LIBRARY AND INFORMATION RESOURCES' SECURITY: TRADITIONAL AND ELECTRONIC SECURITY MEASURES

Omosekejimi Ademola Ferdinand
Federal University of Petroleum Resources P.M.B 1221 Efuurun
Warri, Delta State
NIGERIA

Ijiekhuamhen Osaze Patrick
Federal University of Petroleum Resources P.M.B 1221 Efuurun
Warri, Delta State
NIGERIA

Ojeme Thelma Nneka
Federal University of Petroleum Resources P.M.B 1221 Efuurun
Warri, Delta State
NIGERIA

ABSTRACT

The security of information/knowledge is essential to its effective exploitation or use. As knowledge expands, the need to organize it and to provide adequate security becomes more pressing. This study describes how the information bearing materials of the library can be secured using traditional and electronic measures. Literature were reviewed on the concept of information resources security, features of a good security measures (traditional and electronic), Securing the library resources traditionally, securing the library using telecommunication, benefits of securing the library resources, problems associated with the use of electronic security system in the library, and ways of solving problems with the use of electronic security system in the library.

Keywords: Library, information Resources, Information Security (InfoSec), Library Security.

INTRODUCTION

The exponential growth of information and information bearing materials are a result of the ever increasing growth of knowledge gives impetus for the need to organize information materials and to provide adequate security for these materials. According to Parker (2002), the security of library materials (book and non-book materials are of utmost importance to the librarian and information specialist for the purpose of reducing or avoiding unauthorized access to information bearing materials available in the library. To avoid unauthorized access to library resources, library management and information professionals must devise strategies which will enable them to provide adequate security that can protect the information resources available in the library. Library resources are the information bearing materials which enable the library to fulfill its goal of meeting the information needs of its users (Adomi, 2008). Libraries in their effort to provide a broad array of resources to meet the needs of their users collect resources in various sizes and formats. These library resources can include manifestation of the printed world, audio and video recordings, microforms, visual and electronic resources and generations of requisite equipment for accessing or listening to data stored on them". These resources constitutes library collection that help in meeting the users information needs

Library collections are changing rapidly as more and more electronic resources become available. The proliferation of electronic resources does not mean that printed resources will disappear. According to Aina (2004), library resources or materials must be safe; hence security

devices must be made available by libraries to ensure that the materials are not stolen or mutilated." Though libraries have been providing some level of security measures, for example, making available security staff that is always at the entrance of a library to ensure that all library materials taken out of the library are checked. So also most libraries do not allow patrons to bring their bags and briefcase into the library. In spite of these precautions, library materials are still not safe. Therefore there is need for librarians to device a very concrete physical means of securing the materials available in the library and to have telecommunication or electronic security systems which will help to provide a safe and secure facility for library resources and equipment. To provide adequate security using telecommunication, electronic systems such as building alarm systems, access control systems, video surveillance, telesurveillance etc. can be adopted in the library.

Concept of Information resources' security

Information security, sometimes shortened to InfoSec, is the practice of defending information and information bearing materials from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc...). The definitions of InfoSec suggested in different sources are summarized below:

1. "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2009).
2. "The protection of information bearing materials i.e. book and non-book materials and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (CNSS, 2010).
3. "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (ISACA, 2008).
4. "Information Security is the process of protecting the intellectual property of an organization." (Pipkin, 2000).
7. "Information security is the protection of information, information bearing materials and minimizes the risk of exposing information to unauthorized parties." (Venter and Eloff, 2003)

Features of a good security measure (Physical and Electronic)
Integrity

In securing information bearing materials, data integrity according to Efrim (2011), is very crucial. Meaning to maintain and assure the accuracy and consistency of the data over its entire life-cycle. This means that data/information cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

Availability

Paolo & Resca (2008) opined that for any information bearing materials and system to serve its purpose, the materials, the system and the information contained in them must be available when it is needed. This means that the physical materials such as books carrying the information, the computer systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

Authenticity

In library, information security is necessary to ensure that information bearing materials or documents (electronic or physical) are genuine (Thomas and Teufel, 2003). It is also important for authenticity to validate that both parties involved in the exchange of information and information bearing materials are who they claim to be. Some information security systems incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and was sent by someone possessing the proper signing key.

