Design and Development of Dynamic Information Security Management Models for Sustainable Academic Libraries

J Shivarama *Vaishali A Dawar*

Abstract

In the process of library automation, making digital resources available through library website and during communication with users, there are always chances of information security breaches. Many times, the libraries may need to pay very high price and face uneasy consequences for such incidences. This article tries to create awareness among librarians about the complex process of information security management through overview of various such models. The second part of the paper contributes comparative studies on attributes considered in the selected models. Also, comparative study of attributes in each model with Security Controls Sections in Information Security Standard ISO/IEC 27001:2013 and with functions of management 'POSDCORB' by Gulik and Urwik.

Keywords: Academic Libraries, Digital Information Security, Digital Library, Information Security, Information Security Management Process, Information Security Models

1. Introduction

In February 2016, an incident of defacing JNU Library website after hacking and posting some anti-national text on it created awareness among librarians about security of their website. The Asian Age newspaper of 26 March 2016 informed "A weak security system in the Education and Research Network (ERNET), the registrar for the domain *.ac.in which is used by educational institutions all over India allowed hackers claiming to be from Pakistan divert email and browsing to an external website and not the intended page since Wednesday night. The Indian Institute of Technology Bombay (IIT-B) was one of the websites that got affected." (Dodhiya, 2016). Some other such incidences also had occurred around the world, such as hacking of Bundaberg Regional Libraries website by Syrian activists in January 2015, hacking of Library of Congress Website and publicly available defaced version of the site for one-and-a-half hours on January 17, 2000. Hackers or intruders inventing new techniques every day for intruding into your data, e.g. your phone can be hacked via sound waves controlled by 'Musical Virus'. (Times of India, 2017). Besides hacking the intruders also had damaged computers or network, deleted important files or data, caused data loss, used library computers and network without permission, etc. in libraries many times. The threats included from small data loss to entire system destruction, making the libraries non-trustable for confidentiality or integrity of data. The damages occurred and efforts made for restoration of damaged data or files or websites were in such a scale, which caused libraries too much financial and reputation losses.

Federal Information Security Management Act of 2002, Clause 3542, United States Code, Subchapter

11th International CALIBER-2017
Anna University,Chennai, Tamil Nadu 02-04 August, 2017

III—Information Security (E-Government Act, 2002) stated Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide—

- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
- Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- Availability, which means ensuring timely and reliable access to and use of information. Information Security Management is a process of defining the security controls in order to protect the information assets.

2. Importance of Information security for academic libraries

With presence of infinite information in digital form, the libraries understood the importance of providing services and resources in digital form and the importance of their presence in virtual world through Digital Libraries, library website, social media, and repositories. Through internet the libraries can easily provide library resources, services, tools, software to multiple users anytime and at user's desired destinations across the world.

The role of Information security is protecting the assets of a library, data and digital communication channels in the environment of increasing threats for damages to online information. For the security of the library and users it has become necessary for libraries to seriously consider about information security and take necessary care to protect the information resources in their possession. Information security management is necessarily applicable in the academic library activities such as digital repositories on cloud, digital library, library website/ web portal, providing access to online databases, digital document delivery, digital information resources, social networking usage for information delivery and so on.

One comes to know about the information security problem only after detecting the attempted attack, till then it is difficult to notice this problem. There are various regulations for digital information security. The process of digital information security is complicated and its cost is also high in comparison with print media. Since libraries provide free access to computers, networks and ICT, the librarians must seriously consider about the management of information security.

3. Significance of the study

The information security management consists of various multidisciplinary components such as information and communication technology, physical security, digital security, cloud security, human resource management, environment studies and so on. Consideration of all these factors makes information security management a very complex phenomenon. For thoroughly understanding of the complexity of information security one needs the simplified presentation of all the necessary components of the system. This underlines the importance of models in information security management.

