Send Orders for Reprints to reprints@benthamscience.ae

BENTHAM OPEN

CrossMark

The Open Medical Informatics Journal

Content list available at: www.benthamopen.com/TOMINFOJ/

DOI: 10.2174/1874431101610010004

REVIEW ARTICLE

Reasons in Support of Data Security and Data Security Management as Two Independent Concepts: *A New Model*

Hamid Moghaddasi[*, 1], Samad Sajjadi[2] and Mehran Kamkarhaghighi[3]

[1]*Health Information Management & Medical Informatics, Department of Health Information Technology and Management, Faculty of Paramedical Sciences, Shahid Beheshti University of Medical Sciences. Tehran, Iran*
[2]*Faculty of Paramedical Sciences, Shahid Beheshti University of Medical Sciences. Tehran, Iran*
[3]*Medical Informatics, Faculty of Paramedical Sciences, Shahid Beheshti University of Medical Sciences, Tehran, Iran*

Received: February 7, 2016 Revised: July 20, 2016 Accepted: July 23, 2016

Abstract:

Introduction:

Any information which is generated and saved needs to be protected against accidental or intentional losses and manipulations if it is to be used by the intended users in due time. As such, information managers have adopted numerous measures to achieve data security within data storage systems, along with the spread of information technology.

Background:

The "data security models" presented thus far have unanimously highlighted the significance of data security management. For further clarification, the current study first introduces the "needs and improvement" cycle; the study will then present some independent definitions, together with a support umbrella, in an attempt to shed light on the data security management.

Findings:

Data security focuses on three features or attributes known as integrity, identity of sender(s) and identity of receiver(s). Management in data security follows an endless evolutionary process, to keep up with new developments in information technology and communication. In this process management develops new characteristics with greater capabilities to achieve better data security. The characteristics, continuously increasing in number, with a special focus on control, are as follows: private zone, confidentiality, availability, non-repudiation, possession, accountability, authenticity, authentication and auditability.

Conclusion:

Data security management steadily progresses, resulting in more sophisticated features. The developments are in line with new developments in information and communication technology and novel advances in intrusion detection systems (IDS). Attention to differences between data security and data security management by international organizations such as the International Standard Organization (ISO), and International Telecommunication Union (ITU) is necessary if information quality is to be enhanced.

Keywords: CIA Triad Model, Cryptography, Data security, Data security management, Data security theories, Parkerian Hexad Model.

INTRODUCTION

Any information that is generated and stored should be protected against accidental or intentional manipulation or

* Address correspondence to this author at the Health Information Management & Medical Informatics, Department of Health Information Technology and Management, Faculty of Paramedical Sciences, Shahid Beheshti University of Medical Sciences, Tehran, Iran; Tel: 0098 21 22747373; Fax: 0098 21 22721150; E-mail: moghaddasi@sbmu.ac.ir

destruction if it is to be properly exploited by users [1].

Since the very early days, when writing and information exchange started, all human beings, particularly the rulers and military commanders sought new ways to protect the information and to detect information tampering [2 - 6].

Cryptography, a method of making data confidential, for example, was sed to make the message unintelligible to people other than the intended receiver. Cryptography dates back to nearly 2000 B.C. in Egypt, where hieroglyphics were used to decorate the tombs of the deceased rulers and kings [6 - 9].

Data security cannot be solely limited to information and communication technology (ICT) although the technology has played a significant role in taking the information system to work places and commercial exchanges, resulting in the greater dependence of governments and other organizations on electronic information. Rather, work places and commercial exchanges have also been very influential in developing people's individual and social life. Hence, similar to the ICT, work places should also receive special attention in securing their relevant information [10 - 14].

Along with the penetration of information technology in man's life, a lot of effort has been made to achieve data security within and between systems [6], mainly due to the tricky nature of information and communication technology, particularly when such technology turns out to be abstract in nature. ICT-related tools and equipment are not independent of penetrability rules and influences [4].

