Post event report

e-crime & cybersecurity CONGRESS

The 11th e-Crime & Cybersecurity Congress in Dubai

19th March 2019 | Dubai, UAE

Principal Sponsor

Arrow Five Years Out

RSA

Strategic Sponsors

HELP AG PROTECTING INFORMATION

OPSWAT.

Recorded Future

SOPHOS Cybersecurity made simple.

SHAPE

ThreatMetrix A LexisNexis® Risk Solutions Company

virsec

Education Seminar Sponsors

ANOMALI

KASPERSKY lab

ManageEngine

OneTrust Privacy Management Software

SABSA COURSES.COM

Synack

THALES

Network Security Virtualization TNCT

Networking Sponsors

AIRLOCK DIGITAL

arcon

CLOUDFLARE

DriveLock

emt TECHNOLOGY DISTRIBUTION

PGI

SECURRENT IT SECURITY SOLUTION PROVIDER

Branding Sponsors

FIREEYE™

Green Method

> “e-Crime & Cybersecurity Congress has always provided the best expertise to help and implement solutions for protecting sensitive data from intrusion threats and compromise. Attending the 11th annual e-Crime & Cybersecurity Congress in Dubai was an inspiring experience and I found the presentations very useful and well-structured.”

IT Manager, Al Muqren Exchange

> “To all my fellow IT and IS professionals, “e-Crime & Cybersecurity Congress” is an event you really don’t want to miss. It offers an excellent balance between technical value, market insights and good networking opportunities with peers & vendors. Compared to other events, it is unmatched. The level of organisation is unparalleled, kudos to the AKJ team for their effort.”

Network & Information Security Head, Sharjah Broadcasting Authority

> “It has been an absolute pleasure attending the e-Crime & Cybersecurity Congress in Dubai. It was very useful and insightful, especially for a non-technical professional like me. Amazing efforts in the lead up and execution of the event indeed, it was very well organised and provided a wonderful networking opportunities with fellow professionals.”

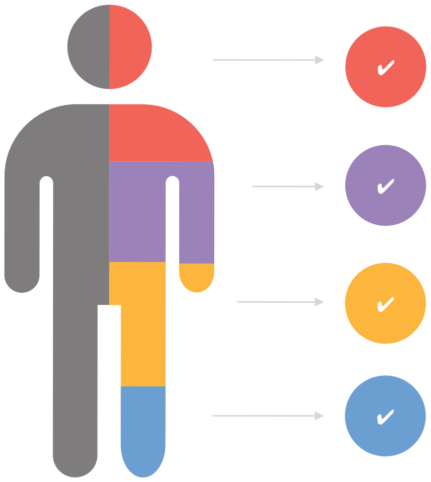
Manager, Quality Control & Service Excellence, Corporate Office Management, EMAAR

Inside this report:

Key themes

- AI: separating the hype from the reality
- Cyber-risk identification, measurement and management
- Securing specialised systems
- The nature of nation state actors
- Cost-effective compliance
- Back to basics

Who attended?



Cyber-security
We have a 15-year track record of producing the events cyber-security professionals take seriously

Risk Management
We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance
We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy
We are a key venue for decision-makers with budget and purchasing authority

Speakers

Ebrahim AL-Alkeem, Information Security Manager, ENEC

Tim Ayling, Kaspersky Fraud Prevention Lead, Kaspersky Lab

Brian Byagaba, Senior Manager Information Security, Commercial Bank International

Antonio Campos Dionisio, Group CIO, MIG Holding

Christos Christou, Chief Compliance Officer, Lulu Exchange

Andrew de Lange, Solutions Consultant, Anomali

Ian Evans, Managing Director, EMEA, OneTrust

Nour Fateen, Pre-sales Consultant, Recorded Future

Bharat Gautam, Head of Information Security, DAMAC Properties

Shuman Ghosemajumder, CTO, Shape Security

Bobby Gupta, VP of Sales for APAC and EMEA, Virsec

Neil Haskins, Head of Security & Technology Operations, Careem

Michael Hirschfeld, Cyber Security Adviser, SABSA

Ilmaz (Kory) Kashkooli, Managing Director, TNCT

Adam Lalani, Group Head of IT, Tristar Transport

Slam Laqtib, Sr. Product Manager, Thales eSecurity

Craig McEwen, Global Head of Cyber Operations, Anglo American

Frank Murray, CISO, Associate Vice President – IT Security, Risk & Business Resilience, MIG Holding

