Post event report

Strategic Sponsors

BeyondTrust
CROWDSTRIKE
DARKTRACE
Fidelis Cybersecurity
LexisNexis RISK SOLUTIONS
SentinelOne
TREND MICRO

Education Seminar Sponsors

Arcon
BULWARK Technologies
netwrix
PGI
Recorded Future
Synack
tripwire

Networking Sponsors

FIREEYE
ManageEngine
ThreatConnect

"Thank you for the opportunity given to participate on this event. It was one of the well planned and organised virtual events I have taken part recently. Online platform was impressive. I haven't missed the experience of the real event except food. It was well replicated with all the necessary resources and informative presentations."
STE, Emirates

"Felt the event was very well organised despite the challenges faced by the pandemic. I really enjoyed most of the presentations and acquired lot of knowledge. Overall I was bit more comfortable on the virtual platform as I could attend most of the sessions at the comfort of home. Once again well done to your team and the experts who took their time to keep us engaged on the conference with a variety of topics and views. It helps developing maturity surrounding security decisions to be taken within an organisation."
Information Security Manager, RSA Insurance Group

"The e-Crime Congress organised virtually on 21st October was one of a kind. The contents were as always excellent and engrossing. What stood out is the format, layout of the website, organisation and logistics – it was absolutely amazing. A huge thank you to AKJ Associates for hosting such a wonderful event!"
Chief Risk Officer, RAKBANK

"I have been attending e-Crime Congress for three years now and by far, this is the one I enjoyed the most."
Technical Lead, Propertywifi.com

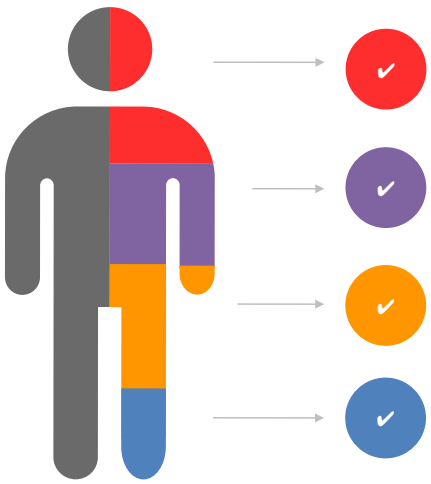
"e-Crime Congress and AKJ always delivers extra value. This is one of the not to miss events in my event radar. The 2020 virtual experience version was delivered with a greater quality in terms of its planning, organisation and content regardless of the COVID-19 limitations and challenges."
CISO and UAE based Digital Transformation & Cyber Security Strategist

Inside this report:

Key themes

- Rethinking identity and access management
- Securing digital currencies
- Building in security: easier said than done?
- Cybersecurity by remote control
- Securing and protecting remote employees
- Cybersecurity for business resilience
- Securing the surveyed citizen
- Protection versus business needs
- Securing the customer – are your websites up to it?
- Stuck in the cloud

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

Majed Alshodari, CISO
Allied Cooperative Insurance Group

Anil Bhandari,
Chief Mentor & Thought Leader
ARCON

Saqib Chaudhry, Head of Digital Innovation and Development
Cleveland Clinic Abu Dhabi

Abdelkader Cornelius,
Threat Intelligence Analyst
Recorded Future

Roland Daccache,
Team Leader – Sales Engineering
CrowdStrike

Hossam Nabil Elshenraki,
Associate Professor
Dubai Police Academy

Tomas Evans, Technical Security Specialist and Trainer
Protection Group International

Romit Gupta,
Cyber Security Account Director
Darktrace

Craig Harber,
Chief Operating Officer
Fidelis Cybersecurity

Illyas Kooliyankal, Chief Information Security Officer
Abu Dhabi Islamic Bank

Karl Lankford,
Director Solutions Engineering
BeyondTrust

Abubakar Latif,
Director of Cyber Security
BNET – Bahrain Network

Mike Loginov,
CISO & CPO Executive Director
NEOM

Dave Meltzer, CTO, Tripwire

Mohamad Mahjoub, CISO Middle East
Veolia

Ahmed Nabil, Regional Senior Information Security and Risk Manager
Leading International Financial Institution

