



## The High Cost of Malicious Exploitation of Information Systems by Insiders: Analysis, Detection and Prevention of the Rise of the Insider Threat

With Beza Belayneh – Founder & CEO - South African Centre for Information Security

### Overview and Rationale

During the past decades, information security developments have been mainly concerned with preventing illegal attacks by outsiders, such as hacking, virus propagation, and spyware. According to a recent Gartner Research Report, information leakage caused by insiders who are legally authorized to have access to some corporate information is increasing dramatically.

As enterprise defenses evolve, so too do the attack vectors leveraged by those seeking to bypass such controls. We are entering an era where attackers are no longer working to punch a hole in the fortress surrounding enterprise IT assets from the outside. They don't need to; they're already inside.

Protecting sensitive information from unauthorized manipulation and disclosure by its insiders has become a major concern for organizations worldwide. Current and former employees, experts, contractors and other insiders pose a substantial threat due to their knowledge and authorized access to corporate and government internal systems and data.

The insider threat is often characterized as an employee performing malicious behavior—through sabotage, stealing data or physical devices, or purposely leaking confidential information. Organizations need to be aware that the insider threat is not just the rogue employee, but rather every employee and every device that stores information.

Insider IT sabotage and espionage share many contributing and facilitating system dynamics features. It follows that they might be detected and deterred by the same or similar administrative and technical safeguards.

Insider threat has currently rated as one of the most crucial information security issues and cited as the most serious security problem that comes in the form of fraud, theft of information and IT sabotage in many studies.

It is also considered the most difficult problem to deal with, because an "insider" has information and capabilities not known to other external attackers.

Identifying an individual who is misusing the data and is allowed to access is much more complicated than detecting or blocking access of an unauthorized external person.

### Challenges

Even as tools and technologies are being improved to protect critical national and enterprise IT infrastructures against external attack, malicious insiders, intent on damaging an organization or turning a profit, remain a pervasive and challenging problem.

In an insider attack, the attacker uses legitimate rights and privileges to inappropriate ends. Such attacks are difficult to detect and defend against.

Insider crimes are among the biggest threats to public and private sector organizations. And yet too many organizations continue to struggle to prevent or even detect these crimes.

Although the problem of insider misuse of IT systems is frequently recognized in the results of computer security surveys, it is less widely accounted for in organizational security practices and available countermeasures.





## Objectives:

- Help staff, management, and human resource personnel understand the social-behavioral factors and technical issues underlying insider threats.
- Help delegates to explore answers to key questions and challenges in preventing the rise of insider threat and their implications for the future of organizational security and national strategic infrastructure in a globally interconnected world.
- Present delegates practical strategies for effectively implementing those tools to detect illicit insider activity
- Help delegates to design and develop a proof of concept model, system and procedures for early indication and warning of malicious insiders.

## Areas you will cover:

- The nature and scale of insider threats
- Indicators/Categories of insider's threats/attacks
- Internal risk assessment models/framework
- Motivations of malicious insiders - sabotage vs. espionage
- Classifications of misusers by reason
- Insider threat scenarios, attack vectors and controls
- Lesson from notable global cases of insider malicious incidents e.g- Societe Generale insider fraud
- Best practices and strategies for the prevention and detection of insider threats
- Human Factors and Organizational Culture, and why they make a difference
- The role of security awareness
- Traditional security management tools to mitigate insider's threat
- -IAM (Identity & Access Management) in mitigating insider threats

Most insider attacks are under-reported to law enforcement agencies or prosecutors. Companies may fear the negative publicity or increased liability that may arise as a result of the incidents. In most cases, by the time the violations are uncovered, the damage is already done. Organizations must build capacity to detect, mitigate and prevent the ever increasing insider threat to their organizations' valuable assets.

## Dates and time

Tuesday, 8 June 2010  
8:00 am to 4:30 pm

## Venue

Kaleb Hotel- Addis Ababa

## Fees

Birr 1100.00  
includes all course materials and catering

## Further Information

Contact - StarCom Network Solutions Plc

✉ info@sacfis.co.za

☎ (011) 4-669 642 - Addis Ababa

📠 (011) 4-669 643

🌐 www.sacfis.co.za

## Registration

Please register early to ensure a place - fax registration form overleaf to (011) 4-669 643. If minimum numbers are not reached by June 1 this event may not proceed.

## Presenter

Beza Belayneh is a well known and experienced speaker and information security professional. Beza has over 15 years of experience in the field of IT and security, with specific emphasis on information security management, eCrime prevention initiatives, IT governance, risk and compliance (GRC) and IT security governance. As a frequent speaker at multiple industry events in various countries, he frequently developed solutions and spoke on subjects of E-crime, PKA, social engineering, insider threat and information warfare as applied in commerce & public infrastructure.

Beza has recently developed and presented offensive information warfare framework and threat modeling at the IT Web Security Summit in Johannesburg, Nairobi and Kuwait. He was instrumental in developing and implementing strategic information security solutions to wide range of clients in Southern Africa.

Beza, prior to SACfIS, worked at IDM, Botswana based Regional consulting firm as Senior IT Consultant and Heading of IT Projects for 10 years. He currently provides strategic guidance to SACfIS, an information security consulting firm that he co-founded to provide information security consultancy and research in the SADC region.

View his profile at [www.bezaspeaks.com](http://www.bezaspeaks.com)





# REGISTRATION FORM

The High Cost of Malicious Exploitation of Information Systems by Insiders:  
Analysis, Detection and Prevention of the Rise of the Insider Threat

4 August 2010, Kaleb Hotel, Addis Ababa

Complete the following and fax to StarCom Network Solutions – Addis Ababa at (011) 4-669 643

First Name:		Last name:	
Position title:			
Organisation:			
Work address:			
Email:			
Telephone:			
Cell Phone:		Fax:	
Special Requirements: (wheelchair access, dietary, etc)			

INVOICE

For attention:	As above <input type="checkbox"/> or Name:
----------------	--

Booking confirmation:

Starcom will e-mail you a booking confirmation advice within 3 working days of receiving your registration form.  
Please phone StarCom on (011) 4-669642 if you do not receive this e-mail confirmation.