4. Importance of Information Security Management Models for sustainable Academic Libraries

Models are an interactive engagement experience of a complex system or structure. A m**odel is a** representation of a system, entity, phenomenon, or process and provides a distinctively powerful strategy, making it easier to understand any complex problem. Information security management models are providing visual overview of the process involved and it ultimately making easy to understand the complex information security process along with its related management issues by dividing it into sub-processes and their real-life implementation. In the present paper an evaluative overview of some information security management models is given along with their comparison with each other. The models selected for this paper are in accordance with their applicability in the academic libraries.

5. Dynamic Information Security Management Models: Harnessing of sustainable Academic libraries:

The nine Information Security Management models selected for this article are as below.

M1. System Dynamics Information Security Management Model (SDISMM)

M2. Model for Information Security Assurance in Organizations (MISAO)

M3. Reference Model of Information Assurance and Security (RMIAS)

M4. Library Information Security Assessment Model (LISAM) – the only model available, which is developed for libraries.

M5. Interpretive Structural Model for Information Security Management (ISMISM)

M6. Business Model for Information Security (BMIS)

M7. Information Security Management System (PDCA model)

M8. Information Security Management Meta Model (ISMMM)

M9. Information System Security Knowledge Management System (ISSKMS)

5.1 Information Security Management Models: An Overview

An overview of all the above-mentioned models in Table 1 shows the founder(s) of the model, year of formation, number of parameters used in the structure of each model, whether the model used any measuring scale, number of steps in each model and the structure or appearance of the model.

Table 1: An overview of the Information security models

Sl. No	Name of the model	Founder	Year of formation	No. of parameters	Scale	Steps	Structure
M1	SDISMM	Derek L. Nazareth, Jae Choi	2015	Several	Normalization scale	Several segments	System Dynamics
M2	MISAO	Eng. Bogdan Tiganoaia	2014	12	No scale	6	3D Cube
M3	RMIAS	Yulia Cherdantseva and Jeremy Hilton	2013	50 approx	No scale	4	Graphical, cyclic. Generic abstraction
M4	LISAM	Roesnita Binti Ismail	2012	5 constructs	Two scales	5	Staircase
M5	ISMISM	Muktesh Chander, Sudhir K. Jain and Ravi Shankar	2011	12	No scale	7 levels	Steps
M6	BMIS	ISACA	2010	10	No scale	No particular steps	Triangle, cyclic
M7	PDCA	Dr. W. Edwards Deming.	2008	4	No scale	4	Lifecycle
M8	ISMMM	Anene L. Nnolim	2007	20	No scale	Several sub-models	complex structure
M9	ISSKMS	Petros Belsis, Spyros Kokolakis and Kiountouzis, E.	2005	6	No scale	2	Triangle in circle

6. Analysis of the Information Security Management Models for sustainable Academic Libraries

6.1 M1 –System Dynamics Information Security Management Model (SDISMM)

Derek L. Nazareth and Jae Choi developed this model in 2015 for guiding managers to take information security management related decisions beneath a variety of circumstances for the financial implications of information security. According to them the effective ISM requires deployment of security resources on multiple fronts, such as attack prevention, vulnerability, reduction and threat deterrence, etc. The model is developed using design science research methodology. This complex model includes

- ❖ Stocks – accumulated or deployed over time
- ❖ Flows – draw from or empty into infinite reservoirs
- ❖ Converters – with values specified by time period
- ❖ Loops – reinforcing or balancing values
- ❖ Segments – addressing attacks, software risks, recovery, vulnerability, and economic considerations

The model is highlighting on quantifying and verifying information security issues and is slanted more at the organizational level and towards an economic perspective. The model is validated by structural validation and behavioural assessment to assess the degree of confidence (Nazareth and Choi, 2015).

6.2 M2 - Model for Information Security Assurance in Organizations (MISAO)

The necessity of the investments in information security is highlighted in this MISAO model based on ISO 27001:2006 and ISO 17799:2005 developed by Eng. Bogdan Tiganoaia. According to him information security is an actual and dynamic domain that is in a continuous change (Tiganoaia, 2013). Bogdan believes the model is suitable for all types of organizations and useful for implementation and certification of an ISM system in accordance with international standards. The model has two main modules:

- v Information security risk management
- v Steganographic system used for secured communication.