Since 1940, simultaneously with World War II, the need for developing confidential data increased resulting in widespread application of 'Enigma' machine for cryptography in battle fields by Germans. At this time the first generation of computers made the production of sophisticated cryptography possible resulting in greater data security [4, 15]. The noticeable point is that, with greater demand for effective communication between information systems, via data integration, the need for data security in information systems increased significantly.

In the field of communication, the presence of information system is inevitable. Such systems function as nodes which exchange information by sending and receiving data. The exchange of information between information systems and the circulation of such information within the system itself would involve the application of security systems for safeguarding the data. Considering such issues, the current study is intended to evaluate theories and models dealing with data security, with an emphasis on the fact that the issue of data security and data security management are two separate, but interrelated, subjects which have not been sufficiently investigated thus far.

BACKGROUND

With the expansion of information and communication technology in the 1980s, data security faced new challenges. Before this *era*, the security issue was trusted upon and left to multiuser computers or, in a sense, to machines which were limited in number. However, since the mid 1980s, with the spread of cheap software and hardware, data invasion increased, resulting in a security shift from computers to the data themselves. This decade marked the beginning of fresh discussions on data confidentiality, data integrity, and on-time data availability for the user. To this end, Saltzer and Schroeder (1975) referred to three types of invasion, from the perspectives of security specialists, known as (a) unauthorized information release (Confidentiality), (b) unauthorized information modification (Integrity) and (c) unauthorized denial of use (Availability). Before this *era*, data security was confined to military environments and was supported by the military men, but from 1980s computers entered the field of commerce. Commercial fields differed from military environments in numerous ways of which the most important were the costs incurred to achieve data security, lack of strict physical data support in commercial settings and attacks initiated by unprofessional users in such settings. Such differences resulted in changes in priorities set up for data security in commercial settings [16, 17].

The following section introduces a number of models known as data security models. The models deal with management in data security, in line with the objectives of this study.

The Confidentiality, Integrity and Availability Model

In 1987 Clark and Wilson presented the confidentiality, integrity and availability (CIA) Triad Model [17 - 20]. In this model, integrity means guarding against destruction or improper information modification. Confidentiality means preserving authorized restrictions in getting access to the information while allowing its legal disclosure only. Availability means ensuring timely and reliable access to the information [20]. The issue of “availability” was further highlighted in 1990s with the introduction of more on-line facilities in the market. In 1988, the first attack, of “service deprivation” type, was launched by an internet worm called Morris Worm which significantly changed our overall

perception of security and reliability of the Internet; such attacks ultimately secured the position of “availability” in data security definitions [17].

Parkerian Hexad Model

Donn B. Parker (1998) added three additional non-overlapping attributes of information to the CIA triad of confidentiality, integrity and availability [17, 21, 22]. The three newly added attributes, in the Parkerian Hexad model, were called possession, authenticity and utility. In this model, 'confidentiality' refers to limits on the individual and the type of information he can retrieve. 'Integrity' refers to being correct or consistent with the intended state of information. 'Availability' means having timely access to the information. 'Possession' means having control or ownership of the information. 'Authenticity' refers to correct labeling or attribution of information and 'utility' refers to usefulness of the information [20, 22].

The Five Pillars of Information Assurance Model

More than two decades after the development of computer networks, special attention was paid to the security of information systems. Accordingly, in 2002, the Five Pillars of Information Assurance model was introduced by the U.S. Department of Defense (DoD). This model presents five concepts of confidentiality, integrity, availability, non-repudiation and authentication to achieve 'information assurance' [23]. In this model, according to the 'confidentiality' attribute, the information should not have been disclosed to individuals, or unauthorized bodies or systems. Authenticity is the attribute of being authentic or of established authority for truth and correctness – being genuine, not fabricated. 'Availability' here also means the users' timely and reliable access to information. In non-repudiation attribute the sender assures that the data is taken to the receiver and the identity of the sender is clear to the receiver; as such, the truth of the processed information cannot be repudiated. Security principles will be used to approve identities and to validate the communication process [24].