Balaji Nagabhushan, Group Chief Administrative Officer, Tristar Transport

Suresh Nair, Chief Information Security Officer, MENAT, GE

Ron Peeters, Managing Director EMEA, Synack

Mike Pitman, CISO, Dunnhumby

Atiq Raza, CEO, Virsec

Andy Renshaw, Senior Director, Market Planning, Fraud and Identity, ThreatMetrix

Nicolai Solling, Chief Technology Officer, Help AG Middle East

Malay Upadhyay, Technical Head Middle East, Sophos

Agenda

08:00	Breakfast networking and registration
08:50	Chairman's welcome
09:00	**In it for the long run; building a sustainable solution to cybersecurity resourcing** **Craig McEwen,** Global Head of Cyber Operations, Anglo American • Current state of affairs – attacks etc • Current state of affairs – recruitment figures • Future touch points – OT (blended or dedicated and a complete lack of existing skill in the OT area) • Winning the war, not the battle – apprenticeships, talent development etc • What should we be looking for – what is easier to train, cyber-skill and a natural talent/analytical mind etc
09:20	**Communicating with the Board effectively – security strategy definition 101** **Antonio Campos Dionisio,** Group CIO, MIG Holding, and **Frank Murray,** CISO, Associate Vice President – IT Security, Risk & Business Resilience, MIG Holding • Understanding your stakeholders. Identify different functions' business risks, and communicate your message accordingly • Hacking the boardroom. Gaining executive management buy-in by adopting the model of a hacker • Defining your priorities. It's not just about the budget or the underlying technologies. Understand the value for the business instead of 'just squeezing money' out of the board
09:40	**The dark secrets of the Dark Web: an insight into this unique asset and risk, and how it differs from other sources of intelligence** **Nour Fateen,** Pre-sales Consultant, Recorded Future • Real-world examples of threat actor activities in dark marketplaces • Methods for uncovering emerging threats using Dark Web sources
10:00	**The emergence of credential stuffing and cybercriminal AI** **Shuman Ghosemajumder,** CTO, Shape Security • Credential stuffing has been named by CSO Online as the #1 most significant security issue in 2019 • Shuman Ghosemajumder, CTO of Shape Security, will explain how this threat has evolved, starting from when Shape first introduced the term to the marketplace over seven years ago, to how it gained international prominence in numerous sophisticated public attacks • He will also provide insights into the heightened challenges businesses are facing as a result of cybercriminals leveraging AI to attack websites and mobile apps in these cases
10:20	**Education Seminar | Session 1**
	Anomali **Threat actor – a love story?** **Andrew de Lange,** Solutions Consultant, Anomali
	Kaspersky Lab **The ceaseless evolution of consumer transformation** **Tim Ayling,** Kaspersky Fraud Prevention Lead, Kaspersky Lab
	OneTrust **Risky business: a privacy & security team's guide to risk scoring** **Ian Evans,** Managing Director, EMEA, OneTrust
	Thales eSecurity **Re-evaluating data security in modern, multi-faceted environments** **Slam Laqtib,** Sr. Product Manager, Thales eSecurity
11:00	Networking and refreshments
11:30	**Running the risks and regulations. The insider truth on cyber-risk management** **Christos Christou,** Chief Compliance Officer, Lulu Exchange • Introduction to AML/CFT risk management – the regulatory requirements • Security – what is required from a business perspective and how important is security to the decision to make or buy? • Cloud vs Hosted services – what is the business perception and what is the regulatory requirement? • How do we manage the AML/CFT risk and security in Lulu Financial Group?
11:50	**Harnessing the power of a digital identity network: reducing e-crime, building trust** **Andy Renshaw,** Senior Director, Market Planning, Fraud and Identity, ThreatMetrix • How harnessing a global view of trust, and risk, helps detect and block advanced fraud • Building trust using digital identity intelligence can help better distinguish between good customers and fraudsters in near real time • An analysis of recent attack patterns and fraud typologies from the ThreatMetrix Digital Identity Network, which analyses 110 million transactions a day
12:10	**FILES: The enfant terrible of any IT environment** **Nicolai Solling,** Chief Technology Officer, Help AG Middle East • There are thousands of file formats and they are ultimately the agents that deliver everything from a website to an attachment in your inbox. While files are good and deliver functionality, they can also be bad, weaponised delivery vehicles for malware • In this session we will talk about files, the types one should be extra careful about and how these are utilised in social engineering, malware and crypto-attacks • In a world where attackers have more resources and capabilities than ever, we will discuss how small changes and new technologies can significantly increase your robustness against both file-based and file-less attacks

