ADDING BUSINESS VALUE THROUGH EFFECTIVE IT SECURITY MANAGEMENT

BY
HUSSEIN K. ISINGOMA
CISA, FCCA, CIA, CPA, MSC, BBS

AG. ASSISTANT COMMISSIONER/INTERNAL AUDIT
MINISTRY OF FINANCE, PLANNING AND ECONOMIC DEVELOPMENT

ISACA- KAMPALA

28th April 2010
• Introduction
• What is IT Security Management?
• Security Management Cycle
• Key IT Security Concerns
• Adding Business Value
• Challenges
• Conclusion
Introduction

Businesses are increasingly dependent on IT to facilitate their operations.

Information is critical not only for business survival but for businesses to thrive.

Businesses are now more concerned about the significant damage that the various IT threats and vulnerabilities can cause.

Business expenditure on IT has been increasing by the day and there is no let up yet!

Challenge of effectively managing IT security has grown in both difficulty and importance.

<table>
<thead>
<tr>
<th></th>
<th>2009</th>
<th>2009</th>
<th>2010</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computing Hardware</td>
<td>326.4</td>
<td>-13.9</td>
<td>331.7</td>
<td>1.6</td>
</tr>
<tr>
<td>Software</td>
<td>220.7</td>
<td>-2.1</td>
<td>231.5</td>
<td>4.9</td>
</tr>
<tr>
<td>IT Services</td>
<td>780.9</td>
<td>-3.5</td>
<td>824.2</td>
<td>5.6</td>
</tr>
<tr>
<td>Telecom</td>
<td>1,887.7</td>
<td>-3.6</td>
<td>1,976.6</td>
<td>4.7</td>
</tr>
<tr>
<td>All IT</td>
<td>3,215.7</td>
<td>-4.6</td>
<td>3,364.0</td>
<td>4.6</td>
</tr>
</tbody>
</table>

Worldwide IT Spending Forecast (Billions of US Dollars)

Source: Gartner (January 2010)
Security Management

Security is a condition that results from the establishment and maintenance of protective measures (preventive or detective) that ensure a state of inviolability from hostile acts or influences.

IT Security Management therefore focuses on:

i. Identity and Access Mgt (3 W’s)

ii. Information Mgt

iii. Threat Management

ITSEC management is about identification of Potential systems problems/vulnerabilities and related controls.

ISACA-KAMPALA

28th April 2010
IT Security Management Cycle

1. Define Environment & Assets
2. Monitoring & Audits
3. Security Administration
4. Security Design Implementation
5. Security Risk Analysis
6. Policies, Standards, & Guidelines
Control Objectives for Information Technology (CoBIT)

Deliver and Support (DS)

Ensure Systems Security (1-21)

5.1 Manage Security Measures

5.2 Identification, Authentication and Access

5.3 Security of Online Access to Data

5.4 User Account Management

5.5 Management Review of User Accounts

5.6 User Control of User Accounts

5.7 Security Surveillance

5.8 Data Classification

ISACA - KAMPALA

28th April 2010

Detailed security standard that can be used by an organization to ensure effective security Management

Formally a British standard BS7799 (1995)

ISO 17799 Security Domains

- Security policy
- Security organisation
- Asset classification
- Personnel security
- Physical and Environmental Security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance
Objectives of IT Security Management

(C) Confidentiality
- Safeguards unauthorized use/disclosure of information

(I) Integrity
- Safeguards the accuracy and completeness of information and processing methods

(A) Availability
- Reliable and timely access to information and associated assets when required.
IT Security Management Concerns

- Data Security
- Physical Security
- Standards
- Disaster Recovery
- Access Security
- Telecommunications
- Database Administration
- Operating System Software
- Production Control
- Operations
- System Development Methodology
<table>
<thead>
<tr>
<th>Operations</th>
<th>Production controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Training-functional and refresher courses</td>
<td>• Maintenance of the master schedule</td>
</tr>
<tr>
<td>• Standard operating procedures / operational manual)</td>
<td>• Controls over updates</td>
</tr>
<tr>
<td>• Preventive maintenance schedules</td>
<td>• Controls over batch input and output processing</td>
</tr>
<tr>
<td>• Separation of duties(SoD)</td>
<td>• Logs maintenance</td>
</tr>
<tr>
<td>• Offsite procedures</td>
<td>• Handling of information</td>
</tr>
</tbody>
</table>

**Operations and Production Security Concerns**

ISACA - KAMPALA

28th April 2010
Telecoms/network security concerns

- Service level agreements (SLA’s) between telecom/network providers.
  - Uptime thresholds,
  - incident response times,
  - 3rd party business continuity arrangements

- Network traffic monitoring; traffic patterns should be reviewed regularly; unusual patterns monitored

- Intrusion prevention and detection (IPDS)

- Are the companies providing the WAN services providing pro-active monitoring and response
Encryption Security Concerns