Securing the Library Physically (Non-Electronic)

The first step in securing library assets includes physical (non-electronic) deterrents. These include architectural considerations, the use of security personnel, and security hardware

Site Design

Site planning and landscape design issues should be considered when planning for a safe and Secure library. Crowe & Timothy (2000) asserts that site lighting at vehicular and pedestrian entrances and circulation areas should be continuous and sufficient to support a secure atmosphere as well as support appropriate surveillance. Appropriate and clear signage should be provided, including off-site and entrance signage as well as on-site signage that should include directional, cautionary, and parking signs for employees, visitors, service vehicles, and pedestrians. Signs should generally not be provided to identify sensitive areas. Landscaping elements should enhance security by deterring unwanted entry while not allowing criminals to conceal themselves from security personnel and CCTV systems. Vehicle control is important; a specified distance from the library building to unscreened vehicles and parking should be appropriately set. Various types of buffers and barriers should be evaluated to enhance the landscape design while still providing the appropriate protection. These buffering features could include walls, fences, trenches, plantings, trees, static barriers, sculptures, and street furniture. Vehicular entrances should be designed to prevent high speed approaches.

Building Design

According to Lynn (2001), the following areas of the library generally pose threat when discussing security issues unless they are appropriately addressed in the design:

1. Exterior entrances
2. Archive and special collection storage spaces
3. Special collection reading areas
4. Children's library area
5. Critical building component locations such as electrical switchgear, communication and security equipment, and building control centers
6. Public toilets
7. Loading docks, mailrooms, and shipping/receiving areas
8. Stairwells
9. Office locations
10. Roof access

Entrances and exits from the library are a particular concern with regard to theft of library materials. When designing a new library, the ideal arrangement is a single point of entry to the secure area of the facility. Magnetic theft detection devices are placed at this location to sound an alarm if unchecked library materials are taken through this point of control. Occasionally, however, it may be desirable for external planning reasons to allow patrons to approach and enter the library from opposite directions, resulting in two points of entry to the building. This could result from site features, required location of parking areas versus public transportation locations, or urban design considerations. It is important in these situations to continue to maintain a single point of entry to the secure area of the library (Lynn, 2001). Although this may require special planning and space arrangement within the library, several layouts, that can accommodate this requirement. Special collections spaces, depending on the value of the collections, require a certain level of security design and electronic systems. The risk of theft, particularly for rare books and artifacts, can be high, and both the architectural space planning and the specialized systems should reflect the determined level of risk. Control of entrance and exit from special collection areas, as well as the design of electronic systems, are discussed below. In general, however, the space planning of special collection areas and their support spaces should be determined as part of the overall security design features. The arrangement of the special collections service desk with regard to the reading areas and any book stacks should be planned so that a clear line of sight exists between the desk and the reading tables. Flat open tables are preferred to enclosed furniture or carrels, so that surveillance can be maintained at all times. If book stacks are located in the special collection reading areas, they should not be positioned so that the visibility of any patron workstation is blocked. Toilets or other enclosed spaces that cannot be readily monitored should not be located within special collection areas. It may also be desirable to institute a checking procedure for personal belongings and bags before a patron is allowed to enter these sensitive areas. This policy requires the location of a locker space near the entrance to the special collection room or suite.

Security Personnel

As part of the security plan, the library security team should evaluate the value and need for security personnel, during both normal working hours as well as after the library is closed. Security personnel typically patrol within the facility as well as on the grounds and operate any implemented CCTV system. The security guards may also be used to enforce appropriate library access at the main lobby.

Window Protection

There are many types of window security including locks, guards, grilles, bars, screens, and films. Window locks should be fitted to all windows that can open and are accessible without the means of a ladder. For best control, these windows should be secured by key-operated locks (not just a simple latch). This includes all ground floor windows, windows above garages or other roof tops, windows near to walls or pipes or other structures, which could be used to access the window. Generally, any window over 60cm. in height (approximately 24 inches) should be fitted with two key-operated window locks to prevent forced opening. If the security risk assessment investigation determines that the library location has the potential for burglary through windows or vandalism to the windows, then guards, grilles, bars, security screens, or security films should be installed. Securing the window through the use of guards, grilles, or bars is not always architecturally acceptable, although they can be a cost effective solution in certain circumstances (Cherdantseva and Hilton 2013).