International Organization for Standardization Model

In 2004, International Organization for Standardization (ISO) proposed a model, commonly referred to as “7 ISO principles”, for data security with seven principles of confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability. According to Confidentiality, the information should not be made accessible or disclosed to unauthorized individuals, entities, or processes. Integrity is the property of safeguarding the accuracy and completeness of assets; availability means the property of being accessible and usable upon demand by an authorized entity; non-repudiation means the ability to prove the occurrence of an action in such a way that the action cannot be repudiated later; accountability denotes the property which ensures that the identity of the individual, with any type of action, in the information system can be traced; authenticity refers to entities such as users, processes, systems and information. Reliability means consistency in the intended behaviors and results [20].

The Traditional 4-Steps Model and the Pentagon of Trust Model

In 2005 Piscitello proposed a model known as 'Pentagon of Trust' which added up the attribute of 'admissibility' to a previously developed model called 'Traditional 4-Steps'. The main features of Traditional 4-Steps Model include confidentiality, integrity, authenticity and availability. 'Admissibility' here refers to a state in which the status of the data is acceptable or lawful [20].

The Evolutionary Circles of Information Security Model

In this model, developed by Cherdantseva and Hilton (2012), fourteen features or attributes are considered for data security, within five evolutionary circles of information security, as follows: reliability, confidentiality, availability, integrity, possession, usefulness, authenticity, non-repudiation, accountability, transparency, auditability, privacy, efficiency and cost-effectiveness. According to designers of this model, security has currently enhanced in meaning, from an elementary concept limited to technical staff to an advanced concept handled by high rank managers. Also, given that the ultimate goal of the organization's leadership is a secure and efficient business, the application of concepts such as validity (meaning compatibility with realities), and accuracy of information is necessary to enhance integrity and authenticity of data. Due to some essential requirements in commerce, new concepts such as transparency, auditability, privacy, efficiency and cost-effectiveness have been added to the goals of data security. Such concepts have accordingly formed some of the features of data security [17].

The noticeable point is that, for some reasons that will be referred to later, the difference between data security and data management has been left unattended thus far. The definitions presented before do not show any significant difference between the two concepts; previous definitions have viewed both concepts as data protection processes [25 - 27]. Besides, all the previous models, discussed in the current work, have solely focused on data security management attributes.

DISCUSSION

The term 'security' would imply a state or condition in which the integrity of an entity is not biased; as such, the entity should remain immune against threats, risks and damages [28 - 35]. Hence, data security is used to refer to a condition in which the integrity of information remains fixed or free from any bias.

Of course, due to its unique nature, information should be exchanged between the sender and receiver, in a communication process; in other words, information is generated in order to be used and exchanged even when the conditional use of classified information by specific users is at the stake. So the senders' and receivers' identity, along with information integrity, belong to attributes that can protect the security of information if they are not biased or distorted.

Anyway, in a normal condition, when there is no particular threat to the integrity of information, data security tends to focus on three characteristics of integrity, identity of the sender and identity of receiver. From quality perspective also data security includes these three attributes.

Of course, it is worth mentioning that, like man's other valuable belongings, information may be stolen, distorted or invaded by individuals or social groups to achieve their illegal interests. Therefore, information security is in need of proper management to remain protected against any kind of threat, theft, robbery or distortion. Also, data security management would involve the process of protecting the integrity of information and the identity of senders and receivers against any sorts of damage, invasion or risks. As such, data security is a condition or state could be achieved by proper management. Fig. (**1**) illustrates the needs for and improvement cycle of data security and its management.

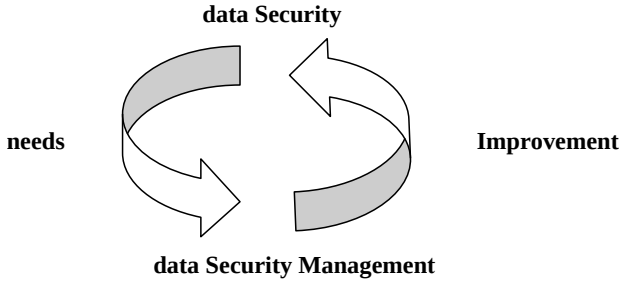

Fig. (1). The needs for and improvement cycle of data Security Management.