Agenda

12:30	**Industrial control, ICS-SCADA and other vital systems** **Atiq Raza,** CEO, Virsec, and **Bobby Gupta,** VP of Sales for APAC and EMEA, Virsec • Critical infrastructure systems around the world are under assault from targeted cyber-attacks seeking to cause damage, disruption, theft and significant financial losses. Advanced attacks like Stuxnet, BlackEnergy, Triton, and Industroyer bypass conventional security and subvert legitimate applications and processes to infiltrate sensitive systems • Virsec is the first solution to provide ICS cybersecurity and protect industrial control systems (ICS), supervisory control and data acquisition (SCADA), and other mission-critical applications at the process memory level. Acting as a memory firewall, Virsec scrutinises application process memory to ensure that critical applications only behave as intended and aren't corrupted by advanced exploits
12:50	**Education Seminar | Session 2** **OneTrust** **A privacy playbook for 'reasonable and appropriate' security measures and safeguards** **Ian Evans,** Managing Director, EMEA, OneTrust **SABSA** **Using SABSA techniques to develop a cybersecurity strategy** **Michael Hirschfeld,** Cyber Security Adviser, SABSA **Synack** **Offensive security testing with a Hacker mindset** **Ron Peeters,** Managing Director EMEA, Synack **TNCT** **Let's demystify cloud security!** **Ilmaz (Kory) Kashkooli,** Managing Director, TNCT
13:30	Lunch and networking
14:30	**Getting smart about threat intelligence** **Ebrahim AL-Alkeem,** Information Security Manager, ENEC • How AI impacts and aids threat intelligence • How AI impacts and aids threat intelligence: how they are using AI in the cybersecurity effort • How and where to invest in AI and machine learning tools
14:50	**Synchronised security: cybersecurity as a system** **Malay Upadhyay,** Technical Head Middle East, Sophos • Ever changing threat landscape • How a tightly integrated cybersecurity system enables you to stay ahead of the adversaries and nation-state attacks • How to turn cybersecurity from a business cost to a business enabler
15:10	**Upping the cybersecurity benchmark. How good is good enough?** **Suresh Nair,** Chief Information Security Officer, MENAT, GE • The various challenges of large multi-national corporations vs. SMEs • Managing third-party security. Is the security of your third parties as important as the security of your organisation itself? How do you audit and benchmark the security of your third parties? • 'Minimum baselines and standards' of cybersecurity. How do you decide what is the bare minimum for your business? • Cyber-risk management. What are the metrics? How do you model and analyse cyber-risk?
15:30	**Cyber: the senior management perspective** **Balaji Nagabhushan,** Group Chief Administrative Officer, Tristar Transport • What do your senior management and stakeholders want to know about the cybersecurity of your organisation? • How does cybersecurity fit alongside other functions such as risk, legal and CSR? • Risk management perspective. How has cybersecurity become a wider part of overall operational risk? Is cyber-risk unique? And should it be measured and valued in the same way as other forms of operational risk? • Communicating with stakeholders. What do they need to know and how does cybersecurity now arguably affect the market share price and commercial value of an organisation?
15:50	Networking and refreshments
16:10	**Journey from the 'dark side': one business leader's journey from vendor to end-user** **Neil Haskins,** Head of Security & Technology Operations, Careem • Double perspectives on navigating the solutions provider landscape and truths about cybersecurity budget and procurement • The journey from the dark side, the transition to the good side. What both sides know – and need to share – about cyber-resilience • Case study from Careem: what went wrong. And what we did to put it right…
16:30	**EXECUTIVE PANEL DISCUSSION** **The new inconvenient truths on AI, machine learning and its impact on business** **Adam Lalani,** Group Head of IT, Tristar Transport **Ebrahim AL-Alkeem,** Information Security Manager, ENEC **Brian Byagaba,** Senior Manager Information Security, Commercial Bank International **Bharat Gautam,** Head of Information Security, DAMAC Properties
16:50	**Making Big data big business. How information security and data governance can work to your commercial advantage** **Mike Pitman,** CISO, Dunnhumby • Information security as a commercial competitive advantage • How your data governance can win or lose you clients • The CISO as business enabler: working with commercial functions • ISO 27001 certification: Does this give your clients confidence or a false sense of security?
17:10	Conference close