A wide range of security screens and films is also available. When using the screens or films, there are no unsightly iron bars, steel mesh, or expanded metal which may not actually protect the glass. Screens and films unobtrusively protect property and glazing by preventing access to windows.

Door Protection

Door protection includes cylindrical locks, deadbolts, mortise locks, and gates. A cylindrical lockset fits into a large hole bored into the door's face with the keyhole in the door knob. The latch assembly is locked and provides the securing of the door, though this type of lock provides the least amount of security in door protection. The addition of a deadbolt provides enhanced protection by increasing the metal support into the door jam. The throw of the deadbolt should be at least one inch. A mortise lockset fits into a rectangular pocket in the door's edge and usually has a deadbolt that is an integrated part of the locking mechanism. When you turn the key from the outside, it releases both the knob and the deadbolt. The mortise lockset is the most secure locking mechanism for a door. If the security risk assessment investigation determines that the library location has the potential for burglary through accessible doors, then security gates should be considered. Securing doors through the use of gates is not always architecturally acceptable and could require special treatment to allow exiting in case of fire. Normally such security gates should be considered only for high crime environments (Timothy2000).

Folding gates are designed to make facilities more secure and still allow frequent, easy access to those who need it. They fold easily back and out of the way when people or equipment need to

pass, but provide a lockable barrier when closed. Security gates are excellent for situations where extensive security is desired when the library is closed or at restricted access points (such as rear entries), but visibility and air flow are desired as well. Securing front doors after-hours, shipping and receiving docks, and other restricted areas such as archive storage is sometimes most cost effective with folding gates. Folding gates typically retract to a fraction of their extended width and pivot up to 270 degrees to clear the doorway. They are typically designed to accept padlocks for secure closing.

Securing the Library Using Telecommunication (Electronic)

Information and information resource security using telecommunication system or devices means protecting information, information systems or books from unauthorized access, damage, theft, or destruction (Kurose and Ross, 2010).The major element of any electronic or telecommunication security include burglar protection, collection security, electronic access control and video surveillance.

Burglary Protection

There are different ways of classifying the types of sensor systems. Sensor can be active or passive, convert or visible, volumetric or line detection. They can also be defined by their mode of application. According to Jadhara and Kulkami (2000) active sensors transmit some type of energy and detect a change in the received energy created by the presence of motion of the intruder. Passive sensors detect some type of energy emitted by the intruder, or detect a change of some natural field of energy caused by the intruder. Convert sensors are hidden from view and visible. Sensors are in plain view. Volumetric sensors detect intrusion on a volume of space, where line detection sensors detect intrusion across a line. Lynn (2001) also asserts that "Door and Window Contacts can also be used to trigger and alarm whenever library doors or windows are opened without authorization." They can be attached to recess within the door or window frame to detect movement.

Collection Security

There are many methods of ensuring that no material leaves the library without being checked out. These systems always contain a security device that is placed on the materials (including books, magazines, video cassettes, audio cassettes, CDs and DVD) as well as a detection device that is typically located at a library's exist. The detection device must be safe for magnetic media, usually have audible/or visible alarms, if desired, the audible alarm can be voice alarm. According to Brown and Patkus, (2003), "there are two major methods currently used for detection; electromagnetic and Radio Frequency Identification (RFID) RFID solutions are being designed to improve library operation/efficiency. This enhanced capability is provided by RFID tags which do not require line of sight to be read, so that books are actually handled less. The tag combines book identification and book security into one label, minimizing labeling time and cost. Patron self-checkout systems are also available to libraries that incorporate RFID technology. Patrons can process several items simultaneously and the security devices can be turned off in a matter of seconds. A patron of the RFID can be allocated for theft detection so that no other tag is required since the antitheft device is in the label, the security gates do not

need to be attached to a central system or interface with the library's central database. According to Brown and Patkus (2003), some of these features are also available on an electromagnetic detection system when used in combination with a barcode. This type of system is limited, however, since the barcode must be visible to the detector to identify the materials and the electromagnetic device with a barcode system does not allow for any additional information to be stored in the tag if desired.

