Cyber Security and Risk Management Summit

18 December 2019 - Cairo Marriot Hotel

A state of Cyber Security, Regulations and Trends in Egypt

Cyber security has emerged as a key enterprise-wide risk for organizations. Cyber-attacks are no more a work of lone warriors or a group of hackers but involve cyber-crime syndicates, collaborating and investing large amount of money, precision, knowledge, expertise and persistence. Their capabilities are equal if not better than state actors.

Statistics suggest that cyber incidents are growing in double digits worldwide and the impact due to incidents has resulted in significant damage, spanning from financial losses, disruption of operational services to erosion of shareholder value and trust.

Due to technological changes, every organization has to deal with cyber security issues. Managing cyber risks is not a snapshot, but an ongoing process. This is partly because technology constantly offers new possibilities, but also because national and international legislation in the field of privacy and supervision is constantly changing.

Across all sectors and in every geography, business executives are asking themselves the same questions:

- Can I balance information protection and accessibility?
- What does a 'good' cyber security strategy look like in my sector?
- Can I prioritize cyber risks based on my company's strategy?
- How do I determine the right level of investment?
- Where should I put my investments?
- How can I prevent or mitigate the disruption of a cyber event?
- How do I ensure that our business returns to normal as quickly as possible?

The Egyptian Center for Economic Studies (ECES) with full sponsorship from KPMG Hazem Hassan are pleased to conduct a summit discussing

(a) global cyber security incidents and trends

(b) regulatory and legal requirements and challenges; and

(c) a framework based approach for enterprises to strengthen the cyber security posture.

We hope to see you in the workshop and please feel free contact me for any further details.

Thank You

Abla Abdelatif
Executive Director and Director of Research
ECES – Egyptian Center for Economic Studies

Hatem Montasser
Managing Partner
KPMG Hazem Hassan

Workshop highlights:

- A keynote session discussing the current threat landscape, global and local cyber security incidents and trends, role of regulators in addressing the cyber security risks and how can enterprises look to strengthen their cyber security posture.
- A technical session to discuss cyber incident management and a blue print to address monitoring capabilities for incident detection, its response and forensics.
- A debate to share ideas and thoughts on upcoming privacy legislation, its impact on business, preparedness and compliance.
- Discussion on cyber security skills and capabilities needed for future, collaboration between academia, industry and government to nurture talent and qualities required for a CISO to be effective.

Registration deadline:
15 Dec. 2019

Cyber Security and Risk Management Summit

18 December 2019 - Cairo Marriot Hotel

Registration process:

Participants need to complete the attached registration form as soon as possible, but no later then 15 December 2019 and sending it by email to: sshaltout@kpmg.com

Questions:

For logistics related questions:
Please contact Ms. Salma Shaltout
(email: sshaltout@kpmg.com)

08:30 - 9:00 am	**Registration & Reception**	
09:00 - 09:15 am	**Introduction & Welcome note**	• Mr. Hatem Montasser • Dr. Abla Abdelatif • Mr. Akhil Bansal • H.E. Shri Rahul Kulshreshth *Ambassador of India to Egypt*
09:15 - 10:00 am	**State of Cyber Security – Global level and Egypt**	• Mr. Akhilesh Tuteja
10:00 - 11:00 am	**Businesses Panel** ***Moderated by:*** ***Mr. Hossam Saleh*** ***Egyptian Media Group***	• Dr. Mahmoud Khattab … **B.Tech** • Mr. Tarek Fahmy …….**MSC** • Mr. Ashraf Wageih ……..**Global Napi** • Mr. Tarek Elkouly …….**SAIB**
11:00 - 11:15 am	**Coffee break**	
11:15 – 12 noon	**Are you ready to recover and respond to cyber attack**	**1st KPMG Presentation** Mr. Chandra Prakash
12 :00 – 1:00 pm	**Lunch break**	
1:00 – 1:45 pm	**Capabilities, Skills & Thinking interactive session**	**2nd KPMG presentation** Mr. Akhilesh Tuteja
1:45 – 2:00 pm	**Coffee break**	
2:00 – 2:45 pm	**Regulators Panel** ***Moderated by:*** ***Dr. Abla Abdelatif*** ***ECES***	• Mr. Hazim Rizkana ……. **Rizkana & Partners** • Mr. Mohamed Gamil ……**Ministry of Justice** • Mr. Mohamed Farid …….**EGX** • Dr. Ashraf Abdelwahab ..**SAP** • Dr. Sherif Hazem ……**CBE**
2:45 – 3:00 pm	**Closing notes**	• Mr. Hatem Montasser • Dr. Abla Abdelatif • Mr. Akhil Bansal

Cyber Security and Risk Management Summit

18 December 2019 - Cairo Marriot Hotel

Turn cyber risk into opportunity

Financial Services

Cyber security is assuming criticality in the organizations reputation. The regulators are looking at these aspects in increasing focused manner. It is estimated that **Financial institutions spend an average of 0.2%-0.4% of their revenue and around 10-12% of their IT budget on cybersecurity.**

JPMorgan Chase CEO Jamie Dimon in a letter to shareholders earlier this year. He went on to say his company spends $600 million annually and employs 3,000 personnel dedicated to cybersecurity.

