ANTI-HACK
Cybersecurity essentials for senior managers

Overview

Middle East leaders rank digital adoption and cybersecurity among the top challenges facing businesses today*. The two are inextricably linked. The digital age is saturated with opportunity, but it is also fraught with risk.

Cyber-attacks are growing in number and complexity. Hackers are no longer just criminals – they include foreign governments, terrorists and rival corporations. How should leaders prepare for this new ‘normal’?

Anti-hack serves to address the growing threat of cybercrime in the digital age. It recognizes that cybersecurity begins with awareness and intent at a board and C-suite level and teaches the security fundamentals of effective cyber risk management.

The question is no longer, “Will I be attacked?” You will. The real question is, will you be ready?

Program takeaways - Key benefits and topics

The purpose of Anti-hack is not to provide solutions to participants’ specific cybersecurity challenges. Rather, it will enable participants to identify critical issues so that they can lead the development of better cybersecurity initiatives.

Anti-hack participants will walk away with:

• A deep understanding of why cybersecurity is crucial to all organizations today.
• A systemic approach to effective investment in cybersecurity.
• A roadmap of the various phases of cybersecurity management, including why these phases are relevant and the risks associated with poor implementation.
• Fluency in the most common terms used in cybersecurity.
• Exposure to the biggest and most common cyber threats.
• Well-debated viewpoints around the best cyber strategies for their business.
• The tools needed to make better management decisions in all aspects related to cybersecurity.

The program concludes with a practical cyber crisis management workshop delivering

• Dynamic role-play methodologies
• Crisis management best practices
• Rehearsal of new competencies acquired
• Cyber response protocols applied in a coordinated manner in a realistic business case based on real incidents.

* View Headspring’s research report here: https://go.headspringexecutive.com/pulsemiddleeast

PROGRAM DETAILS:
Date: 29th Nov to 2nd Dec, 2020
Time: 8am - 3pm (breaks included)
Location: Kuwait Radisson Blu Hotel
Registration deadline: Oct 29, 2020

PARTICIPANT PROFILE:
• Must be employed only by a private company in Kuwait.
• Provide an updated C.V. reflecting current role and responsibilities
• Minimum 4 years of work experience and English proficiency.

APPLY NOW:
To register for this program, please go to: www.kfas.org/cybersecurity
WHO SHOULD ATTEND - IS THIS RIGHT FOR ME?

All those responsible for the management or implementation of cyber strategies in their business, including:

- Operations Manager
- IT Manager
- Technology Manager
- Security Manager
- Cybersecurity Manager
- Risk Manager
- Compliance Manager
- Internal Auditor
- Risk Manager
- Compliance Manager
- Internal Auditor

SELECTION PROCESS

All applicants will undergo a blind-review process by a selection committee. Applicants will be assessed based on experience, area of expertise, and merit. Any late or incomplete submissions will be automatically disqualified.

So, we would recommend:

2+ years in a management position related to business operations if they work for any organization or they lead their own.

CONTACT KFAS:

Enterprise Learning & Human Development
E-mail: training@kfas.org.kw
Tel: +965 22278100

Ander Ortiz
Senior risk management professional with more than 15 years of experience in managing and preventing operational, technology and cyber risks and enabling secure digital transformation and performance for international clients. He also leverages his client-centric background to train executive audiences in universities and business schools.

Gianluca D’Antonio
Academic Director of the masters program in Cybersecurity at IE School of Human Science And Technology. Partner at Deloitte Spain, he leads the practice in cybersecurity to drive organizations through a safe digital journey. Independent Advisor for Spanish National Cybersecurity Strategy review. Former Member of the PSG at European Network and Information Security Agency (ENISA) 2010-2015