Electronic Access Control

Electronic access technology is the best system for controlling access to library building, facilities, resources and rooms. Authorized people are allowed to enter a controlled area by automatically unlocking of the door. Plastic access cards are inexpensive and software can be programmed to restrict access to certain areas while recording the time, date and location of authorized and unauthorized access. According to Dean (2004), "for extra security, access control can be used in conjunction with video surveillance to control and monitor large collections and equipment's." Access cards can be integrated as photo ID cards for library employees and can be used as temporary keys for library clientele to have access to restricted areas. The access system can also be used for monitoring employee time and attendance, security patrols of the property and can limit access to sensitive areas, information or equipment. Electronic access control system enhances safety and protects valuable library assets. Access control solution range from simple authorized access systems to advanced close circuit monitoring and exception reports delivered through secure internet connections. The most popular types of cards is the magnetic strip cards, which looks like a credit card and carries two or more tracks of information on the magnetic stripe, these can be used for access control and other services. Dean (2004), asserts that the proximity card is more expensive but is also more durable an easier to use. For internal use, a close range type is used; for car parking entrance, a longer range of up to one yard or so is possible. Proximity card readers can be hidden behind a wall surface for aesthetic purposes, with just a marker on the wall. Other available card readers include bar code readers and RFID readers.

Paul (2009) stated that entry keypads can also be included within access control system for entry without a card or in addition to the card. Biometrics entry systems are available included fingerprint recognition, palm recognition, and scanning system for high security measure.

Securing the Library and information Resources Using Video Surveillance

Video surveillance and closed-circuit television (CCTV) systems serve as a way to monitor and record security, deter crime and ensure safety. Advances in CCTV technology and reduction in cost have also made video surveillance a cost effective management tool for library facilities. McCahill and Norris (2002) noted that "libraries can use closed-circuit television (CCTV) to identify visitors and employees, monitor work areas, deter theft and ensure the security can also use to monitor and record evidence on clientele and staff misconduct in the library. CTv systems are quickly becoming one of the most important and economic security and safety tools available to libraries. The key steps when considering the designing a CCTV system for library according to McCahill and Norris (2002), includes:

* Determine the primary application of the CCTV system
* Define the layout and characteristics of the control area(s) of the library building
* Decide on camera type and features
* Determine the best location for viewing monitors
* Determine the best method of signal transmission
* Decide on the type of recording/archival equipment for the system

According to Jodhar and Kulkami (2000), "The primary purpose of a CCTV system are detection, observe, monitor and record observation, provide real time information for detection identification, recording, provides after the tact material for assessment, analysis and review, usually with overlaid time, date and location information.

Securing the Library and Information Resources Using Surveillance camera

CCTV cameras use small high definition color cameras, but by linking the control of the cameras to a computer objects can be tracked semi-automatically. According to Bannister et al… (2009), the technology that enable this is often referred to as VCA (video content analysis) and is currently being developed by a large number of technology company around the world and can be adopted by the library for the purpose of securing their resources. These current technologies enable the system to recognize if a moving object is a moving person or a crawling person. It can also deter mine the movement of people i.e.staff and users within the storage area of the library as to how they are moving and whether they are assessing library resources or just reading. Based on this information, the system developers implement features such as blurring faces of "virtually wall" that block the sight of a camera where it is not allowed to film. It is also possible to provide thesystem with rules, such as for example "sound the alarm whenever a person is walking close to the shelf area of the library without authorizes access. Marcus (2007) asserted that "VCA also has the ability to position people on a map by calculating their position from the images". It is then possible to link many cameras and track people through the library building. This can also be done for forensic purposes where a person can be tracked between cameras without anyone having to analysis any hours of film. According to Marcus (2007), these surveillance motion detection imaging and camera can be used to monitor the following places in the library premises:

* Monitor driveway to the library building
* Monitor the parking area of the library
* Monitor the library shelf areas
* Monitor the library equipment, such as library computers located in each offices
* Monitor the movement of staff and users within the library
* Monitor the exchange of materials within the library, etc.