Education Seminars	
Anomali **Threat actor – a love story?** **Andrew de Lange,** Solutions Consultant, Anomali	Do we romanticise cyber-threat actors? When a cyber-incident strikes, we may love the idea that it is some APT (insert number here) or Fancy/Angry (insert animal here) or some other famous threat actor, perhaps with nation-state abilities. But we may also hate the idea that it might be: these are the most dangerous adversaries. In reality our enemies aren't even on our radar, because we turn a blind eye to the smaller signals our controls catch for us. But sometimes these are small pieces of a bigger puzzle we need to understand. What you will learn in this seminar: • Leveraging critical thinking and finding trends in the noise • Actor profiling • The importance of remaining unbiased in your research • Collaboration to find the common enemy
Kaspersky Lab **The ceaseless evolution of consumer transformation** **Tim Ayling,** Kaspersky Fraud Prevention Lead, Kaspersky Lab	In this presentation, hear about the recent history and the future of technology and consumer patterns and drivers. This session explores the continued proliferation of social media, IoT, cryptocurrency & artificial intelligence and the implications of this technology. The huge rise in cybercrime and fraud highlights the challenges businesses face across all industries. This session takes a look at what those challenges are, how we can react to them and what we can do better. It covers: • Changes in our digital lives and how this drives the consumer • The value of data in today's world and the implications of this • The current state of e-fraud
OneTrust **Risky business: a privacy & security team's guide to risk scoring** **Ian Evans,** Managing Director, EMEA, OneTrust	Risk scoring across vendor management, breach notifications, DPIAs and other activities is imperative for compliance with many global privacy laws and security frameworks. Organisations routinely tailor their data protection and security activities based on the results of detailed risk assessments, but this leads to a myriad of questions. How do you calculate risk? What constitutes low, medium or high risk? How do you define a risk criteria? What's the difference between inherent, current and residual risk? In this session, we'll detail the importance of conducting risk assessments under global privacy laws like the GDPR and security frameworks such as ISO 27001, provide scenario-based approaches to risk assessment and give examples on how to tailor your approaches based on risk level. • Understand various approaches to conducting risk assessments • Learn how to define a risk criteria and how to calculate risk level • Learn how to tailor your privacy and security programmes using a risk-based approach
OneTrust **A privacy playbook for 'reasonable and appropriate' security measures and safeguards** **Ian Evans,** Managing Director, EMEA, OneTrust	With a new era of privacy regulations upon us, requirements for implementing 'reasonable and appropriate' security measures and safeguards are becoming more common than ever. While privacy and security professionals often view security from different perspectives and may have competing priorities, there are a number of ways in which these differences can be used to the advantage of both teams. In this session, we'll share a playbook on how to build a harmonised and risk-based security framework that addresses a variety of divisions within an organisation, as well as how security and privacy teams can work together to become more effective. • Understand the requirements and importance of implementing 'reasonable and appropriate' security measures and safeguards for privacy professionals • Outline several areas of common ground that should help every organisation align their security and privacy operations • Take away a playbook for building a harmonised and risk-based security framework

Education Seminars

SABSA

Using SABSA techniques to develop a cybersecurity strategy

Michael Hirschfeld, Cyber Security Adviser, SABSA

The SABSA architectural methodology has a number of tools, techniques and frameworks that can help IT security professionals understand the challenges they face, present and discuss with their executive and stakeholders when building and progressing a cybersecurity programme.

