Security Awareness Training?

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for KnowBe4

May 2016

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

What Constitutes Effective Security Awareness Training?

Introduction

Employees are a critical part of an organization's defense against many IT security threats. Just as having the correct technology solutions is important, training personnel to recognize security threats is a critical part of any security strategy. As part of that strategy, organizations must consider both the content and the training methods. Training that does not engage employees or provide for continuous learning and reinforcement is not sufficient to truly make employees more security aware.

Security Awareness Programs Have a lot to Learn

A recently changing trend, and an encouraging sign, is that many companies are recognizing the critical need for employee security awareness. In 2014, EMA conducted a security research study that showed only 44% of respondents had security training from a current or previous employer. When the research was conducted again in 2015, 59% of respondents indicated they had received some form of security awareness training.

Not only are more employees being trained, but they are receiving more training. In a 2014 study, only 15% of respondents received five or more hours of security training. In 2015, that number jumped to 23%. This is also true with the periodicity of training. In 2014 only 2% of respondents indicated they had received training post incident, while in 2015 respondents who received training grew to 65%.

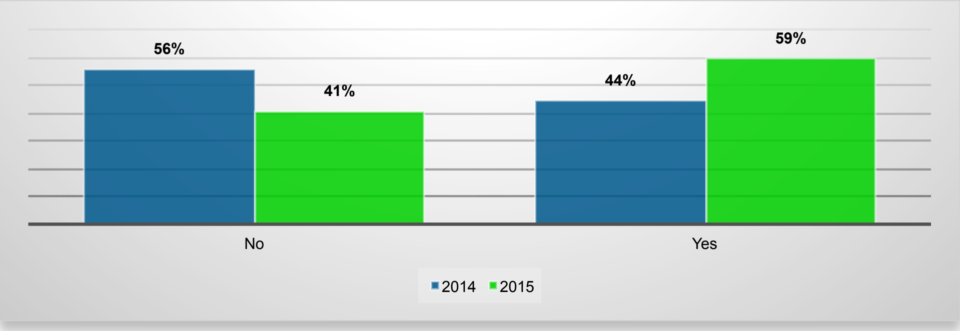


Figure 1a: Security Awareness Training 2014 vs. 2015

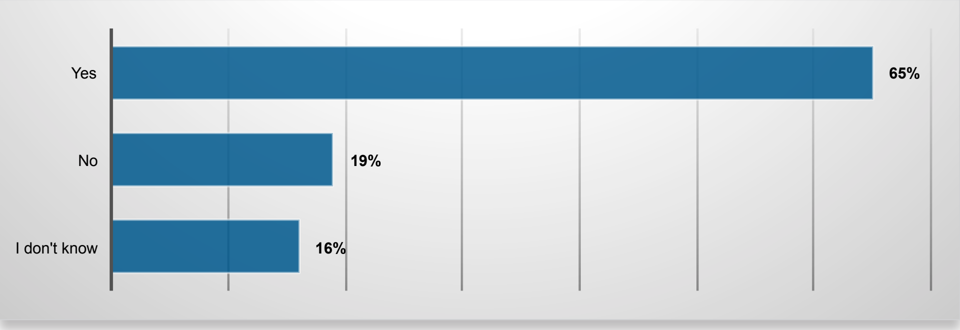


Figure 1b: Organizations Providing Post Incident Awareness Training

What Constitutes Effective Security Awareness Training?

Interactive training methods are known to be far more effective at not only engaging attendees, but improving retention of content. These include programs that present employees with realistic content, security scenarios, and even simulated phishing attacks. These methods are also more continuous in nature. Rather than going to a lecture and forgetting it a week later, continuous training can be directed to present employees with shorter bursts of training at multiple points throughout the year.

Of course, the final piece to effective training is measuring success. Unfortunately, many security training programs still measure effectiveness through attendance. However, attendance cannot measure the most important factors, like how much an employee is actually retaining and changes in behavior that ultimately identify how much less likely they are to fall victim to an attack.

Interactive training methods are known to be far more effective at not only engaging attendees, but improving retention of content.

What is Effective Security Awareness Training?

Research proved that effective security training is a must. Certain methods are simply more effective than others, but what strategies are companies currently employing? KnowBe4 categorized training strategies into five approaches:

- **The Do Nothing Approach** - We do not really provide security awareness training.
- **The Break Room Approach** - We gather employees for a lunch or special meeting and tell them what to avoid when surfing the Web, in emails from unknown sources, etc.
- **The Monthly Security Video Approach** - We have employees view short security awareness training videos to learn how to keep the network and organization safe and secure.
- **The Phishing Test Approach** - We preselect certain employees, send them a simulated phishing attack, and see if they fall prey to the phishing attack.
- **The Human Firewall Approach** - We test everyone in the organization find the percentage of employees who are prone to phishing attacks and then train everyone on major attack vectors, sending simulated phishing attacks on a regular basis.

Forty-one percent of organizations are still doing nothing about security training. Of the companies that are providing security awareness training, almost 60% are using less effective methods such as the Break Room Approach (23%) and the Monthly Security Video Approach (36%). Thus, fully two-thirds of companies are using training methods that are less than ideal, and do not necessarily result in security awareness.