Ron Peeters,
Vice President Middle East and Emerging Markets
Synack

Hani Abdul Qader, Systems Engineer
Trend Micro

Shahab Siddiqui,
Global Head of Cyber Security
Petrofac

Ed Sleiman,
Head of Information Security
King Abdullah University of Science and Technology (KAUST)

Ilia Sotnikov,
Vice President of Product Management
Netwrix Corporation

Jan Tietze,
Director Security Strategy EMEA
SentinelOne

Agenda

08:00 Login and networking

08:55 Chairman's welcome

09:00 **The changing role of the CISO: risks and rewards**

Illyas Kooliyankal, Chief Information Security Officer, Abu Dhabi Islamic Bank

- It has never been more important for security teams to understand and support the business, how should CISOs adapt?
- Digital transformation has increased the risk appetite of many organisations; what does this mean for your security strategy?
- Empowering your security teams: How to equip your team for the rise of AI and Big Data
- Monitoring and access management for data-centric security

09:20 **Reducing time to containment: THE security priority**

Jan Tietze, Director Security Strategy EMEA, SentinelOne

With limited resources, an ever-growing skills gap and an escalating volume of security alerts, organisations are left vulnerable to what is perceived to be unavoidable risk. This environment is demanding more of already resource-constrained CISOs. In this keynote we will be discussing how automation can help to:

- Drastically reduce the amount of uninvestigated and unresolved alerts
- Automate time-consuming investigations and remediate well-known threats
- Act as a force multiplier for resource-constrained security teams

09:40 **UPM: Empowering a remote workforce and improving your security posture with Universal Privilege Management**

Karl Lankford, Director Solutions Engineering, BeyondTrust

The new normal of a remote workforce has changed the threat model of the organisation overnight. Join this session and learn:

- Considerations for a secure remote working environment
- How to balance remote workers security and productivity
- Recommendations to support a remote workforce with a PAM solution

10:00 **Cybersecurity governance in the new normal**

Majed Alshodari, CISO, Allied Cooperative Insurance Group

- The COVID-19 pandemic has changed the risk tolerance of many businesses: how to adapt the cybersecurity policies and procedures to suit changing business norms
- Onboarding new technologies and minimising the security risks of the virtual collaboration tools
- Developing an effective communication strategy with the board to embed cybersecurity into the business
- Optimising and embedding the information security into the new era of emerging technologies and digital business transformation

10:20 **Education Seminars | Session 1**

Recorded Future	Synack	Tripwire
You get what you pay for – cybercriminal operations in the Middle East underground economy **Abdelkader Cornelius,** Threat Intelligence Analyst, Recorded Future	**Transition to offensive security testing with crowdsourcing** **Ron Peeters,** Vice President Middle East and Emerging Markets, Synack	**Case studies in integrity: Why small changes keep causing big breaches, and how to stop it** **Dave Meltzer,** CTO, Tripwire

10:50 Networking break

11:20 **Security for the truly digital business**

Shahab Siddiqui, Global Head of Cyber Security, Petrofac

- The acceleration of digitalisation has changed the threat landscape: threat actors are on the rise in the Middle East and attackers are exploiting new attack vectors; how can organisations defend against these changing threats?
- Managing insider threats and access management in the remote digital workplace
- Cloud vs. on-premise: finding the right balance for your business and addressing the security challenges

11:40 **Going beyond malware – stopping 'living off the land' attackers in their tracks**

Roland Daccache, Team Leader – Sales Engineering, CrowdStrike

- Evolution of sophisticated attacks to evade detection
- The behavioural indicators of an advanced intrusion
- Analysis of well-crafted hands-on-keyboard attacks
- Technology advancements and the use of AI in detecting and stopping 'living-off-the-land' intrusions

12:00 **Presentation by LexisNexis Risk Solutions**

Agenda

12:20 — Offensive AI vs. Defensive AI: Battle of the algorithms

Romit Gupta, Cyber Security Account Director, Darktrace

- Paradigm shifts in the cyber-landscape: The emergence of AI-enhanced malware is making cyber-attacks exponentially more dangerous and harder to identify. In the near future, we will begin to see supercharged, AI-powered cyber-attacks leveraged at scale
- To protect against offensive AI attacks, organisations are turning to defensive cyber AI, which can identify and neutralise emerging malicious activity, no matter when, or where, it strikes
- Learn about the immune system approach to cybersecurity and defensive, and autonomous response capabilities
- We will explore real-world examples of emerging threats that were stopped with Cyber AI

