



Information Security Governance for Executives: Mitigating the emerging cybercrime threat to information

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

Overview and Rationale

Until recently, the focus of security had been on protecting the IT systems that process and store the vast majority of information, rather than on the information itself.

However, this approach is too narrow to accomplish the level of integration, process assurance and overall protection that is now required. To achieve effectiveness and sustainability in today's complex, interconnected world, information security must be addressed at the highest levels of the organization, instead of making it a technical specialty relegated to the IT department.

At a time when risks are high and consumer confidence is low, corporate boards of directors, heads of government agencies, senior executives and directors must pay enough attention to information security and cyber threats. Information Security is one of several business risks that management must address as part of its day-to-day responsibilities.

When it comes to information security, what you don't know can hurt you and your organization. Senior leaders must understand what's at risk, how information is protected and what their institutions or agencies are doing to protect their valuable information.

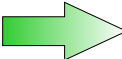
Today, in the middle of the worst economic downturn in thirty years, information security has an enormously important role to play. The rising tide of cybercrime and threats to critical information assets mandate that boards of directors and senior executives are fully engaged at the governance level to ensure the security and integrity of the information assets.

Computer assisted Crimes targeting online systems and critical infrastructure are soaring as economic difficulties deepen.

This is coupled with significant threats of information systems disruptions from insider malicious, hackers, worms, viruses and organized crime, have resulted in a need for a governance approach to information management, protecting the organizations' most critical assets—its information and reputation.

Objectives:

- Through this conference, delegates will learn that effective security requires the active involvement of executives to assess emerging threats and the organization's response to them.
- To help executives understand the current paradigm shift in Information Security space.

From  To

Scope problem:	Technical	Business problem
Ownership:	IT	Business
Costs:	Expenses	Investment
Execution:	Intermittent	Integrated, continuous
Approach:	Practice-based	Process-based
Objective:	IT Security	Business continuity/resilience

What is at risk?

- Trust- public and stakeholders
- Competitive advantage; market & investor confidence
- Ethics and duty of care
- Relationships with business partners
- Customer retention & growth
- Business continuity & resilience
- Ability to offer and fulfill transactions
- Reputation, brand, image



The purpose of information security governance is to ensure that agencies are proactively implementing appropriate information security controls to support their mission in a cost-effective manner, while managing evolving information security risks.





Information Security Governance for Executives: Mitigating the emerging cybercrime threat to information.

Key learning areas

- Information Security Governance — Introduction and Overview
- The importance of information Security and Information Security Governance
- Information Security Strategic Planning – requirements and components
- Key governance roles and responsibilities
- Illustrative roles Matrix of outcomes
 - Boards of Directors/CEOs
 - Executives/ Steering Committee.
 - IT managers/Directors
- Learn what Information Security Governance delivers.
 - Strategic Alignment.
 - Risk Management
 - Resource Management
 - Performance Measurement
 - Value Delivery
- Recommendations for Successfully Implement Information Security Governance.
- How Does your Organisation Compare on Information Security Governance?
- Maturity Level Description
- Information security governance challenges and keys to success

Challenges

- Organizations continue to witness information-related crime and vandalism becoming the choice of a growing global criminal element while organizations are experiencing lack of awareness, policies and inadequate resources.
- A large portion of the task of protecting critical information resources falls squarely on the shoulders of executives and boards of directors who

To enable secure business operations, an organization must have an effective security governance strategy. The complexity and criticality of information security and its governance demand that it be elevated to the highest organizational levels. As a critical resource, information must be treated like any other asset essential to the survival and success of the organization.

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





South African Centre for
Information Security

REGISTRATION FORM

Information Security Governance for Executives: Mitigating the emerging cyber
crime threats to business and government

Tuesday, 3 August 2010

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.

Direct your enquiries on this events contact StarCom Network Solutions Plc Debre Zeit Road Baleker Tower, 7th
Floor Room No. 702 Addis Ababa, Ethiopia Tel: +251-114-669642 Fax: +251-114-669643
email: i email- daniel@sacfis.co.za for technical enquiries beza@sacfis.co.za