



**CYBER  
CRIME**  
Prevention Workshop 2011



**Combating Cyber crime and illegal innovation:** *How to deter and detect cyber crime and defend personal, corporate and public information assets from cyber criminals and malicious insiders -30-31 March 2011, Addis Ababa, Ethiopia*

**Overview of the workshop**

**A crime epidemic is silently sweeping the globe as criminals turn our ever-increasing dependence on computers against us.**

Considering the anonymity of cyberspace, it may in fact be one of the most dangerous criminal threats we will ever face. Almost two thirds of all adult web users globally have fallen victim to some sort of cyber crime, from spam email scams to having their credit card details stolen. It is no longer just high school kids in their bedrooms sending out malicious emails, It's organised criminals. They carry out silent, hit-and-run attacks.

In recent years, the internet has considerably facilitated communication and promoted global development and interaction. At the same time, new, modern challenges have emerged in the form of cyber crime as organized criminal groups exploit these technological advances. A Wikileaks phenomenon regarded as the most vicious insider malicious attack brings the need for developing robust data loss prevention strategies in organisations.

The growth in popularity of social networks and cloud computing – internet-based computing where resources, software and data are stored and shared online – enables remote access to data from any location and therefore makes data vulnerable to external attacks. This raises concerns about whether security measures will be properly enforced by the storage provider, or understood by the data owner or customer. The key to the success of cloud computing regarded as one of the most significant shift in information technology will be whether the convenience of remote access will be matched by confidence in its security provisions. This workshop will address crucial current information security and cyber crime issues in the world.

**Objectives of the workshop**

The 2011 Combating Cyber crime Workshop will give you the essential tools you need to detect, deter, and defeat the cyber criminals that are after your organisation's assets!

Learn about the latest practices, trends, technologies and techniques used by today's most sophisticated cyber criminals. And gain practical knowledge to help your organization protect itself – and your customers – against a growing epidemic of corporate account hijacking, data leakage, insider threat, social network attack, Wikileaks saga, cloud crime

<p>Get opportunities to dialogue in order to develop unified, speedy and effective solutions to cyber crime challenges in your organisation</p>	<p>Cyber crime threats and methods targeting organisations are increasing faster than many organisations can combat them</p>
---	--

www.sacifs.co.za

In Association with StarCom Network Solutions Plc Ethiopia

SOUTH AFRICAN CENTRE FOR INFORMATION SECURITY  
**CYBER CRIME CONFERENCE 2011**  
 MARCH 30-31, 2011 | ADDIS ABABA, ETHIOPIA





## Highlights of the workshop

The workshop will concentrate on key current crucial threats and areas:

1. Current cyber crime business models, trends, intrusion and attacks
2. Cyber crime and Wikileaks phenomena
3. Cyber crime against Cloud computing
4. Malicious insiders' as vicious cyber criminal
5. Social networking as playground of cyber criminals
6. The growing threat of cyber espionage targeting nations' and companies trade secrets.
7. Legislative and jurisdiction challenges of cyber crime in Ethiopia

This workshop empowers you to deploy more effective (risk based) security solutions than current traditional security models (traditional 'wall-and-fortress' approaches) that are only minimally effective against cyber criminals.

The biggest problem, and the criminal's greatest advantage, is complacency, absence and enforcement of risk mitigation strategies and lack of knowledge of cyber crimes and cyber criminals.

Organisations learn about most costly or damaging attacks caused by insiders (employees or contractors with authorized access) in various environments.

## Detailed objectives

The workshop will enable delegates to:

- **Focus** on the new developments and threats in the field of High-Tech and Cyber crime.
- **Exchange** good practices related to combating Cyber crime.
- **Understand** the impact of cyber crime on business and individuals
- **Learn** trends developments and business models of cyber crime
- **Understand** and use the latest preventative measures that constitute best practice in combating cyber crime
- **Strengthen** the knowledge and application of combating cyber crime techniques
- **Learn** best practices of combating cyber crime from different parts of the world.
- **Strengthen** networking and active participation in combating cyber crime.
- **Develop** strategies and a blueprint of action for combating various types of cyber crimes
- **Learn** crucial strategies and practices to prevent data loss
- **Develop** techniques, best practices and strategies to defend your valuable information assets.
- **Influence** leaders, including key policy makers and executives, to increase their commitment to combat cyber crime

**Intended for:**

CEOs, CIOs, CISOs, Business Owners, Managing Directors, IT Managers, Diplomats, Office Staff, Online Traders, Online Buyers, Manufacturers, Lawyers, Magistrates, Computer users, Government officials, Police officers, Diplomats, Intelligence Analysts, Senior military officers, IT lecturers, Cyber Crime Investigators.