Benefits Associated with the Use of Telecommunication in Securing Library and Information Resources

Libraries are essential cultural institution, we use them at every stage of our lives, and their facilities make large bodies of books, research materials, and the internet available to the public for universal use, video surveillance security cameras and other security measure are great tools

for libraries, as they can protect large areas of space and allow librarians and staff to immediately check in on concerns from the reference desk or office. According to McCahill and Norris, (2002), the major benefits of using electronic security system in the library are:

1. **Maximum security**: Patrons of all ages and types use libraries every day. Security cameras places around the library can help to keep safe while reading, researching and browsing as well as the information resources they are using.
2. **Prevent theft**: Every part of a library's collection is valuable. A video surveillance system working in conjunction with a barcode and magnetic book control system could help prevent book theft and monitor the move of books and other resources as it moves from one user to another.
3. **Flexibility**: If video systems allow users to place cameras where they are needed, and reconfigure them in a whim libraries, especially those that host community events, author readings or children book clubs, could greatly benefit from the flexible security that IP video provides
4. **Remote monitoring**: Video surveillance systems that use the cameras and network recorder (NVR) allow libraries to broadcast their surveillance footage over the internet. This allows management and security to check in on libraries at any time should security concerns arise, the broadcast function could also be to archive speakers or special events at the library.

Problems of Using Electronic Security System in Library

As telecommunication or electronic security systems has greatly helped the libraries to provide maximum security for their resources and equipment, so also, there are problems and difficulties faced by libraries and information Centre's on the use of telecommunication security systems and devices. As stated by Voters (2007), the problems are:

1. **Inadequate fund**: Libraries and information Centre's lack the financial; resources to purchase and install the telecommunication security systems and devices that can help to protect the level of security required as a result of the budgetary allocations from their parent organization.
2. **Lack of literate or skilled personnel**: libraries and information Centre's lack skilled personnel that can operate, teach and instruct the use of these telecommunication security systems even when they are made available in the library.
3. **Poor power supply**: These telecommunication security systems or devices need electricity to power them and due to the poor power supply, these systems often time are not working and as such are incapable of performing their expected task of securing the library and its collection.
4. **Hardware and software failure**: This is major threat to the use of telecommunication security system in the library. When there is software failure or hardware breakdown that may require the need for an engineer who may not be available to put them in place as at when due, then the library system and its collections is at risk.
5. Libraries in remote areas do not have access to telecommunication security system because they cannot afford the money to purchase the devices and cannot adequately cater for them.

Ways of Solving Problems with the Use of electronic security system in the Library

According to Voters (2007), the factor militating against the effective use of telecommunication security systems and devices can be subdued in the following ways:

1. **Enlightening the parent organization on the importance of using telecommunication security devices and systems in the library**: The librarian and information experts should take out time to educate their parent organization on the benefits associated with libraries and information Centre's in the use of telecommunication security systems and devices so that the library parent body can release adequate fund which will be used for the purchase of telecommunication security devices in the library.
2. **User education**: This is very important, because most of the staff do not know how to operate telecommunication devices, especially the security system devices that requires extra skills. As a result of these, there is need for user education so that all library staff will be taught on how to operate these devices to how they are mounted and where.
3. **Making available an organizational based engineers**: An organizational based engineer should be made available who will always be available to take up issues in case of hardware breakdown or software failure.
4. Making available in the library alternative power supply i.e. a stand-by generator that can serve the whole library when there is failure in power supply.

CONCLUSION

Since the essence and usefulness of telecommunication security system and devices in libraries are to help provide maximum and adequate security for the library employees, resources and equipment as well patrons and the entire library building, it is necessary that these telecommunication systems and devices are made available in the library. The usefulness of telecommunication security systems and devices in the library cannot be over emphasized due to the following benefits: maximum security for library building and resources, prevention of theft in the library, flexibility, remote monitoring etc.

However, the use of telecommunication security system and devices require budgetary management support, staff support, software development and hardware upgrade for the attainment of the set goals thereby appealing to the library management to release funds that is needed to accomplish this task. Based on this, the researchers advice libraries to:

1. Ensure that sufficient/adequate is allocated to libraries for the purchases, development and maintenance of telecommunication security systems and devices.
2. Organize user education programme and in-service training for the staff on how to use telecommunication security system and devices to secure resources.
3. Organize seminars, workshops, conferences etc. for the board members, directors, administrator and management of libraries and information Centre's in other to create awareness among library authorities about the advantage and benefits of using ICT facilities and telecommunication security systems.

