INFORMATION SYSTEMS AUDITS

BACKGROUND

Most organizations rely on IT for day to day information processing, storage and transmission. Take the case of the accounts department at Egerton University- the Accpac accounting package is used to capture student fees payments, government grants, incomes from other activities, salaries and wages (for 4000 plus employees) and other expenses- and automatically generate financial reports. The academic department relies on IT to capture, and to process and store students' grades (For 30,000 plus students) and to generate student performance reports and academic transcripts.

A system regardless of its size will normally consist of the following elements

- Batch vs. online processing
  In batch processing, input data are gathered and processed periodically in discrete groups. In online processing, transactions data may be entered directly from originators at remote locations. A system could be **online, real-time**, where data input is processed immediately, or **online batch**, where data input is accumulated and later processed as a discrete group.
- Database system
  Here integrated database files are shared among many users, as opposed to having many computers each with its own data files loaded. This system reduces data redundancy.
- IT Networks
  Transfer of information across networks has been made possible by telecommunications- the transmission of information by radio, wire, fiber optics, microwave, and so on. A network could be a LAN, WAN, PAN, e.t.c.
- End user
  As opposed to the IT department having custody of all the data and applications, in end user computing, the end user departments are responsible for the generation and use of information.

Whereas IT has undoubtedly very positive impacts on employees' productivity and efficiency in service delivery, it has some drawbacks. Take the following scenario:

- Burglars break into the Finance department offices and take away the computer hosting all the university finance records (This is very common in our country, unfortunately).
- The academic department is in the process of updating students' academic records in readiness for a graduation ceremony due next week. Just before they print out the graduation list, the computer crashes (God knows why).
- Mrs. X gains unauthorized access to the students' academic records and makes changes to the grades obtained by Mr. Y, a fourth year student who is also his relative. Consequently, Mr. Y average grade is changed from C to A.
- Unknown people hack into the finance department computers, and transfer money from the bank account of Egerton University to an account at another Bank in Kenya. This other account was opened using forged identification documents and so catching the perpetrators is almost impossible.
- A fire razes down both the finance and academic department offices and all the computers and hard copies of source documents e.g. receipts, supplier, invoices e.t.c.

By eliminating the human errors, IT based systems enhance reliability of financial information. This however is not without risks.

THE CHALLENGE

Like fraud, IT crime is big business and the real scale is unknown. Most organizations choose not to report the crimes in order to protect their reputation. An ordinary street robber or mugger would be all too happy to switch to IT crime (where there is no chance of getting shot dead by a policeman with no regard for human rights or getting lynched by an irate mob) had he the sufficient knowhow. Evidence is there that more and more criminals are resorting to IT crime. It is worth noting that In IT based systems, there is the lack of hard copy paper documentation (paper trail) to link individual transactions with the summary figures in the financial statements.

To support the continuing flow of business, comply with the regulatory environment and provide the necessary accountability, organizations should create and maintain authentic, reliable and usable records and protect the integrity of those records for as long as required.[i] The challenge is for the IT Auditor to examine the controls put in place by the management over information systems and to assess their adequacy at ensuring authenticity, reliability and usability of records. In other words, the IS Auditor verifies that internal controls over information assets exists, that they are adequate, and being applied and working as they are supposed to. In modern competitive environments, organizations need to protect their information assets- namely business secrets like new designs, formulas, and preliminary results of the other R&D projects in progress. Thus confidentiality of records is of great importance.

CHARACTERISTICS OF GOOD RECORDS

Every record should correctly reflect what was communicated or decided. For example if a student scores grade A in Auditing II course, the records should reflect that. If a student has paid Ksh. 70,000.00 in fees for the semester, the records should not reflect an amount higher or lower than that. Records management, policies, procedures and practices should lead to authoritative records that have the following characteristics.[ii]

- Authenticity- An authentic record is one that can be proven to:
    - Be what it purports to be.
    - Have been created or sent by the person purported to have created or sent it.
    - Have been created or sent at the time purported.
- Reliability- A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities. Records should be created at the time of the transaction or incident to which they relate, or soon afterwards, by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction.
- Integrity- The integrity of a record refers to it being complete, and unaltered. It is necessary that a record be protected against unauthorized alteration. Records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what conditions additions or annotations may be authorized, and who is authorized to make them. Any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