12:40 — Education Seminars | Session 2

ARCON	Netwrix	PGI
Design thinking and zero trust architecture: key to strong cybersecurity posture **Anil Bhandari,** Chief Mentor & Thought Leader, ARCON	**Calculating ROI for security: Why this is so difficult? Do you need it?** **Ilia Sotnikov,** Vice President of Product Management, Netwrix Corporation	**Manual file carving for DFIR practitioners** **Tomas Evans,** Technical Security Specialist and Trainer, Protection Group International

13:10 — Lunch and networking break

14:10 — A new vision: NEOM as a cybersecurity utopia

Mike Loginov, CISO & CPO Executive Director, NEOM

- Managing the complex ecosystems of smart megacities: increased connectivity = increased risks
- Developing operational technologies with security built-in to thwart attacks
- Mobilising cybersecurity skills to ensure security teams adapt and keep up with the changing security landscape
- How NEOM is developing an intelligent and reliable security system from the ground-up

14:30 — Stack rationalisation – gaining the decisive advantage

Craig Harber, Chief Operating Officer, Fidelis Cybersecurity

- Ensuring continuous real time visibility of managed and unmanaged assets
- Building threat driven operations
- Shaping the adversary experience to build your advantage
- Building proactive, protective, predictive, retrospective and reactive defence capabilities

14:50 — From on-prem to the cloud, securing email systems is still a top priority

Hani Abdul Qader, Systems Engineer, Trend Micro

- Traditional email system security challenges migrated with it to the cloud
- New challenges/tweaks are on the rise
- Adapting comprehensive multilayered protection, detection, and response is the solution

15:10 — EXECUTIVE PANEL DISCUSSION: A new beginning: cybersecurity and the acceleration of digital transformation

Many organisations in the Middle East are making significant in-roads into their digital transformation journey. In recent years, big data analytics, IoT, AI and cloud have been readily welcomed as organisations come to terms with the long-term value of digital initiatives. For many organisations, the recent COVID-19 crisis has changed digital transformation priorities as businesses have been forced to operate entirely online and this rapid, unplanned digitalisation has increased the risk and impact of cyber-attacks. So as digitalisation accelerates, how should cybersecurity adapt?

Mohamad Mahjoub, CISO Middle East, Veolia
Abubakar Latif, Director of Cyber Security, BNET – Bahrain Network
Ahmed Nabil, Regional Senior Information Security and Risk Manager, Leading International Financial Institution

15:30 — Networking break

16:00 — 2020 strategies for effective security team management

Ed Sleiman, Head of Information Security, King Abdullah University of Science and Technology (KAUST)

- Addressing the cybersecurity talent shortage – what methods should we be implementing to hire and maintain talent within security teams?
- How to strike the balance between your people and technology/automation to address security risks – can they be successfully combined?
- Information security teams need unfettered remote access to the most sensitive systems and information – are they the weakest link? How to ensure they're not hacked when operating remotely

16:20 — The effects of COVID-19 on cybercrime and online fraud

Hossam Nabil Elshenraki, Associate Professor, Dubai Police Academy

- The new wave of cyber-scams and new criminal methods during COVID-19
- How cybercriminals have adapted to a changing world: targeting online schooling and remote workers
- Case studies from police operations

16:40 — Incorporating cybersecurity into digital innovation projects from the get-go

Saqib Chaudhry, Head of Digital Innovation and Development, Cleveland Clinic Abu Dhabi

- Medical innovation at CCAD: how innovation is transforming the healthcare industry
- Ensuring digital innovation and cybersecurity are partners in developing projects from the beginning
- Implementing effective risk management into digital innovation projects
- Actioning a cybersecurity strategy that supports and enables the business' transformation goals

17:00 — Networking break

17:30 — Conference close

Education Seminars

ARCON

Design thinking and zero trust architecture: key to strong cybersecurity posture

Anil Bhandari, Chief Mentor & Thought Leader, ARCON

Absence or poor privileged access control policy and user authorisation mechanism results in employees accessing resources, applications or critical systems that they are not supposed to access. This is a major and serious loophole organisations leave in the remote IT infrastructure where the malicious actors misuse it by compromising privileged accounts and siphoning off confidential information. ARCON Mentor Anil Bhandari breaks down design thinking and zero trust architecture framework.