Attention to differences between data security and data security management is essential not only in terms of terminology but also in relation to the quality issue because data security and data security management are two separate but interrelated subjects which need continuous improvement. Therefore the proposed models (*i.e.* the CIA Triad, Parkerian Hexad, Five Pillars Information Assurance, 7 ISO principles, Traditional 4-Steps, Pentagon of Trust and Evolutionary Circles of Information Security) are viewed as data security management models. Table **1** depicts these models and their related attributes.

Table 1. Characteristics of data security models.

Model's Name Features	CIA Triad Model	Parkerian Hexad Model	Five Pillar Information Assurance	7ISO principles	Traditional 4-Steps	Pentagon of Trust	Evolutionary Circles of Information Security
Confidentiality	■	■	■	■	■	■	■
Integrity	■	■	■	■	■	■	■
Availability	■	■	■	■	■	■	■
Authenticity		■		■	■	■	■
Admissibility						■	
Non-Repudiation			■	■			■
Authentication			■				

(Table 1) contd.....

Model's Name Features	CIA Triad Model	Parkerian Hexad Model	Five Pillar Information Assurance	7ISO principles	Traditional 4-Steps	Pentagon of Trust	Evolutionary Circles of Information Security
Possession		■					■
Utility		■					■
Reliability				■			■
Accountability				■			■
Transparency							■
Auditability							■
Privacy							■
Efficiency							■
Cost-effectiveness							■

As the models under study indicate, data security management, in an unlimited evolutionary process, in line with other developments in information technology, would gradually build up new attributes with greater capabilities to achieve data security. In addition to its direct link with developments in the knowledge of Intrusion Detection System, data security management, with invaluable capabilities, has been able to extend its features, as a support umbrella, to safeguard data security. These features or characteristics, that are continuously increasing in number, unanimously highlight the role of control and assurance; their current characteristics appear in the **box** below:

Features	**province**
Private zone	integrity attributes
Confidentiality	three features of data security
Accessibility	three features of data security
Non-repudiation	the identity of receiver and sender
Possession	three features of data security
Accountability	three features of data security
Authenticity	three features of data security
Identity confirmation	identity of receiver and sender
Auditability	three features of data security

Here, a graphic representation of data security management, in the form of a model, may help to get a better sense of the way it functions in supporting data security. As such, the following figure, known as 'support umbrella model, is used to clarify the supportive role played by data security management to secure data.

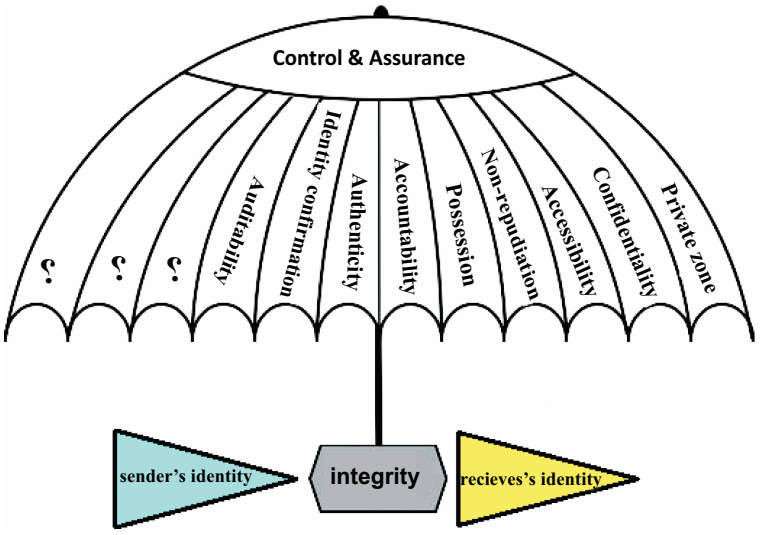

Fig. (2). A support umbrella model for data security management.