"The threat of cyber security may very well be the biggest threat to the U.S. financial system. I have written in previous letters about the enormous effort and resources we dedicate to protect ourselves and our clients – we spend nearly $600 million a year on these efforts and have more than 3,000 employees deployed to this mission in some way. Indirectly, we also spend a lot of time and effort trying to protect our company in different ways as part of the ordinary course of running the business. But the financial system is interconnected, and adversaries are smart and relentless – so we must continue to be vigilant. The good news is that the industry (plus many other industries), along with the full power of the federal government, is increasingly being mobilized to combat this threat..."

Jamie Dimon, CEO, JPMorgan Chase

Source : https://www.jpmorganchase.com/corporate/investor-relations/annual-report-proxy.htm

Telecom Sector

Given that telecom companies control critical infrastructure, the impact of an attack can be very high and far-reaching. In fact, even the false claim of an attack can force a telecom company to shut down critical services that consumers and businesses rely on the cyber risk in telecom sector is assuming higher proportion. With 5G technologies coming in, the older IP based cyber risk management technologies are getting outdated. The main threats impacting the sector will by Data protection, Privacy, Cloud, Internet of Things, Supply Chain, Signalling, etc.

Shipping

With shipping industry relying heavily on IT systems, in communication, navigation, loading / unloading of vessels, container tracking / cargo handling, inventories management, and the computer systems used mainland and at major ports, make it more susceptible to cyber-attacks. Smooth running of these systems is essential to the successful operation of the vessel and therefore economically important not only to the vessel/cargo owner but also to other vessels. The importance of safeguarding against cyber risks in the maritime industry has been widely recognized. In 2017, the International Maritime Organization (the "IMO") published concise Guidelines for maritime cyber risk management which are suitable for a variety of different organizations. Further to, and in support of, their guidelines, the IMO has also given ship owners a deadline of 1 January 2021 to incorporate cyber risk management into a vessel's SMS Code Safety Management.

Supply Chain and Logistics

Supply chain and Logistics companies may often overlook one important aspect that is becoming a crucial part of the industry – cybersecurity. The consequences of cyberattacks in logistics can be damaging to multiple supply chains. It can result in data hostage for ransom, or malware that can immediately destroy information, or break the supply chain and end up on money loss. Although it's impossible to provide a hundred percent protection against digital threats. Supply chain and Logistics companies are raising their state of cybersecurity by taking steps in developing high-quality risk management.

Logistics

Meeting venue:

Cairo Marriott Hotel (Hall room "Aida Ballroom") - 16 Saray El, Gezira St, Cairo Governorate 11211, Egypt

Estimated start time:	Estimated end time:
8:30 am on Wednesday, 18 December 2019	3:00 pm on Wednesday, 18 December 2019

Costs:

KPMG Hazem Hassan covers the full cost of the workshop. Accordingly, there is no workshop attendance fee.

Cyber Security and Risk Management Summit

18 December 2019 - Cairo Marriot Hotel

Key Presenters:

Akhilesh Tuteja

Global Cyber Security practice Co-leader and Partner, KPMG

Akhilesh serves as the Global Cyber Security practice Co-leader and heads the IT Advisory practice for KPMG the Europe Middle East and Africa (EMA) region and India.

Akhilesh is passionate about developments in the area of information technology and how these can help businesses drive smart processes and effective outcomes. He has advised over 200 clients on matters relating to cyber security, IT strategy, and selection of technologies and helped them realize the business benefits of technology. He possesses good knowledge of behavior psychology and is enthusiastic about addressing the issues of IT risk in a holistic manner, especially through application of user behavior analytics.

In the industry, Akhilesh has played an instrumental role and is widely recognized for his strong blend of business and technical skills. Combined with his positioning as an independent expert, he has been a member of jury for a number of awards over the last few years. Akhilesh is a frequent contributor to business and technology publications. He is a notable speaker on cyber security and its implication to enterprise businesses.

Akhilesh is also a member of the steering committee of Data Security Council of India (DSCI), which is a self-regulatory organization. He has also played an active part in developing security and privacy frameworks for the banking industry in India.

Chandra Prakash Suryawanshi

Cyber Security expert, Partner, KPMG

Chandra Prakash comes with over 20 years of experience in Cyber Security domain with significant experience in Data Protection, IT GRC, SOC Deployments, Security assessments and Security Program Management. Chandra Prakash has executed several complex cyber security consulting and implementation projects for Banks, Telecommunication and Technology firms worldwide. Some of his significant experience comes from overseas projects in the US, UK, Germany, Saudi Arabia and India

Chandra Prakash has been an invitation speaker in various cyber security conferences like DSCI, CSO Forum, MIS (UK) and GISEC (Dubai).

Chandra Prakash's domain of specialization are Next Generation SOC comprising of SIEM, IR Automation, EDR, Threat Hunting and UEBA as well as Cyber Security Strategy Consulting with IT GRC, IAM and Data Protection.

At KPMG, our global network of business-savvy cyber security member firm professionals understands that businesses cannot be held back by cyber risk. KPMG professionals recognize that cyber security is about risk management – not risk elimination. No matter where you are on the cyber security journey, KPMG can help you reach the destination: a place of confidence that you can operate without crippling disruption from a cyber security event. Working shoulder-to-shoulder with you, KPMG member firm professionals can help you work through strategy and governance, organizational transformation, cyber defense and cyber response. And cyber security professionals don't just recommend solutions — they also help implement them. From penetration testing and privacy strategy to access management and cultural change, KPMG can help you every step of the way.