The model occupies six modules along with input and output mechanisms in these two main modules.

- ❖ Information security policy
- ❖ Information security risk management
- ❖ The security of Human Resources
- ❖ The security of communications
- ❖ The security of information resources (measures for protection and recovery)
- ❖ Access control to information (policy)

6.3 M3 – Reference Model of Information Assurance and Security (RMIAS)

Yulia Cherdantseva and Jeremy Hilton in their RMIAS model had addressed two trends in Information Assurance and Security (IAS) evolution i.e. 'diversification' and 'deperimetrisation'. This model provides a common ground for all professionals of ICT. The model has four dimensions:

- ❖ Information system security lifestyle – 5 stages
- ❖ Information taxonomy – 4 attributes
- ❖ Security goals – 8 goals presenting Octave
- ❖ Security countermeasures – 4 types

These four dimensions are deemed compulsory and sufficient for an understanding of the IAS domain at the chosen high level of abstraction and its conceptual model should be regularly revised to reflect the changes in the domain. They do not overlap and do not duplicate each other. (Cherdantseva and Hilton, 2013). The goal based approach is more useful for taking decisions in cost-effectively implementation of information security.

RMIAS's five stages Security Development Lifecycle demands consistent addressing of information security needs in all stages of the system lifecycle and establishing a time-bound sequence of IAS activities. The four attributes of Information Taxonomy (Form, State, Location, Sensitivity) provides basis for the specification and selection of security goals and its countermeasures. The model presents 8 goals for information security. The description of the interrelationship between the dimensions of the RMIAS starts from the top left quadrant. An organization defines its current stage at the security lifecycle and then goes over the other three dimensions to come back to the next stage of the lifecycle (Cherdantseva and Hilton, 2013).

6.4 M4 - Library Information Security Assessment Model (LISAM)

Based on Hagen, Abrechtsen and Hoveden's (2008) Organizational Information Security Staircase Model of four steps this LISAM model is developed by Roesnita Binti Ismail. LISAM has some additional factors and one more step addition i.e. 'Technological Security Foundation Including Technological Measures' to the previous staircase model. This model developed in Malaysia and is the only model, which specifically focuses the library settings. This model specifies that in order for effective information security measures, security should be built like a staircase of combined measures. The model also highlights that the higher the position on the staircase, the more complex is the state of information system security management in a library (Ismail, 2012).

The five steps of the staircase are -

- ❖ Technological Security Foundation
- ❖ Information Security Policy
- ❖ Procedures and Control
- ❖ Administrative tools and methods
- ❖ Awareness creation.

This model also provides two scales of measures as assessment instruments useful for indicating the overall information security level in library.

- ❖ Degree of implementation (very high to very low)
- ❖ Overall Security level/ status (very good practice to very poor practice)

6.5 M5 - Interpretive Structural Model for Information Security Management (ISMISM)

This model ISMISM is formed by three Indian authors Muktesh Chander, Sudhir K. Jain and Ravi Shankar in 2013 using interpretive structural modelling (ISM) technique, which is useful in understanding and interpreting complex system by mapping the relationships among its components (Chander, 2013). For development of this model various mathematical techniques were used, such as, binary comparison, structural self-interaction matrix, graph, transitivity relationships, etc. The authors acknowledged following twelve critical parameters in information security management:

- ❖ Top management commitment
- ❖ Identification and classification of information assets of organization
- ❖ Technological tools and solutions
- ❖ Providing information security policies and procedures
- ❖ Providing information security organizational structure and resources

- ❖ Awareness, education and training of stakeholders
- ❖ Motivation, reward and punishment
- ❖ Physical and environmental security of organization
- ❖ Information system audit, testing and certification
- ❖ Compliance to legal and regulatory provisions
- ❖ Incident management, business continuity planning and disaster recovery
- ❖ Developing information security culture in the organization.

A directed graph (digraph) was prepared by mapping these twelve parameters and then using MICMAC analysis technique the directed graph converted into ISM-based model. As per the digraph all the parameters were retained in seven levels and then the structure is converted into Interpretive Structural Model. The level 5 possessed three parameters and level 7 had four parameters and level 1 to 4 and 6 denoted only one parameter each. The relationships between the parameters were shown by arrows.