Fig. (**2**) a support umbrella model for data security management with capabilities for further extension. The noticeable point is that, the suggested model ted to use the accessibility feature, instead of availability, because accessibility is essential for quick access to reliable data. Besides, the three features of utility, admissibility and transparency are not included in the new model because, according to their definitions, they could be achieved during

the process of data development and management as they do not belong to data management security. The efficiency feature and cost-effectiveness also are not included in the support umbrella model of data security management because, in management, the optimal use of resources, with minimum losses, is of special significance. Also, the realization of these two features (*i.e.* efficiency and cost-effectiveness) will not affect on data security, as attention to them is inevitable in any kind of management, including data security management.

CONCLUSION

Exact definitions of the concepts could help different people to have similar understanding of the terms, as an essential requirement for effective communication. Proper definitions are additionally important for investigating the quality of the concepts and phenomenon. Also, identification of the precise characteristics of different phenomena and concepts is at the stake of accurate definitions.

Making a distinction between the concepts of data security and data security management is an important requirement which has been left unattended thus far although proper attention to such concepts could enhance quality. A noticeable point is that, along with new developments in information and communication technologies and novel advances in intrusion detection systems, data security management would continuously progress resulting in the development of more features in the management.

Data security management is a process which involves the implementation of certain measures to achieve data security as a condition in which, the integrity of data and the identity of the sender and recipient are properly established. In this regard, the introduction of a model that matches the definitions of the two concepts of data security and data security management is of special importance, because such a model could help to identify the services and facilities that are necessary for information security which, in turn, could facilitate the development of information security management.

Attention to differences between data security and data security management by international organizations like ISO, ITU, ASTM and IEEE, with long-time experience on data security and very effective roles in establishing internationally valid standards, could help to formulate more accurate studies to enhance the quality of work in both areas.

AUTHORSHIP CONTRIBUTION

Hamid Moghaddasi proposed the topic; suggested the Umbrella model; and the Need - Improvement cycle theory, formulated research problem and helped with the methodology.

Mehran Kamkarhaghighi collected the data and carried out statistical analyses.

Samad Sajjadi reviewed the literature.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] Kabay M. What's Important for Information Security: A Manager's Guide 2000. [Internet] [cited 2015 March 5]; Available from: http://www.mekabay.com/infosecmgmt/mgrguidesec.pdf.

[2] Agnesse A. Stream Ciphers: from Correlation Attacks to the Cube Attack Thesis. Italy, Rome: Universit'a degli Studi Roma Tre 2007-2008.

[3] Churchhouse RF. Codes and ciphers: Julius Caesar, the Enigma, and the internet. United Kingdom: Cambridge University Press 2001. [http://dx.doi.org/10.1017/CBO9780511542978]

[4] Dlamini MT, Eloff JH, Eloff MM. Information security: The moving target. Comput Secur 2009; 28(3): 189-98.

[5] Holvast J. History of privacy. In: Matyas VV, Fischer-Hübner S, Cvrcek D, Švenda P, Eds. IFIP Summer School on the Future of Identity in the Information Society. Berlin Heidelberg: Springer-Verlag 2008; pp. 13-42. [http://dx.doi.org/10.1007/978-3-642-03315-5_2]

[6] Information Security. Wikipedia: The Free Encyclopedia [Internet]: Wikimedia Foundation, Inc. [updated 2015 May] [cited 2015 May 27]; Available from: https://en.wikipedia.org/wiki/Information_security

[7] Menezes AJ, van Oorschot PC, Vanstone SA. Handbook of Applied Cryptography. United States: CRC Press 1996.

[8] Cohen F. Cryptographic Protection: A short history of cryptography Introductory Information Protection. United State: ITU Press 1995.

[9] Denning DE, Denning PJ. Data security. ACM Comput Surv 1979; 11(3): 227-49.

[10] Baskerville R. Information systems security design methods: implications for information systems development. ACM Comput Surv 1993; 25(4): 375-414.

[11] Leeson PT, Coyne CJ. The Economics of Computer Hacking. JL Econ Pol'y 2005; 2(1): 511-32.

[12] Loch KD, Carr HH, Warkentin ME. Threats to information systems: today's reality, yesterday's understanding. MIS Q 1992; 16(2): 173-86.

[13] Saltzer JH, Schroeder MD. The protection of information in computer systems. Proc IEEE 1975; 63(9): 1278-308.