In Association with StarCom Network Solutions Plc Ethiopia

SOUTH AFRICAN CENTRE FOR INFORMATION SECURITY

# CYBER CRIME CONFERENCE 2011

MARCH 30-31, 2011 | ADDIS ABABA, ETHIOPIA





# CYBER CRIME

Prevention Workshop 2011

## WORKSHOP AGENDA Day 1



### Registration: 7:30 – 8:15

### Session 1 8:30 – 10:20

#### Current trends and development of cyber crime, intrusions, attacks

- o The underground economy of cyber crime
- o cyber crime digital ecosystem
- o Cyber crime Return on Investment analysis
- o Global distribution of cyber crime
- o The cyber crime value chain
- o Capabilities and specialisation of cyber criminals
- o Cyber crime business models
- o Why South Africa is becoming a cyber crime hub
- o Top emerging cyber crime threats –
  - o Recommendations to defend your information and organization from cyber crooks.

#### Case studies

### Session 2 10:30 – 12:30

#### Insider threats : Cyber criminals' weapon of choice and the biggest threat to information security

- o Understanding the risk and defending the enterprise
- o Why insider threat is government's and industry's greatest concern
- o Key internal threats exploited by cyber criminals
- o Insider threat behind Wikileaks cyber security saga
- o Serious data loss breaches by insiders
- o Motivation for malicious insiders

It is crucial for organisations to empower themselves with knowledge of current trends, developments and tools of combating cyber crime.

- o Strategies to secure confidential data from internal theft.
- o Risk Mitigation Models:
- o Lessons Learned from Actual Insider Attacks
- o Predictive Modeling and other solutions for insider threat Mitigation

#### Case studies: Global and South African cases of malicious insiders' attacks

### Session 3 2:00 – 3:00

#### Wikileaks phenomena – Can it be the perfect cyber crime model?

- o Anatomy and overview of Wikileaks
- o Will Wikileaks hurt your business and government?
- o Wikileaks attack on corporate information assets
- o Mitigating corporate data theft
- o Lesson for government and business from Wikileaks
- o Keeping Your Organization Safe from the Wikileaks phenomenon through data loss prevention strategies and practices.

#### Case studies : Wikileaks phenomena and the rise of cyber war

### Session 4 3:30 – 4:30

#### e-Espionage gone cyber – Cyber criminals go after your Data.

- o E-espionage: Growing dimension of cyber crime and a growing threat to all businesses
- o Current trends and development in cyber espionage- secret data theft
- o How big is the threat?
- o Assessing the e-Espionage risk
- o Theft of computerized information
- o Fighting the threat: next steps for companies and government
- o Steps to protect your data from Cyber Espionage
- o **Case study - eEspionage at Renault in France and Chinese cyber attack on Germany's secret commerce data**

www.sacfis.co.za

In Association with StarCom Network Solutions Plc Ethiopia

SOUTH AFRICAN CENTRE FOR INFORMATION SECURITY

# CYBER CRIME CONFERENCE 2011

MARCH 30-31, 2011 | ADDIS ABABA, ETHIOPIA





## WORKSHOP AGENDA Day 2

### Session 5 8:30 – 10:15

#### Cyber crime legislative framework, legal aspects and jurisdiction issues of cyber crime in Ethiopia

- South African banking sector and cyber crime
- Lesson from the banking sector
- Guidance in public-private sector collaboration in combating cyber crime.
- Challenges in cyber crime investigation
- Case studies – Lesson for Ethiopia