6.6 M6 - Business Model for Information Security (BMIS)

This model BMIS useful to inspect security issues from a systems perspective and holistic security management was established by ISACA (ISACA, 2010), a non-profit global association developing practices for information systems. This model essentially focused on the corporate and business sector. It is a very simple model, the first of its kind and useful for understandings factors related to information security. The BMIS consists of four elements-

- ❖ Organization design and strategy element
- ❖ People element
- ❖ Process element
- ❖ Technology element

These four elements are linked by six functional interconnections: governing, culture, enabling and support, emergence, human factors

6.7 M7 - Information Security Management System- PDCA model

This model is very important because of its incorporation in many British Standards and ISO standards related to information security and is also applicable to all the processes in information security management systems. The PDCA cycle (also known as Deming cycle developed by Dr William Edwards Deming in 1950s.) was introduced in 2002 version of British Standard of information security i.e. BS7799-2 and is also aligned with quality standards such as ISO-9000;27001:2005. The standard implies "the part of the management system dealing with information security is referred to as the Information Security Management System (ISMS). The ISMS specify the instruments and methods that the management should use to clearly manage (plan, adopt, implement, supervise and improve) the tasks and activities aimed at achieving information security" (BSI, 2008). The revised version of this standard ISO/IEC 27001-2013 edition also states "the organization shall determine the boundaries and applicability of the information security management system to establish its scope" (INB/NK 149, 2013).

The model involves four essential constituents – principles of management, resources, personnel and information security process (policy, concept, organization). The model indicates that the entire information security process has a lifecycle including planning, implementation, performance and improvement or optimization. To describe the underlying forces of the information security process in a simple way possible it is frequently divided into 4 phases- Plan, Do, Check and Act and due to this the model is also referred as PDCA model. It is in principle being applicable to all tasks of the information security process and is applicable for all organizations. PDCA model is considered as a basis for many other information security management models.

6.8 M8 - Information Security Management Meta Model (ISMMM)

Anene L. Nnolim (Nnolim, 2007) presented this enterprise focused model ISMMM. This model has a potential for integration of ISM goals and objectives with other lifecycle process of the organization, e.g. strategic planning, budgeting. ISMMM model considers organization's business strategy and mission as fundamental inputs.

This model has no pattern and hence appears as a complex nonlinear structure. For preparing this conceptual model the author had used a framework-based approach. The model also comprises of some more models within itself such as Information Security Management Process Model, Information Security Process Improvement Model, Security Model and Information Security Planning model. This complex model is a bit difficult to understand the next step after any step. The model does not give a flawless view of information security management and it requires further simplification.

6.9 M9 - Information System Security Knowledge Management System Model (ISSKMS)

Petros Belsis, Spyros Kokolakis and Kiountouzis, E. (Belsis, 2005) offered a simplistic model of information security in the form of a triangle and a circle. The structural or hierarchical background of the model has three layers:

- ❖ Policy – a set of high level instructions and directions
- ❖ Guidelines – Specific operational steps for policy implementation
- ❖ Measures – the security controls or specific actions for implementing the guidelines

The organization related information sources, which were not embodied in the above categories:

- ❖ Risk analysis,
- ❖ Information security related knowledge
- ❖ Organizational environment.

These three information sources categories provide knowledge about information security requirements of an organization to the above mentioned three layers.

Though it gave an impression as a simple model, it provided a very systematic structure for 'Information System Security Knowledge Management' required for the organizations.

7. Comparison of Information Security Management Models Process:

The above analysis indicates different approaches and different purposes of the selected information security management models. The number of parameters used in the model shows the complexity of the information security process. The study

shows that the new models are more complex in nature than the older models developed prior to 2008 indicating the increasing complexity of the information security problems with new developments in ICT. Only two of the above models show use of scale for measuring information security levels. According to three models information security is cyclic process, whereas in other models there is no further process or any repetition implied in the process after achieving a desired information security.

