



# MEFMI

Macroeconomic and Financial Management  
Institute of Eastern and Southern Africa

Cyber  
security

cyber  
crime

## CYBER FINANCIAL SECURITY

Banks and the entire financial services sector have become a key target for cyber criminals because of the potential for profits. 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.

### WORKSHOP OBJECTIVES

This workshop unpacks the cyber threat landscape and the types of cybercrimes which are currently victimizing both financial institutions and their customers. Participants will learn detection, investigation, reporting and prevention techniques, as well as appropriate risk management tools and techniques for judicially valid and admissible investigations.

### WHO SHOULD ATTEND?

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**.

### WORKSHOP OVERVIEW

The course will comprise approximately 32 hours of sessions/slides presentations, audio visual material, case studies, small group discussions including practical exercises and instrument demonstrations. A memory stick, containing the presentations and other information will be distributed during the course. There will be group exercises and team presentations for practical orientation. 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.

**FEE: USD850**  
**Early Bird: USD800**

Venue: Lusaka, Zambia

Dates: 6 – 10 May 2019

Language: The course will be delivered in English

Deadline for Registration: 26 April 2019

For further details and registration contact [Sharon.Wallett@mefmi.org](mailto:Sharon.Wallett@mefmi.org)

Twitter: @mefmiorg

Website: [www.mefmi.org](http://www.mefmi.org)



## REGISTRATION FORM

**Deadline for registration: Friday 26 April 2019**

**COURSE: CYBER FINANCIAL SECURITY**

**DATE**

**6 – 10 May 2019**

**VENUE**

**Lusaka, ZAMBIA**

### DELEGATE DETAILS

<b>Surname</b>	<input type="text"/>	<b>Forenames</b>	<input type="text"/>
<b>Gender</b>	<input type="text"/>	<b>Country</b>	<input type="text"/>
<b>Job Title/Position</b>	<input type="text"/>	<b>Organisation</b>	<input type="text"/>
<b>Physical Address</b>	<input type="text"/>		
<b>Mobile:</b>	<input type="text"/>	<b>Email</b>	<input type="text"/>
		<b>Signature</b>	<input type="text"/>

### SPONSOR:

<b>Name</b>	<input type="text"/>	<b>Signature</b>	<input type="text"/>
<b>Organisation</b>	<input type="text"/>	<b>Position</b>	<input type="text"/>
<b>Address</b>	<input type="text"/>		
<b>Mobile</b>	<input type="text"/>	<b>Email</b>	<input type="text"/>
		<b>Date</b>	<input type="text"/> <input type="text"/> <input type="text"/> 2019
		DD:	MM:

**THIS BOOKING IS INVALID WITHOUT A SIGNATURE**

**REGISTRATION FEES: USD850 (Eight Hundred & Fifty Dollars)** per person (for conferencing and workshop materials only).  
**Early bird Fee of USD800** if payment is received by **26 April 2019**.

**Payments by Telegraphic or Direct Bank Transfer Only into the following banking account details:**

Bank:	Stanbic Bank Zimbabwe	Account Name:	MEFMI Business Development Unit
Account Number:	9140001013083 (Nostro Account)	Swift Code:	SBICZWHX
Branch Name:	Minerva		

### TERMS & CONDITIONS

**Payment Terms:** Payment must be completed seven (7) days before the event. Admission to the event is dependent on proof of full payment.

**Cancellations:** All cancellations or postponements must be confirmed in writing and e-mailed to [Sharon.Wallett@mefmi.org](mailto:Sharon.Wallett@mefmi.org) or [tafadzwa.choto@mefmi.org](mailto:tafadzwa.choto@mefmi.org). Cancellations five (5) to ten (10) business days prior to the event will attract a 25% cancellation fee. Cancellations received less than five (5) business days prior to the event will result in a 50% cancellation fee. No shows will attract a 100% cancellation fee. Delegates are however welcome to substitute attendance with an appropriately qualified colleague. Non-attendance without notification is treated as cancellation with no entitlement to any refund or credit.

**GENERAL NOTES:** In the event of unforeseen circumstances, MEFMI reserves the right to change the speakers, the venue or the date. Delegates will be notified of changes or cancellations of events no later than five (5) business days prior to the event and all paid-up invoices will be fully refunded in a case of cancellation or credited to another event within six (6) months. MEFMI is absolved from and indemnified against any loss or damage as a result of any cancellation, postponement, substitution or alteration arising from any cause whatsoever.

**Upon completion send to: 9 Earls Road, Alexandra Park, Harare, Zimbabwe or**  
Email: [Sharon.Wallett@mefmi.org](mailto:Sharon.Wallett@mefmi.org)