### 10:15 – Tea Break - Networking

### Session 6 10:30 – 12:30

#### Cloud computing – is it a super highway for cyber crime?

#### Cloud computing Security challenges and solutions for users & vendors

- Security – Cloud Crime is no 1 inhibitor to cloud adoptions
- Cloud computing overview- delivery and deployment models
- Current top threats to cloud computing
- Security threats from cloud
- Cyber crime goes cloud – ccas,cfas
- Security benefits of cloud computing
- Risks and vulnerabilities in cloud-legal, technical, organizational
- Information assurance framework for cloud computing
- Industry best practices for securely adopting cloud computing

**Learn** crucial strategies and practices to prevent data loss



#### Dates and time

March 30-31 2011  
8:00 am to 4:30 pm

**Venue:** Kaleb Hotel- Addis Ababa

#### Fees : Birr 3500.00 per delegate

Contact - StarCom Network Solutions Plc

Addis Ababa – Ethiopia

Tel (011) 4-669 642 -

Email: info@sacifs.co.za

#### Registration

Please register early to ensure a place - fax registration form to (011) 4-669 643.

- Developing cloud security strategy and reducing data breaches
- Cloud security organisations and standards – CSA, Jericho,DMTF
  - Key security guidance for cloud computing

#### Case studies : analysis of your cloud security posture.

### Session 7 2:00 – 3:15

#### Web 2.0 social networking – Hotbed of malicious attacks and new playground of cyber criminals

*“Social media connections will eventually replace email as the primary vector for distributing malicious code and links*

- Power of social media for business
- How social networks empower cyber criminals
- Social networks for researching and breaching targets spear-phishing" exploits
- Strategies to mitigate security risks of using social networks
- Tools and tricks of cyber criminals in social networks
- Guidance for secure utilization of social networks in enterprise

### Session 8 03:30 – 4:15

#### Panel discussion

- Wikileaks – for vs. against.
- Social media for business for vs against
- Go cloud vs cloud is a no go zone?

### Session 9 4:15 – 4:30

- Final panel and closure

**Develop techniques, best practices and strategies to defend your valuable information assets.**

In Association with StarCom Network Solutions Plc Ethiopia

SOUTH AFRICAN CENTRE FOR INFORMATION SECURITY

**CYBER CRIME  
CONFERENCE 2011**

MARCH 30-31, 2011 | ADDIS ABABA, ETHIOPIA





## Facilitator profile

### Mr. Beza Belayneh

Chief Information Security Architect and Founder – South African Centre for Information Security.  
Centre for Information Security Botswana.

**Beza Belayneh** is a high level information security, cyber crime and assurance Consultant, researcher and speaker. He uniquely and effectively combines the expert knowledge of information security and its effective implementation in defending critical information assets in business and government. He helped many organisations to realize the risk their information is facing and establish various information security policies and strategies to defend their information assets.

He has carried out extensive researches and delivered solutions and papers at high level international workshops and seminars on areas such as: PKI, DLP, cyber crime, information warfare, information security governance, malicious insider threat, information security awareness strategies, security policy development and web application security for wide range of clients and sectors.

Regionally well known speaker, trainer, consultant, and writer, Beza has presented his hands-on INFOSEC related programs, seminars and workshops at all levels of management in Botswana, Lesotho, Swaziland, Namibia, South Africa, Kenya, Ethiopia, Kuwait and Belgium for wide range of clients and forums for over a decade.

Beza has recently developed and presented an “offensive information warfare model – Lesson from Shaka Zulu” at the 2<sup>nd</sup> Kuwait Information Security Summit in Kuwait City. He had also developed a unique model to mitigate the rising insider threats to information and information systems

Beza has managed information security compliance requirements for wide range of clients in multi sectors and implemented various institutions' information security programs at corporate and business unit level and developed robust information security governance and awareness training programs.

Beza is sought-after speaker and works with a team of information security experts and practitioners in South Africa and Botswana. Beza is a seasoned presenter and is recognised as a leading professional in the field of information security and is currently the CISA and Founder of information security and assurance consultancy and research firm, South African Centre for Information Security.

www.sacifs.co.za



In Association with StarCom Network Solutions Plc Ethiopia

SOUTH AFRICAN CENTRE FOR INFORMATION SECURITY



# CYBER CRIME CONFERENCE 2011

MARCH 30-31, 2011 | ADDIS ABABA, ETHIOPIA