Fundamentally, a strategy is a document that sets out how you plan to achieve a series of long-term objectives.

Within cybersecurity our objectives must be closely aligned with those of the ICT group and, just as importantly, with those of the business as a whole.

If our cybersecurity strategy isn't helping the business or ICT meet their objectives, then we will struggle to articulate our relevance and we will find it difficult to get budget. On the other hand, when our strategy clearly aligns and strengthens the business we are viewed more as a partner.

This presentation will cover a few of the basics of SABSA, provide you with a framework for a cybersecurity strategy and then demonstrate
how understanding and applying some key techniques from the SABSA tool kit can assist you in developing and presenting a coherent and aligned cybersecurity strategy that the business will understand.

What attendees will learn:

- The basics of SABSA
- How to structure a cybersecurity strategy
- Key inputs into the cybersecurity strategy
- Key techniques for developing a cybersecurity strategy

Synack

Offensive security testing with a Hacker mindset

Ron Peeters, Managing Director EMEA, Synack

CISOs are experiencing exponential growth in cyber-attacks, and those attacks are increasingly sophisticated with greater break-in success. Traditional vulnerability scanning and compliance-based penetration testing have proven insufficient to reduce vulnerability against such malicious hackers and Nation State attacks.

During this session, attendees will learn:

- Why traditional solutions such as vulnerability scanners and pen testing are no longer sufficient enough to protect against cyber attacks
- Of a revolutionary security testing approach that deploys large teams of international, top-class security researchers
- How a controlled crowdsourced deployment platform can find serious vulnerabilities in any live system within a matter of hours
- And you'll hear about several case studies, including one on the Pentagon where Synack was able to break in within just four hours

Education Seminars	
Thales eSecurity **Re-evaluating data security in modern, multi-faceted environments** **Slam Laqtib,** Sr. Product Manager, Thales eSecurity	Businesses, institutions and government agencies continue to be breached. Hackers have proven that traditional technologies and conventional approaches are not enough to prevent this epidemic. This is true even for the most sophisticated organisations with world-class security specialists and scientists. And now the challenge has become more complex, with deployments involving the rise of multi-faceted environments, including on-premises, public cloud and hybrid cloud implementations. Because breaches are inevitable, rendering data useless to hackers by applying data security best practices is critical: using key management and encryption to attach security to the data itself is the only way out. In this talk, we will do a deep dive into: • Securing data and rendering it useless in multi-cloud and hybrid environments • Best practice key management, encryption, tokenisation and de-identification techniques • Cloud management as a service with true multi-cloud support
TNCT **Let's demystify cloud security!** **Ilmaz (Kory) Kashkooli,** Managing Director, TNCT	• How much of the 'cloud' do we really use on a day-to-day basis? ○ Chances are we think we do not use any form of cloud-based services. In fact, it is otherwise and we will be reviewing some examples in our daily lives which are clear indications of how extensively we actually utilise cloud-based services in our daily lives. ○ The reality of 'shadow-IT' as an inevitable result of using cloud! • A quick introduction of cloud-based services (Something-as-a-Service)! ○ Nowadays we come across a long list of 'something-as-a-service'! Let's take a look at some of these terms and demystify them a bit. • A closer look at SaaS and IaaS as well as their use cases and some of the security concerns. ○ Why, where and when do we seem to use SaaS or IaaS based cloud-based services? ○ Before starting to use SaaS and IaaS we must really be aware of the fundamental security concerns around them in a corporate context. ○ How can we address the listed security concerns as of today using the available technologies? ○ Let's explore some of the challenges that are still not addressed today. • Final take away – visibility! ○ Cloud is Complex! Security is Complex! And Securing our Cloud usage can be quite Complex! A bird's-eye-view and holistic visibility is KEY to effectively and more pro-actively securing our cloud usage.