securityrisk solutions

Information Security Management Present and Future

By: Jona Owitti, CISA
Director, Security Risk Solutions Limited
Immediate Past Chairman, ISACA Kenya Chapter

One Step Ahead

securityrisk solutions

About SRS – www.securityrisksolutions.net - Prelude -

Security Risk Solutions Limited is a privately owned Kenyan company that was established in 2007.

The company is specialised in providing services in Information Security, Business Continuity and Computer Forensics as well as physical and operational risk advice. Serving clients is the core of our mission. We offer consistent solution delivery based on proven methodologies, leading practices and global knowledge management.

The company operates in key markets across Africa and has established regional offices to serve our clients in Nairobi (Kenya) and Kampala (Uganda). Our geographical expansion has been driven by client demand for local services. Our client portfolio runs across the telecommunications sector, financial and insurance sectors, transportation and manufacturing, and the government.

OUR VALUE TO CLIENTS
With our comprehensive portfolio of services, *Security Risk Solutions Ltd* assists with testing, design, remediation, and implementation of effective enterprise information security solutions. An expanding and very important area of our business with the growing computerisation of East Africa is:

a) ***Compliance solutions*** – many financial institutions are now required to comply with various international regulations, such as the Payment Card Industry (PCI) set of standards;

b) ***Computer Forensics and Fraud Investigations*** – East Africa has seen a massive upsurge in electronic crime;

c) ***Business Continuity and Disaster Recovery*** – organizations are now realizing that effective enterprise emergency plans are mandatory if they plan to stay in business during and after a disaster or unexpected business interruption; and

d) ***IT Security Testing and Vulnerability Assessments*** – to prove to clients that they are on the right track with protecting their own, and client's, information.

IS Management and Governance Seminar Theme

The opinions expressed here are mine (presenter) and do not necessarily represent the opinions of the employer. Use a risk-based approach before attempting this at home!

Information Security Management Agenda

- Information Security Management (ISM) – Importance
- Information Security Governance
- Co-sourcing and the Role of Managed Services
- Future of IT – InfoSec Concerns
- Conclusion – Prediction (Present ➔ Future of IT)
- Q & A

IS Management and Governance Seminar Theme

Restoring Public Trust in Institutional Governance

Information Security Management Introduction / Definition

- **Information Security Management (ISM)**
  - describes controls that an organization needs to implement to ensure that it is sensibly managing risks that relate to the protection of information and information infrastructure assets (risk of loss, disclosure or damage).
- **Information Security Governance (ISG)**
  - "is a subset of enterprise governance that provides strategic direction, ensures objectives are achieved, manages risk appropriately, uses organizational resources responsibility, and monitors the success or failure of the enterprise security programme." - ITGI

ISM – Present and Future
Quote – Information Security Governance

"Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing **strategic direction**, ensuring that **objectives are achieved**, ascertaining that **risks are managed appropriately** and verifying that the enterprise's **resources are used responsibly**."

– IT Governance Institute

ISM – Present and Future
Quote – Information Security Management

"Failure to hit the bullseye is never the fault of the target."

- Gilbert Arland

- relates to responsibility of management and wise use of their power of choice to:
  - do poorly on a security assessment
  - fail an audit
  - experience a security breach, and
  - fall out of compliance

ISM – Present and Future
Quote – Information Security Management

"When they feel the heat they'll see the light."

- Herman Cain

- relates to the lack of management support on information security initiatives year after year.
- However, once a breach occurs, suddenly finding it in them to make things happen.

ISM – Present and Future
Quote – Information Security Governance

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.

– *Terry Hancock, CEO*
Easy I Group

ISM – Present and Future
Quote – Information Security Governance

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 those resources.

— *Sirley M. Hufstedler, Board of Directors, Harman International Industries*

ISM – Present and Future
Quote – Information Security Governance

To enable secure business operations, an organization must have an effective security governance strategy.

— *Sunil Misra, Chief Security Advisor and Managing Partner*

Unysis Corp.

ISM – Present and Future
Quote – Information Security Governance

To enable secure business operations, an organization must have an effective security governance strategy.

— *Sunil Misra, Chief Security Advisor and Managing Partner*

Unysis Corp.

IS Management and Governance

Information Security Management: Importance

Seminar Theme:

Restoring Public Trust in Institutional Governance

Information Security Management

- Effective ISM critical in protecting information assets and privacy
- Profile of information and privacy risk raised by:
  - the advent of electronic trading through service providers and directly with customers;
  - the loss of organisational barriers through use of remote access facilities; and
  - high-profile security exposures – e.g. unauthorised access, disclosures and identity theft over the Internet, viruses, denial-of service (DoS) attacks, and intrusions.

15

Information Security Management

- Objectives of Information Security, include:
  - Preserve **confidentiality** of sensitive data
  - Ensure **integrity** of information
  - Ensure continued **availability** of information systems
  - Ensure compliance with applicable laws, regulations and standards

16

Information Security Management (ISM)

- Key elements of ISM
  - Senior management commitment and support
  - Policies and procedures
  - Organisation
  - Security awareness and education
  - Monitoring and compliance
  - Incident handling and response

IS Management and Governance

Information Security Governance

Seminar Theme:

Restoring Public Trust in Institutional Governance

Information Security Governance (ISG)

- Is an integral part of enterprise governance
- ISG function:
  - Provides strategic direction;
  - Ensures objectives are achieved;
  - Ensures security risks are managed appropriately;
  - Ensures organisational resources are used responsibility;
  - Monitors the success or failure of the enterprise security programme.