  If information is to be used in criminal proceedings, organizations must be able to identify who has had access to a particular record at any given time from collection, to creation of evidence copy, to presentation as evidence. The evidentiary weighting of records will be substantially reduced if the chain of custody cannot be adequately established or is discredited.
- Usability- A usable record is one that can be located, retrieved, presented and interpreted. It should be directly connected to the business activity or transaction that produced it. The contextual linkages of records should carry the information needed for an understanding of the transactions that created and used them. It should be possible to identify a record within the context of broader business activities and functions. The links between records that document a sequence of activities should be maintained.

INFORMATION SYSTEMS RISK

The risk of poor information systems and unreliable security and back-up arrangements leads to possible fraud, error, non-compliance with data protection rules, customer dissatisfaction and security breaches. Poor information systems can undermine an organization and its entire reputation may be at stake. The IIA (UK and Ireland) Information Technology Briefing Note Three covers Internet Security (A Guide for Internal Auditors) and suggests a number of IS risk areas[iii]:

- Theft of proprietary information.
- Sabotage of data or networks.
- Eavesdropping.
- System penetration.
- Abuse of Internet.
- Access Fraud.
- Denial of service.
- Spoofing.

In a majority of cases, the criminals insert malicious code (a worm or a virus) into the target computer to achieve their objective. Examples of malicious programs used are key loggers, screen capture software e.t.c. In addition, a notable increase in phishing and fraudulent transactions has been noted. Less serious but very prevalent and annoying problems include spam emails.

Spoofing refers to fraudulent spam e-mail: a method of sending e-mail using a false name or e-mail address to make it appear that the e-mail comes from somebody other than the true sender[iv]. This is very common- you have probably received such mail claiming to be from Microsoft, The UN, e.t.c.

Phishing is the commission of fraud to get financial information or other confidential information: to trick somebody into providing bank or credit-card information by sending a fraudulent e-mail purporting to be from a bank, Internet provider, etc. asking for verification of an account number or password[v] spear phishing on the other hand targets executives by convincing them to click on a link that will download malware/ Trojans on their computers.

Fraudulent transactions result in financial loss or damage to the reputation of the organization. It would include the fraudulent transfer of cash from a bank account of the organization to criminals, and the more common theft of credit card numbers of customers.

THE INSIDER THREAT

Computer emergency readiness team (CERT) shows that 80% of all malicious activity comes from current or former employees, yet most organizations spend over 75% of their IT security budgets to protect against outsiders[vi]. The era of building fences around the IT infrastructure is over, and controls to be put in place should protect the organization from the insider threat.

RISK MITIGATION MEASURES/ CONTROL ACTIVITIES IN AN IT SYSTEM

The following controls may be undertaken to enhance security over information and the infrastructure used to generate and store the information.

1. Entity level controls

The starting point in implementing all other controls in an organization is to put in place entity level controls. Without the entity level controls, all the other controls may not be very effective. The entity level controls include:

- Security policy definition- the organization should have a well defined security policy covering all business processes. The policy must be communicated to employees.
- The security policy should be updated in a timely manner, and a periodic communication of the updates made to all employees in an organization.
- There must be security awareness among employees. Cases of spear phishing occur because the employees lack awareness and hence click on links that download malware into their computers.
- Pre-employment background screening- research shows that most employees engaged in fraud and other malpractices have a predisposition towards fraud that could have been detected via background screening.

2. **General control activities**

   a) **Controls in the development and customization of programs/ systems**

   The specific controls include,

   - Policies that require user involvement in systems development or purchase process.
   - Appropriate testing of programs and systems.
   - Technical input during program development e.g. the internal audits to advice on appropriate controls to be inbuilt into the system.
   - Proper documentation in the form of flowcharts and / or other descriptions.
   - Obtain over the shelf software only from reputable sources.
   - Prohibit use of unauthorized programs.
   - Prohibit downloading of programs from sources such as computer bulletin boards.
   - Use computer virus detection software.

   b) **Changing existing programs or systems**

   The specific controls are, among others,

   - Appropriate review and approval of all changes.
   - Thorough testing of modified program/ system.
   - Comprehensive documentation of changes, showing what was changed, with appropriate justification.

   c) **Access controls over programs and data**

To start with, risk associated with access controls should be identified. The level of the risks identified should be assessed in order to identify sound policies and procedures for granting authorized user access while simultaneously protecting against unauthorized access[vii]. The following are some of the measures that can be taken to address risks of unauthorized access.