- Policies on data to be encrypted
- Who is responsible for encryption keys. Do custodians understand and accept their key-custodian responsibilities?
- Frequency of change of passwords
- Storage of copies and destruction of obsolete keys
- Key Creation Procedures
- Key Rotation Procedures
Access security Concerns

- Access should be based on least privilege i.e. granting users only those accesses required to perform their duties

- Review of Access Control Lists (ACL’s) i.e. list of users and type of permitted access

- User registration/supplier creation (Weigh the pros and cons of centralized/decentralized controls)

- Password use/management

- Terminal log on/off procedures

- Deprovisioning of access rights and accounts for consultants, IT service providers etc
Transaction Logs Maintenance

- Who/ what has access to the logs?
- How long are the logs maintained (record retention time)?
- How are the logs backed up; log server separate from transaction server?
- Responsibility for periodic review of systems generated logs

**Objective?**

Ensure the integrity of audit trail data against unauthorized modification
Policies and Procedures Concerns

- Do policies exist e.g. on Encryption, data/log retentions, passwords, 3rd party access etc

- Do they meet mgt’s compliance needs

- Periodic reviews
  - Relevance
  - Performance
  - Conformity
  - Regulatory requirements

- Best practices; COSO, COBIT
Security Assurance issues

- Define a disaster
- Business continuity/Disaster Recovery Plan
- Recovery time objectives in case of disaster
- Resource requirements
- System/network recovery plan
- Evidence of testing the plan
- Resource requirements
  - People
  - Equipment etc
- Outsourced service provider BCP/DRP arrangements

Disaster?

ISACA - KAMPALA

28th April 2010
Compliance - Legal and regulatory framework

- Do legal and regulatory requirements for enforceability and remedies for data electronically transmitted and received exist?

- Is compliance reviewed?

- Does IT processes conflict with other existing legal framework?

- Acknowledgment of transactions/receipts/payers in e-transactions; what do the laws regulations require?
Service Level Management

- Mutual compliance
- Performance metrics are measured and reported on periodically
- Charges for lapses and rewards for over performances defined
- Rights to inspection/audit of service provider defined e.g SAS 70 in the USA.
ITSEC Management; Adding Business Value

The benefits of an effective, well designed Security Management system extend to foundations of business itself!

Benefits are derived through enhancement of Confidentiality, Integrity and Availability of Information systems

Pro-active threat management (part of Security Management) delivers business value!

Business Value of Pro-Active threat Management!

• Cost Management
  ○ Reduction of number and frequency of successful attacks increases productivity as less time is spent on recovery efforts

• Business Continuity
  ○ Impact on the availability of critical systems could result onto loss production time, million dollar transactions, loss of key clients, suppliers and business relationships

• Risk mitigation
  ○ Reduction of attacks and potential attacks improves business risk profile

• Asset protection
  ○ Web applications, operating systems and critical business processes

• Improved management control
  ○ Better quality and increased scope of available information across business

• Operational efficiencies
  ○ Improvement in the input – output ratios
Contd.........; Adding Business Value...CIA?

Confidentiality
- Increased Compliance e.g data protection, copyrights
- Insulation of trade secrets
- Clients and User information protection
- Improved customer confidence; business growth/market Devt.

Integrity
- Protection of business data against unauthorized access and alteration
- Access of business information/data on a need to know, have and do basis !-Access privileges
- Security of business Info/data across networks- Encryptions

Availability
- Increased systems reliability
- Continuous business operations; less downtimes, outages
- Increased productivity ; ensuring systems uptime
- Increased user/client satisfaction and client relationships

ISACA- KAMPALA

28th April 2010
Business Value; The BSC?

- Supply chain mgt - Amazon
- e-payments - credit cards
- Production
- Profitability
- Sales turnover - Airtime
- Reporting and disclosure
- Improvement of Business image
- Product differentiation
- Product development - mobile money?
- Availability of information on markets, stocks, investments etc
- Business Innovations
- Growth and Learning
- Customer focus
- Financial
- Processes

ISACA - KAMPALA

28th April 2010
the Challenges

- The weakest point in ITSEC; Human factor
- Availability of skilled, knowledgeable and experienced IT security resources
- The broader and varied view of security across business; Finance, Sales and Board
- Security monitoring 24x7. Lights out operations in production Job scheduling
- Increase in Social Engineering in all its forms
- Lack of a pro-active management of Security – reaction mode!
- Dynamic business risk profile
- Management of third Party IT service providers
- Lack of business Security awareness programmes
- Business IT Governance maturity levels
- Balancing security with systems performance
Conclusion and think about it!

Key ITSEC Investment Questions!

- How much is the lack of security costing business?
- What impact is the lack of security having on productivity?
- What impact would a material security breach have?
- What are the cost effective Security solutions?
- Is the exposure being reduced?

Source: G41: Return on Security and Investment (ROSI)

Thank you!