Table 2 gives an analysis of attributes or factors considered in the above listed information security management models. The table shows technical security procedure, security measures/ controls, policy/ guidelines, staff training/education, information security awareness/ culture as mostly used attributes in the above evaluated models. Whereas, reporting attack/ damage, security goals, legal/ statutory provision, recovery assurance, cost as least used attributes. In all the above studied models planning, risk assessment, review/ audit are moderately used attributes.

Table 2: Attributes or factors considered in the information security management models

Attributes? Model?	Planning	Risk Assessment	Security goals	Technical security procedure	Policy/ Guidelines	Staff training/education	IS Awareness/ Culture	Reporting attack/ damage	Review/ Audit	Legal/ Statutory provision	Recovery assurance	Security measures/ Controls	Cost
SDISMM	No	No	No	Yes	No	No	No	Yes	No	No	Yes	No	Yes
MISAO	No	Yes	No	Yes	Yes	Yes	Yes	No	No	No	Yes	No	Yes
RMIAS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
LISAM	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No
ISMISM	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	No
BMIS	Yes	Yes	No	Yes	No	Yes	Yes	No	No	No	No	Yes	No
PDCA	Yes	No	No	Yes	No	No	No	No	Yes	No	No	Yes	No
ISMMM	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes	No
ISSKMS	No	Yes	No	No	Yes	No	No	No	No	No	No	Yes	No

7.1 Comparison of Information security management models with Security Control Sections in Information Security Standard ISO/IEC 27001:2013

ISO/IEC 27001:2013 is an International Standard for an Information Security Management System (ISMS) published in 2013 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).). Its previous version ISO/IEC 27001:2005 titled "Information technology – Security techniques – Information security management systems – Requirements" is superseded by ISO/IEC 27001:2013 in the year 2013. ISO/IEC 27001:2013 (ISO, 2013) gives a framework of policies and procedures with, physical, technical and legal controls for managing security of information assets in any organization. The information assets may include intellectual property, employee details, financial information, or any such information entrusted to us by third party. By adopting and implementing this standard any organization can bring information security under the explicit management control. ISO/IEC 27001:2013 (ISO, 2013) has now 114 security controls organized in 14 sections and 35 control objectives. The Table-3 compares components in Information Security Management Models with Security Control Sections in Information Security Standard ISO/IEC 27001:2013.

Table 3 - Comparison of Information security management models components with Security Control Sections in Information Security Standard ISO/IEC 27001:2013

Sl. No. as in Standard	Security Control Sections in Information Security Standard ISO/IEC 27001:2013	M1	M2	M3	M4	M5	M6	M7	M8	M9
A.5	Information security policy	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes
A.6	Organization of information security	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.7	Human resources security	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
A.8	Asset management	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes
A.9	Access control	No	Yes	Yes	Yes	Yes	No	No	No	Yes
A.10	Cryptography	No	No	Yes	No	No	No	No	No	No
A.11	Physical and environmental security	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes
A.12	Operations security	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes
A.13	Communications security	No	Yes	Yes	Yes	No	No	No	No	No
A.14	Information systems acquisition, development and maintenance	No	No	Yes	No	No	No	No	No	No
A.15	Relationship with external parties	No	Yes	Yes	Yes	No	No	No	No	No

Sl. No. as in Standard	Security Control Sections in Information Security Standard ISO/IEC 27001:2013	M1	M2	M3	M4	M5	M6	M7	M8	M9
A.16	Information security incident management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.17	Information security in business continuity management	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No
A.18	Compliance with legal and contractual requirements	No	No	Yes	Yes	Yes	No	No	No	No

7.2 Comparison of Information security management models with functions of management by Gulik and Urwik (PODSCORB):

Gulik and Urwik had classified all functions of management in seven categories, which are popularly known as 'PODSCORB' (Appannaiah, 2016). The following table 4 shows the directly indicated functions of management in Information Security Management Model. Since these models shows the management of information security, if any function is not directly indicated in the model means that function is indirectly involved.

Table 4: Examining the involvement of functions of management in Information Security Management Model.

