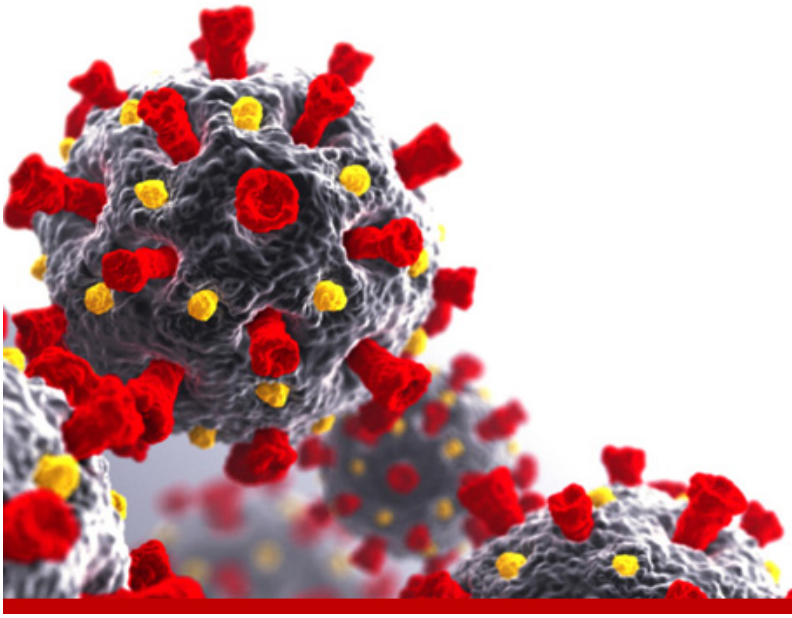
VALOORES

Business Academy



Cyber-COVID

in Times of Financial Crimes, and Cybersecurity

With International Regulators…

VALOORES

Upcoming Webinar

May 28th 2020, 13:00 GMT

BACKGROUND

A third of the world's population is in coronavirus lockdown. An estimated 300 million office workers globally may be working from home, including up to 90% of banking and insurance workers. Most of these staff log into their firms' sites remotely, attending meetings using teleworking arrangements, and/or accessing non-public data online - sometimes via home computers and private devices. Since the customers of most financial institutions are also staying at home, doing financial transactions online has become not just a convenience but a necessity.

The lockdown increases the scope for criminals to exploit vulnerabilities and commit financial crime. The increased online presence of virtually everyone has led to new, and in some cases more naïve, targets for online fraudsters. Work-from-home arrangements with remote access to corporate networks have significantly expanded the attack surface for cyber criminals. Money launderers can also take advantage of the increased need for financial institutions to identify and onboard their customers online. In normal times, cyber-attacks and AML violations expose financial institutions to significant operational and reputational risks. In exceptional circumstances like the current one, those risks could be further exacerbated.

This webinar outlines official responses to the increasing levels of financial crime during the global lockdown. It highlights Financial Crime and Risk Management, seen so far, during the current crisis.

On the other hand, COVID-19 is reshaping the Cyber-Crime Economy.

We'll discuss how Cyber-criminal merchants are going All in and seeking more exposure; we'll see how the demand for ransomware is on the rise, we'll touch upon new and emerging risk issues for financial crime linked to the COVID-19 pandemic, and we'll address the issues and recommendations for collective action in combatting illicit financial flows during the COVID-19 pandemic, and beyond.

OBJECTIVES

- **What COVID-19 changed, Before, During & Beyond… in the Financial Industry?**
  Collective Action in Combatting Illicit Financial Flows
- **Raising Cyber Crime Awareness… by Financial Authorities**
  Cyber Crime Awareness on Increasing Levels of Cyber Crime
- **Is IFRS 9 / CECL impact the same During & Beyond COVID-19, & What is the Alternative?**
  Assessment Adjustment & Scenario Analysis in this Uncertain Environment
- **What is the COVID-19 Impact on AML/CFT Regimes & Obligations?**
  Impact on Government and Private sectors' AML/CFT Obligations
- **How COVID could impact our Near Future on AML/CFT Measures & Guidance?**
  AML Measures with FATF & Other Authorities' Guidance
- **How are Cybercriminals Taking Advantage of the COVID-19 Pandemic?**
  Criminals Exploit WFH, Unemployment, Uncertainty, & Play on Fears

WHO SHOULD ATTEND THIS WEBINAR

- Chief Compliance officers and Managers
- Chief Technology Officers and IT Managers
- Chief Risk Officers and Managers
- Information Security Officers
- IT Auditors

TOPIC AND AGENDA

Duration: 40 minutes and 10 minutes for QAs

Topic: Cyber-COVID in times of Financial Crimes and Cybersecurity with International Regulators

Agenda:

- Collective Action in Combatting Illicit Financial Flows
- Cyber Crime Awareness on Increasing Levels of Cyber Crime
- Assessment Adjustment & Scenario Analysis in this Uncertain Environment
- Impact on Government and Private sectors' AML/CFT obligations
- AML Measures with FATF & Other Authorities' Guidance
- Criminals Exploit WFH & Unemployment Uncertainty & Play on Fears

You will receive the Material along with the Recorded Webinar on your Email address

For more information kindly send your questions on:

academy@valoores.com