[14] Yeh Q-J, Chang AJ-T. Threats and countermeasures for information system security: A cross-industry study. Inform Manag 2007; 44(5): 480-91.

[15] Schechter S. The effects of military and other government spending on the computer industry: The early years. Santa Monica, CA: RAND Corporation 1989.

[16] Kumar S. Classification and detection of computer intrusions. United States: Purdue University 1995.

[17] Cherdantseva Y, Hilton J. The Evolution of Information Security Goals from the 1960s to today. [Internet]: Cardif University; 2012 [cited 2015 May 10]; Available from: https://users.cs.cf.ac.uk/Y.V.Cherdantseva/LectureEvolutionInfoSecGOALS.pdf.

[18] Clark DD, Wilson DR. A comparison of commercial and military computer security policies. Security and Privacy, IEEE Symposium on 1987 Apr 27 IEEE 1987; 184-94.
[http://dx.doi.org/10.1109/SP.1987.10001]

[19] Stallings W. Cryptography and network security: principles and prac ces. 4th ed. United States: Prentice Hall 2005.

[20] Steichen P. Principles and fundamentals of security methodologies of information systems Introduction. [Internet] 2012 [cited 2015 March 17]; Available from: https://www. scribd.com/document/48899546/ISO-IEC-27002 -2005.

[21] Khosravi M. Security policy development for SME. [Internet] 2012 [cited 2015 May 4]; Available from: http://www.majidkhosravi.com/security-policy-development/

[22] Marzigliano L. Advice: Security *vs*. Utility. [Internet] 2013 [cited 2015 May 12]; Available from: http://www.zigthis.com/145.

[23] Dardick G. Australian Digital Forensics Conference: Cyber forensics assurance School of Computer and Information Science [Internet]. Perth, Western Australia: Edith Cowan University 2010. [cited 2015 May 22]; Available from: http://ro.ecu.edu.au/adf/77/

[24] CNSS Instruc on No. 4009: National Information Assurance[Internet]. United States: Committee on National Security Systems 2010 [cited 2015 May 15]; Available from: http://www.usna.edu/CS/si110arch/si110AY12F/lec/l23/lec.html.

[25] Khosrowpour M. Managing Social and Economic Change with Information Technology. Proceedings of the 5th Information Resources Management Association. International Conference; SanAntonio, Texas: Idea Group Publication 1994.

[26] Nnolim AL. A framework and methodology for information security management. Thesis: Lawrence Technological University 2007.

[27] Ciampa M. Security awareness: Applying practical security in your world. United States: Cengage Learning 2009.

[28] Ferraro A. Electronic commerce: The issues and challenges to creating trust and a positive image in consumer saleson the World Wide Web. First Monday. 1998; 3(6). [Internet] Available from: https://firstmonday.org/ojs/index.php/fm/article/view/601/522

[29] Booth K. Theory of world security. United Kingdom: Cambridge University Press 2007.
[http://dx.doi.org/10.1017/CBO9780511840210]

[30] Shirey R. Internet security glossary, version 2 [Internet]. The IETF Trust; 2007 [cited 2015 May 15]. Available from: https://tools.ietf.org/html/rfc4949

[31] Tadjbakhsh S, Chenoy A. Human security: Concepts and implications. United States: Routledge 2007.

[32] Kissel R. NISTIR 7298: Glossary of key information security terms, Revision 2. United States Department of Commerce: National Institute of Standards and Technology 2013.
[http://dx.doi.org/10.6028/NIST.IR.7298r2]

[33] Whitman M, Mattord HJ. Principles of Information Security. United States: Course Technology Press, Cengage Learning 2012.

[34] Security. Merriam-Webster Online Dictionary[Internet]. Merriam Webster Incorporated; c2015. [cited 2015 May 7]; Available from: http://www.merriam-webster.com/dictionary/security.

[35] Security. Wikipedia: The Free Encyclopedia. [Internet]: Wikimedia Foundation, Inc.; [updated 2015 May; cited 2015 May 27]; Available from: https://en.wikipedia.org/wiki/Security.