- Authorization and authentication of users in the access rights policies and procedures.

  Authorization controls are meant to ensure that the person seeking access is authorized. It involves the use of login credentials, normally the user ID and password. A major weakness here is that most authorized users use weak passwords. It is worth noting that hackers have developed methods to crack weak passwords. A strong password should:

  - At least eight characters long.
  - Includes at least one special character (%, $, @ and so on).
  - Includes at least one number.
  - Have characters with mixed cases (upper case/ lower case).
  - Makes use of incoherent phrases (like **nH1k%j@tG** instead of **Nairobi**)
  - Passwords should be changed periodically, i.e. not static.

  The problem is that good passwords are always harder to recall. To thwart imposters, computer systems usually limit the number of attempts and restrict the number of times or the duration which the password is valid. In addition, there should be a policy that requires authorized users to change their login credentials regularly

  Authentication is aimed at ensuring that people logging into systems are who they claim they are. The following controls are used for authentication.

  - Biometric identification methods that use unique personal characteristics, such as fingerprints, retinal patterns, facial characteristics, or voice recordings.
  - A more secure method is to require possession and use of tamper-resistant plastic cards with microprocessor chips, known as "smart cards," which contain a stored password that automatically changes after each use. When a user logs on, the computer reads the card's password, as well as another password entered by the user, and matches these two respectively to an identical card password generated by the computer and the user's password stored in the computer in encrypted form.
  - USB Tokens refer to hardware devices that must be connected to the remote computer in a USB slot before access will be granted.
  - Temporary PINs are numbers sent back to a prearranged device, such as a text message to a cell phone number in which to gain remote access. Usually users have limited time to enter the PIN along with their ID and password.

- Logging and review of logs over all failed access attempts.

- Need to Know basis for accessing applications and data
  Once logged in, an authorized and authenticated user should be constrained from having access to all data and applications. Employees should have access only to those applications necessary to do their particular job. Thus there is need for additional log in credentials for sensitive applications. Compliance with the need to know can be determined by reviewing the user membership in the Active Directory (AD) groups for rights appropriate to the user's job duties[viii]. The data from the AD may be extracted and analyzed using the data analytics tools. Here it is important to review system logs for access rights.
- Systems administrators and the "Keys to the Kingdom"
  Users who have privileged access have ability to create an unauthorized account, access an existing shared account or compromise an existing account belonging to a different user.

  System administrators are an example of users that have access to almost all applications. In other words they hold "Keys to the Kingdom." Administrators' access can be hard to manage, but the following controls over administrators at least help reduce risks associated with them.

  - Avoid using a default user ID and passwords for administrators.
  - Minimize the number of employees with access to administrative rights.
  - Establish a mode for segregating duties in the form of role based access controls among the system administrators.
- Termination, hiring, and transfer of employees
  When employees are terminated, there should be effective controls in place to terminate the employees' access to the system. In case of newly recruited employees, the employees need to know basis should be assessed and access granted only to those applications and data necessary for that person's job responsibilities. When an employee is transferred, their access rights may change. Thus, the human resources transfer policy should include a review and change, if necessary, of access rights.

d. Controls over transmission

The integrity of a record refers to it being complete, and unaltered. As data is transmitted over the network, it may get intercepted and changed, or get corrupted. Integrity is key in all data, but is especially critical in e-commerce, e-mail, EFT, EDT (Electronic data interchange), electronic finance (e.g. m-pesa pay bill/ shopping), E-money models, among others. In an EFT transaction for example, suppose a bank is transferring Ksh. 2,000,000.00, and the transaction is intercepted and altered. The controls that should be in place over these systems are:

- Firewall mechanisms to mediate between the public network and the private network for the organizations.
- Implement a system of identifying uniquely the participant in a transaction e.g. certifying key pairs and public/ private key encryption.
- Digital signatures so initiator of e-commerce transaction could be uniquely identified with.
- Establishment of key audit trails that could be utilized by the auditor.
- Message acknowledgements using echo checks.
- Use of private dedicated lines as opposed to shared lines to transmit data of critical importance.

e. <u>Storing retrieving, transportation and disposing of confidential information</u>

Management should define and implement procedures to prevent access to, or loss of, sensitive information and software from computers, software and other equipment or media when they are stored, disposed or transferred to another user. This should be done for:

- <u>Backup files of databases</u>
  Data should be backed up and stored in a different geographic area from the business. In addition, the backup should be encrypted to protect the data from unauthorized access.
- <u>Disposal of media previously used to hold confidential information</u>
  Such media should be reformatted and then conducting a secure wipe using the appropriate software. In extreme cases the media should be demagnetized or destroyed
- <u>Management of equipment sent for offsite maintenance</u>
  Some organizations contract third parties to maintain their computers. Before a computer is sent to a third party for maintenance, the data files/ software should be backed up and then erased. Computers holding very confidential data should never be sent out for maintenance.
- <u>Preserving information during shipment/ storage</u>
  Manufacturers usually publish the recommended temperatures and humidity in which to store media. To minimize potential damage, media should:
  - Be kept out of direct sunlight.
  - Kept free of dust.
  - Kept free of liquids
  - Kept away from exposure from magnetic fields, radio equipment and any vibrations.

f. <u>IT Operations controls</u>

- To prevent unauthorized changes to programs, the computer/ system operators should not have access to detailed program documentation (source code) beyond what is necessary in performing their daily tasks.
- Careful job scheduling and monitoring of program modification.
- Segregation of duties.
- Review of computer operators logs by the data control group[ix].

3. <u>Application control activities</u>

These are controls that relate to individual transactions- the use of IT to initiate, record, process and report transactions or other financial data. The controls include:

- Proper authorization of transactions to be processed.
- Use of programmed control (inbuilt in computer programs) activities such as:
  - Limit tests- these are tests for reasonableness, using a predetermined upper and lower limit.
  - Validity test refers to comparison of data against a master file/ table for accuracy.
  - Self checking number, which includes redundant data attached to a piece of data to check for accuracy.

- Use of input validation checks, such as
  - Item/ record count, a count of the number of items being input in a given batch.
  - Control totals, the totals of each fields of information for items in a batch.
  - Hash total, the total of one field of information for all items in a batch, regardless of them being unlike. For example, in entering inventory, suppose you have 4 computers, and 2 vehicles; the hash total will be 6 (meaningless). The control totals will be 4 and 2 respectively.

Conclusion

The controls above would only work if the management is committed and has communicated the security policies, and created a risk aware culture by conducting risk awareness, openly discussing risk components with employees and establishing and maintaining acceptable levels of risks. Even with all these in place, there will still be criminals out to commit fraud, or disgruntled employees seeking revenge for one reason or the other. Thus IT security is continuous, and controls are no guarantee against security breaches. The price of freedom is eternal vigilance.

References

[i] International organization for standardization, ISO 15489-1: 2001, *Information and documentation- Records management- Part 1: General*, 2001.

[ii] Ibid.

[iii] Pickett, Spencer (2005), *The essential handbook of internal auditing*, John Wiley & Sons, LTD, Chirchester, England

[iv] *Microsoft ® Encarta ® 2009*. © Microsoft Corporation, USA.

[v] ISACA, *Five questions with ….. Robert Schperberg, CISM ®, EnCEP*, ISACA Journal Vol. 5, 2010

[vi] Singleton, Tommie W., PhD, *Mitigating IT Risks for Logical Access,* ISACA Journal Vol. 5, 2010

[vii] Ibid

[viii] Hoesing, Michael, CISA, ACDA, CDP, CIA, CISSP, CMA, CPA, *Applying Data Analytics to IS Audits*, ISACA Journal, Vol. 4, 2010.

[ix] Whittington, Ray; Pany, Kurt (2004), *Principles of auditing and other assurance services, fourteenth edition*, McGraw Irwin, Boston.