- Spectrum of cybersecurity
- Principles of design thinking
- Identity management
- Remote access management
- Maintaining low friction high security and much more

Netwrix

Calculating ROI for security: Why this is so difficult? Do you need It?

Ilia Sotnikov, Vice President of Product Management, Netwrix Corporation

The ongoing stream of data leaks and other breaches of consumer trust is a top concern for executives at organisations around the world. To make sound decisions about cybersecurity strategy, especially during challenging times like these, when budgets are tight, they need accurate assessments of the effectiveness of proposed security investments. However, providing those estimates of ROI can be extremely difficult for CISOs, who often struggle to quantify the expected impact of security measures.

Join us for this educational session and learn:

- What are the 4 key benefits of a security investment
- How to effectively communicate the value of cybersecurity investment to senior decision makers
- How to convince executives to make data security investments right now

PGI

Manual file carving for DFIR practitioners

Tomas Evans, Technical Security Specialist and Trainer, Protection Group International

This is a technical cybersecurity skills module from PGI's 5-day UK Government Certified Digital Forensics and Incident Response Practitioner course, which can be taken as preparation for the CREST Registered Intrusion Analyst certification. The module is designed to explain how the Wireshark extraction tool works and how to deal with tool failures by performing the same task manually. PGI's technical skills training is designed to ensure that UK government certified cyber-professionals understand how and when to use tools, and also know what the tools are doing for them, and how to deal with tool failures by reverting to first principles. This is especially important in the unpredictable and complex field of DFIR where the unexpected is expected.

In this session you will learn:

- When and how to use Wireshark to perform extraction of image files from a packet capture file using the automated capabilities of the tool
- How to extract the transferred assets manually
- How to save out the raw conversation
- How to edit the transfer with a hex editor

Education Seminars

Recorded Future

You get what you pay for – cybercriminal operations in the Middle East underground economy

Abdelkader Cornelius, Threat Intelligence Analyst, Recorded Future

In our digital age, companies that transact business online find their data targeted by various forms of cyber-fraud. These cyber-fraud products and access broker services can be bought and rented freely on the dark web with ease. This is fuelling sophisticated payment systems on the underground economy in the Middle East.

During this session, we will cover:

- Exclusive access to live threat intelligence feeds from the region
- A detailed review of some of the methods being used in the underground economy
- How to use security intelligence to defend your organisation

Synack

Transition to offensive security testing with crowdsourcing

Ron Peeters, Vice President Middle East and Emerging Markets, Synack

Although you might have a sense of security that you are well protected, increasingly sophisticated cyber-attacks can easily breach your most important web and mobile applications and networks, demonstrating that vulnerability scanners and traditional pen testing are no longer good enough to find many of these exploitable breach points.

In this session you'll learn:

- About a next generation security testing platform incorporating advanced, offensive and adversarial security testing with artificial intelligence
- How one of the world's most elite hacking teams of over 1,500 international, top-class security researchers can be virtually deployed at short notice
- Why deploying teams of top security experts on your IT assets will typically lead to finding serious exploits in a matter of hours or days
- Of use cases and POCs performed at customers in the Middle East (UAE/Saudi Arabia)

Tripwire

Case studies in integrity: Why small changes keep causing big breaches, and how to stop it

Dave Meltzer, CTO, Tripwire

Misconfigurations and inadequate change control are consistently cited as a top cause of breaches – whether its within traditional IT data centres, in the cloud, or on factory floors. This is not the inevitable result of the increasing pace of change and sprawl of infrastructure, but it is an indication that for many organisations, changes are outpacing the security team's ability to monitor and respond to risks they pose. During this session, you will hear Tripwire's CTO share his experience working with leading companies around the world and learn:

- Case studies in how integrity is being managed in security programmes from leading companies in financial services, telecommunications, and energy sectors around the world
- Attributes of effective integrity assurance programmes
- How to evaluate the maturity of your existing programme
- How to get started with a new integrity programme, or take your current one to the next level of maturity
- The benefits for security, IT operations, and compliance from running an effective integrity programme