IS Management and Governance

Co-sourcing and the Role of Managed Services

Seminar Theme:

Restoring Public Trust in Institutional Governance

IS Management and Governance

- Co-Sourcing
  - a business practice where a service is performed by both staff from inside an organisation and also by an external service provider
- A major reason for Co-Sourcing is to increase economies of scale and realize efficiencies

IS Management and Governance

- Co-Sourcing Benefits
  - Helps to increase coverage without increasing overhead
  - Turns fixed cost into a variable cost model and headcount in the budget
  - Customer retains “high-end” competencies which helps them reduce Risk and maintain Quality control
  - Enables customers to provide Global solutions (cultures, language and coverage)
  - Reduced employment liability (partner company plays role of a managed service solution provider instead of an individual or contractor’s role usually played in other models)
  - Offers flexibility for Capacity Management - flexing of staff and alternate skills where required

IS Management and Governance

Future of IT – Information Security Concerns

Seminar Theme:

Restoring Public Trust in Institutional Governance

One Step Ahead
securityrisk solutions

IS Management and Governance
Future of IT – Information Security Concerns

- Big Issues
  - People
    - Skills and experience
    - Executive detachment
    - Who "owns" data
  - Culture
    - Cost cutting pressures
    - Cost of insecurity not known

(Adapted from Dr. Eduardo Gelbstein Presentation)

IS Management and Governance
Future of IT – Information Security Concerns

- Big Issues (cont'd)
  - Process
    - IT – Infosec boundaries
    - Governance of IT and infosec
    - Standards and certification
    - Vulnerability management
    - Understanding Risk
    - Disposals
    - Outsourcing, Offshoring
    - Data governance, Legal framework

IS Management and Governance
Future of IT – Information Security Concerns

- Big Issues (cont'd)
  - Technology
    - Military strength malware
    - Software complexity
    - Software quality
    - New technologies and services (possible unknowns)

IS Management and Governance
Future of IT – Information Security Concerns

- Vulnerabilities known today include:
  - Unaudited outsourcers
  - Offshore software development
  - Contractors and Temp staff
  - Malicious insider
  - No backup for critical people
  - Virtualisation
  - Cloud computing
  - Mobile e-everything
  - Social networks

IS Management and Governance
Future of IT – Information Security Concerns

- Vulnerabilities known today (cont'd):
  - Disclosures/ leakage
  - Security as an after-thought
  - Unmonitored security policies
  - Weak identity management
  - Weak privileged password management
  - Incomplete or untested DR/BC plans

IS Management and Governance
Future of IT – Information Security Concerns

- Vulnerabilities known today (cont'd):
  - Complexity
  - Patching
  - Single Points of Failure
  - Weak configuration mgmt
  - "No More Money"

IS Management and Governance
Future of IT – Information Security Concerns

- Insecurity Waves:
  - Wave #1: Attacks on Availability
    - Attackers are smart and keep learning!
  - Wave #2: Attack on Confidentiality
  - Wave #3 (The emerging wave): Data Integrity attacks against trusted systems
    - Common in this category is Fraud

IS Management and Governance
Future of IT – Information Security Concerns

- Consider Emerging Technologies and Associated risks:
  - Cloud Computing
  - Virtualisation
  - "Social Media": Consider Corporate usage
    - Facebook
    - Twitter
- **Questions:** Do information security management and governance considerations keep up with advancement in technology? How clear are we with risks associated with emerging technologies?

IS Management and Governance
Future of IT – Information Security Concerns

- Cloud Computing (an emerging technology)
  - refers to the delivery of scalable IT resources over the Internet, as opposed to hosting and operating those resources locally, such as on an organisation's network
  - The resources can include applications and services, as well as the infrastructure on which they operate.
  - By deploying IT infrastructure and services over the network, an organisation can purchase resources on an as-needed basis only thereby avoiding the capital costs of software and hardware
- Are we clear on information security concerns and related Information Security standards?

IS Management and Governance Concluding Remarks

- *Responsibility* cannot be delegated; it is only *Performance* that can be delegated
- Our public accountants have a critical role to play in the area of information security management and governance
- With emerging technologies, the mindset of the accountant must change regarding protection of information assets
- In a nutshell: What is the role of the accountant in the protection of information assets?

IS Management and Governance Concluding Remarks

- My Prediction
  - *Our great grandchildren will wonder how we economically survived by relying on in-house IT infrastructure (server rooms, etc.) just like we wonder today how our forefathers/mothers survived before the invention and generation of commercially viable electric power.*
  - Each of our forefathers/mothers had to generate their own individual power/fire for cooking and heating. Today, we simply 'rent' the electric power. Tomorrow, 'cloud computing' will be the way to do business!

Discussion / Q&A

Q & A

and / or

THANK YOU

SRS Website – www.securityrisksolutions.net

ISACA Website – www.isaca.org

e-mail Address: Office – jona.owitti@securityrisksolutions.net

Personal – jona.owitti@yahoo.com

Phone Contact: +254 (0)20 273-5401/2; +254 (0)722 74-2525