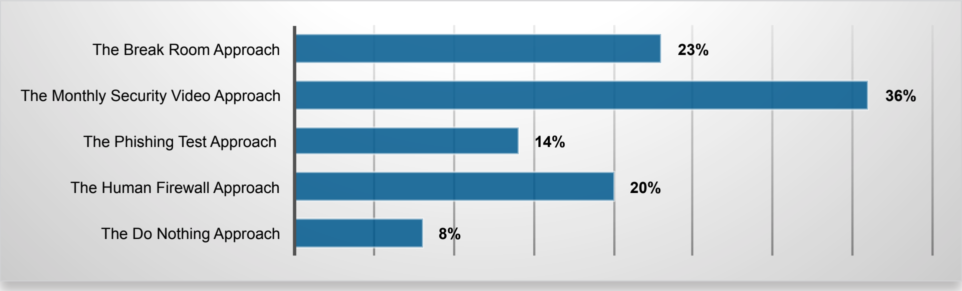


Figure 2: Organizational Approaches to Security Awareness Training

What Constitutes Effective Security Awareness Training?

These numbers demonstrate that despite the training program improvements, there is still significant room for growth in the more interactive, and thus more effective, methods. The Phishing Test Approach, which creates a simulated phishing attack, was employed by just 14% of companies. The Human Firewall Approach, which should really be the goal of a mature awareness program, was used in only 20% of companies that participated.

These results are surprisingly consistent across companies of all sizes and with a variety of employee roles. The results are also fairly consistent across industries. However, education shows a particular lack of more robust training, with no respondents indicating they use the Human Firewall Approach, and just 12% using simulated phishing options. Retail and wholesale organizations also seem to rely heavily on the Break Room Approach (33%) and Monthly Videos (44%) at the expense of more interactive training methods.

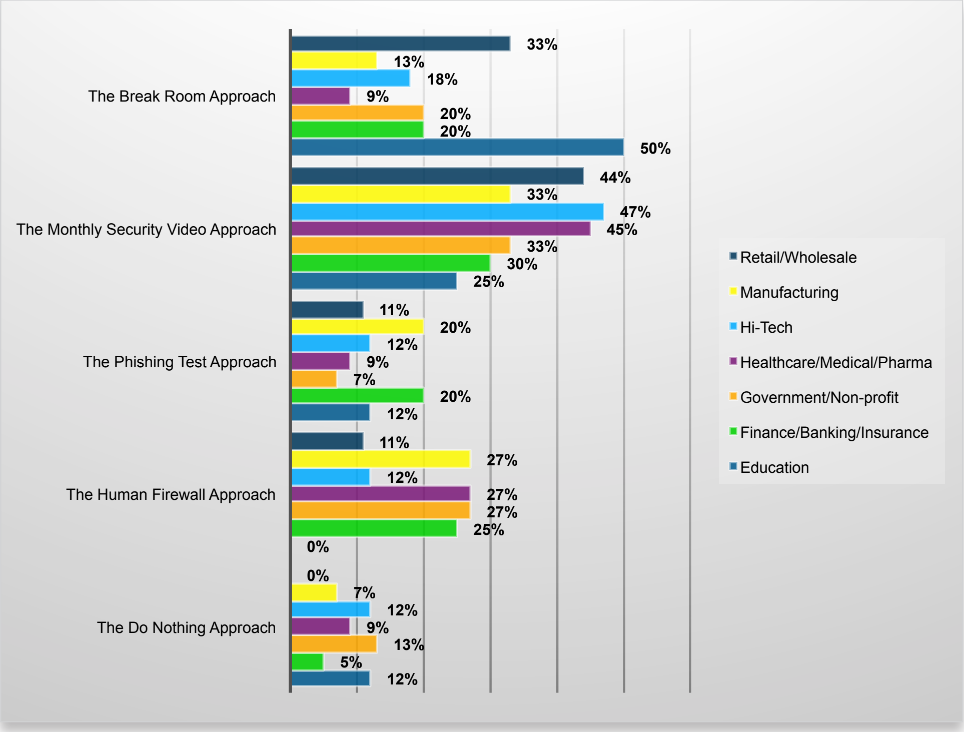


Figure 3: Approaches to Security Awareness Training by Industry

EMA Perspective

Does training lead to confidence that employees are, in fact, well trained against phishing attacks?

It comes back to the type of awareness training. As this paper indicated, the types of training that truly result in security awareness:

- involve interactive elements
- are continuous in nature, with regular follow-ups
- simulate real-life attacks
- have their effectiveness monitored

To achieve security awareness, and thus effective defense, companies must employ comprehensive, interactive training.

Research shows that most of the training employees receive does not offer simulated attacks, testing, or interactivity. The Break Room Approach and Monthly Security Video Approach are still more popular than the more effective training methods such as the Phishing Test Approach and Human Firewall Approach.

To achieve security awareness, and thus effective defense, companies must employ comprehensive, interactive training. This training must be updated regularly, and its effectiveness must be measured through strategies, or another word like employee susceptibility to attack, post incident follow up, and improvement tracking.

If a company is not taking these steps, its employees will not be security aware and the company certainly is not getting the most for its training dollar.

About KnowBe4

KnowBe4 is the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school awareness training approach. This method integrates baseline testing using mock attacks, engaging interactive training, continuous assessment through simulated phishing, vishing and smishing attacks, and enterprise-strength reporting to build a more resilient organization with security top of mind. Thousands of organizations use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government, and insurance. To learn more visit www.KnowBe4.com.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3395.052316

Alliance Chapters

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

CIO Alliances

Johannesburg
Cape Town
Nairobi
Sydney
Melbourne

CISO Alliances

Johannesburg
Cape Town
Durban
Windhoek
Nairobi
Sydney
Melbourne
Lagos

CMO Alliances

Johannesburg
Durban

Executive Business Exchange

South Africa
United Kingdom
DACH
Benelux
Nordics
France