4. Employ competent and experienced in-house computer engineers who can handle the repairs of the telecommunication security systems and devices in case of software failure or hardware breakdown.
5. Make available a power generating plant i.e. generators that can supply electricity in case of power failure.

REFERENCES

Adomi, E.E (2008), Foundation of Reference and Information Science.

Aino L.O (2004) Library and Information Science Text for Africa: Third World information services limited Ibadan, Nigeria.

Banister, J Mackenzien, A. and Norris, P. (2009), Public Space CCTV in Scotland: Scottish Centre for Crime and Justice Research (Research Report).

Baram Marcus (2007), "Eye on the City" Do Cameras Reduce Crime? ABC News.

Braw Parker E. (2002), Library and Safety: Handbook of Prevention, Policies and Procedures Chicago American Library Association.

Boritz, J. Efrim. "IS Practitioners' Views on Core Concepts of Information Integrity". International Journal of Accounting Information Systems. Elsevier. Retrieved 12 August 2011.

Cherdantseva Y. and Hilton J. "A Reference Model of Information Assurance & Security," SecOnt 2013 workshop in conjunction with the 8th International Conference on Availability, Reliability and Security (ARES) 2013, University of Regensburg, Germany. September 2–6, 2013. IEEE Proceedings.

Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.

Crowe, Timothy D. (2000) Crime Prevention through Environmental Design: Applications of Architectural Design and Space Management Concepts, Second Edition, Butterworth: Stoneham, MA and National Crime Prevention Institute.

Edward Dean (2004), Theft and Loss from Uk Libraries: A National Survey. Home Office Research Group, Crime prevention Unit Paper no 37. Home Office Police Research Group.

Guidelines for the Security of Rare Books, Manuscripts, and Other Special Collections (Final version approved July 1999), Prepared by the ACRL Rare Books and Manuscripts Section's Security Committee.

ISACA. (2008).Glossary of terms, 2008. Retrieved from http://www.isaca.org/Knowledge-Center/ Documents/Glossary/glossary.pdf

ISO/IEC 27000:2009 (E). (2009). Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC.

Ives, Rao D. (2005), Security Management Strategy for protecting your Libraries Network and library Computers.

James F. Kurose, Keith W. Ross (2010) Computer networking: a top down approach.

Kiountouzis, E.A.; Kokolakis, S.A. Information systems security: facing the information society of the 21st century. London: Chapman & Hall, Ltd. ISBN 0-412-78120-4

Levis, Paul (2009), Every step you take: Uk underground Centre, the spy capital of the world. Nigerian Guardian March 2, 2009.

Librarians Glossary and reference book (1999)

Lim, Joo S., et al. "Exploring the Relationship between Organizational Culture and Information Security Culture." Australian Information Security Management Conference
Mary Lynn (2001), The Design and evaluation of Physical protection systems, butter worth; Stone harm, NA guidelines for the security of rare books, manuscripts, and other special collection

Mccahill, M.N and Norris P. (2002) Electronic Security: A case Study of IIT, Bombay Central Library, Proceedings of the CALIBER 3, available at www.library.iitb.ac.in/-mnj/caliber3.pdf

Patkus, B.L (2003), Collection Security: Planning and Prevention for libraries and archives. Available at http://www.nedec.org/plam.3/heat312.htm.

Pipkin, D. (2000). Information security: Protecting the global enterprise. New York: Hewlett-Packard Company.

Schlienger, Thomas, and Stephanie Teufel. "Information security culture-from analysis to change." South African Computer Journal 31 (2003): 46-52.

Spagnoletti, Paolo; Resca A. (2008). "The duality of Information Security Management: fighting against predictable and unpredictable threats". Journal of Information System Security 4 (3): 46–62.

Venter, H. S., & Eloff, J. H. P. (2003). A taxonomy for information security technologies. Computers & Security, 22(4), 299–307. doi:10.1016/S0167- 4048(03)00406-

Voters B. (2007), Best answers chosen by Voters: Prospect and Problems of the use of telecommunication facilities: the way forward.