E-LEARNING COURSE

on Cyber Security in the Financial Services Sector

MEFMI
Macroeconomic and Financial Management Institute of Eastern and Southern Africa

Banks and the entire financial services sector have become a key target for cyber criminals because of the potential for high illicit proceeds. The criminals have become organised and sophisticated enough to threaten entire systems of individual firms and critical parts of the financial sector infrastructure. Businesses must, therefore, secure their networks from increasingly aggressive hackers, who have shown they are capable of shutting down critical infrastructure and crippling corporate and government networks.

Profile of the Facilitator

Dr. Richard Young is a seasoned risk executive with extensive hands-on expertise for establishing and maintaining the enterprise strategy to ensure information assets are adequately protected; shape and drive strategy work for the implementation of new technologies and promoting digital transformation through the delivery of business application modernization strategies across client application portfolios. Dr. Young has led various exercises of formulating new Information, Technology and Business Resiliency Risk enterprise-wide policies, standards procedures and the risk appetite statement and framework. He co-programme managed a multi-million dollar new Citibank-wide programme (Secure File Transfer Protocol) – a solution which improved the secure electronic data transfer of data within Citibank and its partners. Some of his qualifications include Ph.D in the Management of Information Systems and Leadership (University of Phoenix), MSc. Enterprise Risk Management (John Hopkins University), MSc. Cybersecurity (New York University – School of Engineering). Dr. Young has over 20 years' experience of training in Cyber Risk, Leadership, customer excellence & product development, just to mention a few.

Course Objectives

The objective of the course is to impart practical skills to participants on mitigating cyber financial crimes. Participants will also learn techniques for judicially valid and admissible investigations as well as evidence gathering from computers or networks. The Federal Bureau Investigation (FBI) report of April 2020 indicates there has been a spike in cyber crime since the onset of the coronavirus (COVID-19) pandemic as businesses and individuals are increasingly using the internet to transact.

Who Should Participate?

All firms who are keen to better understand how to mitigate risks from cyber financial crimes and be able to have a detection plan in place with a synchronised reporting structure need to attend. The workshop is aimed at senior and middle level professionals from ***Internal Audit, Risk Management, Security, Legal, Regulatory Compliance, Operations and Finance.***

Course Overview

The course will comprise presentations, audio visual material, case studies, online group discussions including practical quizzes. At the end of the workshop, participants will:

1. Understand the impact of cybercrime and how it threatens the financial services industry.
2. Be aware of how IT, physical and socially engineered methods are used to commit or facilitate cybercrime.
3. Gain a familiarity with the major fraud typologies used by cyber criminals.
4. Master the key security methods used to prevent cybercrime and how they can be made to be more effective
5. Recognize and react to the warning signs of Cyber financial crime.
6. Define the role of ethics in financial fraud prevention.
7. Identify and implement anti-fraud measures and manage fraud risks.
8. Learn to investigate and form a legal case to prosecute suspected fraudsters.

Date	28 September 2020
Language	The course will be delivered in English
Deadline for Registration	21 September 2020

www.mefmi.org

FEE US$500 per Delegate

Local participants can pay in ZWL equivalent at the prevailing auction rate.

For further details and registration contact

Sharon.Wallett@mefmi.org Twitter: @mefmiorg Website: www.mefmi.org