Sl. No.	Functions of Management	M1	M2	M3	M4	M5	M6	M7	M8	M9
1	planning	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2	organizing	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
3	directing	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
4	staffing	No	Yes	Yes	Yes	Yes	Yes	No	No	No
5	coordinating	No	No	No	No	No	Yes	No	No	No
6	reporting	Yes	No	Yes	Yes	Yes	No	No	No	No
7	budgeting	Yes	Yes	Yes	No	No	No	No	No	No

The table 4 shows that there is no consistency in directly indicating functions of management in information security management models. Some functions are directly indicated some functions are indirectly indicated by using another term. The indirect indication is either through synonymous terms or through some other variables.

8. Conclusion

In this world of digital disruption library needs to make themselves suitable for satisfying the needs of their users. The only model established specifically for libraries is 'Library Information Security Assessment Model (LISAM)' developed by Malaysian academic libraries. Other than LISAM the most significantly useful models for academic libraries are Reference Model of Information Assurance and Security (RMIAS), Model for Information Security Assurance in Organizations ((MISAO) and Interpretive Structural Model for Information Security Management (ISMISM). Whereas, Information Security Management System (PDCA model) used in standards is considered as a basic model for information security. The significance of any of these models to academic libraries dependents on the purpose of information security defined by that library's management. The comparative study of the models with Security Control Sections in Information Security Standard ISO/IEC 27001:2013 and Functions of Management 'POSDCORB' will be useful for librarians while applying these models in information security management of their library.

References

1. Appannaiah, H.R., Dinakar, G and Bhaskara, H.A. (2016). Management (multi-dimensional approach). Mumbai, Himalaya Publishing House.
2. Belsis, P., Kokolakis, S., and Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. Information Management and Computer Security, 13(2), 189-202.
3. Chander, Muktesh, Jain, Sushir K., and Shankar, Ravi (2013). Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach. Journal of Modelling in Management, 171-189.
4. Cherdantseva, Yulia and Hilton, Jeremy (2013). A Reference Model of Information Assurance and Security. Eighth International Conference on Availability, Reliability and Security (ARES), p. 546-555
5. Dodhiya, K. A. (2016, March 26). IIT-B website, others hacked. The Asian Age, p.3
6. E-Government Act of 2002. PUBLIC LAW 107-347—DEC. 17, 2002. Federal Information Security Management Act of 2002. Accessed on October 10, 2015, from http://www.gpo.gov/fdsys/pkg/STATUTE-116/pdf/STATUTE-116-Pg2899.pdf
7. Federal Office for Information Security (BSI) (2008). BSI-Standard 100-1: Information Security Management Systems (ISMS). Accessed on March 2, 2016 from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile
8. ISACA (2010). The Business Model for Information Security. Rolling Meadows, IL: ISACA.

9. Ismail, Roesnita Binti (2012). Assessing information security management in Malaysian academic libraries. Kaula Lumpur: University of Malaya.

10. Nazareth, Derek L. and Choi, Jae (2015). A system dynamics model for information security management. Information & Management (52), p.123-134.

11. Nnolim, Anene L. (2007). A Framework and Methodology for Information Security Management. Southfield, MI: Lawrence Technological University.

12. The standardization committee INB/NK 149 (2013 Nov). SN ISO/IEC 27001:2013(E) - Information technology - Security techniques - Information security management systems - Requirements. Geneva, ISO copyright office.

13. Tiganoaia, Bogdan (2013 Nov). A new model for information security assurance in organizations - proposal and case study. **International Conference on Management and Industrial Engineering** 6: 189-196. Bucharest (Romania): Niculescu Publishing House.

14. Times of India (2017, 15 March). Your phone can be hacked via sound waves. P.19.

About Authors

J. Shivarama, Assistant Professor, Tata Institute of Social Sciences, Mumbai–400088
Email: shivaramatoo32@gmail.com

Mrs. Vaishali A. Dawar, Librarian, Narsee Monjee College of Commerce and Economics, JVPDS, VileParle (West), Mumbai.
Email: vadawar@gmail.com