Towards a Management Framework to Protect Sensitive Information during Migrations

Olusegun A. AJIGINI
School of Computing, College of Science, Engineering and Technology,
University of South Africa
Pretoria, Gauteng Province, South Africa

John A. VAN DER POLL
School of Computing, College of Science, Engineering and Technology,
University of South Africa
Pretoria, Gauteng Province, South Africa

and

Jan H. KROEZE
School of Computing, College of Science, Engineering and Technology,
University of South Africa
Pretoria, Gauteng Province, South Africa

ABSTRACT

The protection of sensitive information during the migration from one computing platform to another, e.g. from a Proprietary Platform to a Free Open Source Platform remains a challenge. While our aim is to develop a generic framework for platform migrations, in this paper the scope is limited to migrations from a Proprietary Platform to a Free Open Source Software (FOSS) platform. Free Open Source Software (FOSS) is used in government sectors globally and there is a trend to move from Proprietary Software to FOSS both in government and private sectors. In South Africa, the State Information Technology Agency (SITA) has been in the vanguard of migrating from Proprietary Software to FOSS. Generally, sensitive information is information that ought to be protected to safeguard its integrity, confidentiality and availability. Traditional approaches to such protection have an Information Security flavour, but in this paper we argue the case for using a Management Framework to facilitate traditional approaches. The particular challenges and requirements are sourced from the literature and on the strength of these we propose a rudimentary management framework to fulfil such task.

Keywords: Free Open Source Software (FOSS), policy, National governments, sensitive information, migration of systems, framework, management, privacy.

1. INTRODUCTION

The implementation of Free Open Source Software (FOSS) has been spearheaded by many governments globally [37]. The South African (SA) government has been at the forefront of advocating the use of FOSS [24]. Mtsweni and Biermann [37] indicate that a number of governments implemented FOSS on their servers and workstations.

Therefore, there were migrations from Proprietary Software to FOSS performed worldwide. In this paper, our main focus is on establishing a need for developing a management framework to protect sensitive information during the migration from Proprietary Software to FOSS. Such framework will augment and oversee the traditional Information Security approaches.

The layout of the paper follows: Section 2 describes sensitive information using definitions from different authors in the literature. Section 3 focuses on FOSS initiatives, both by the South African Government and Foreign Governments, while Section 4 highlights some security challenges in FOSS. Section 5 presents standard security solutions and also considers the properties of a management framework as an enrichment of existing solutions. Section 6 focuses on the challenges during the Migration from a Proprietary Platform to a FOSS Platform while Section 7 proposes our Rudimentary Management Framework to oversee the processes described in this paper. Conclusions and future work are covered in Section 8.

2. WHAT IS SENSITIVE INFORMATION?

Many authors have defined sensitive information in the literature, e.g. [20], [59], [60] and [33] to name but a few. Table 1 depicts the definitions of sensitive information from different authors.

Table 1. Definitions of sensitive information

Authors	Definitions of sensitive information by each author
Gennotte and Trueman [20]	"information that is protected to increase the probability of a favourable outcome for the person, group, or organisation that controls that information, or to preserve or increase the options for future action or decisions"
ALRC [3]	The Australian Privacy Law & Practice (ALRC) Report 108 defines sensitive information as "information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs, or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices or criminal record."
Thompson and Kaarst-Brown [59]	"information that the owner (the entity that has the right to the information) does not want to reveal to others". They also state that sensitive information is "information that an individual has acquired about a social organisation or from members of that social group which the individual feels must not be made known outside the social organisation".
TJNAF [60]	"information that must have the potential to damage Laboratory, governmental, commercial or private interests if disseminated to persons who do not need the information to perform their jobs".
McCullagh [33]	The European Union defines sensitive data as "the personal data exposing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the health or sex life processed data".
NIST [43]	The US Computer Security Act defines sensitive information as "any information, the loss, misuse, or unauthorised access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled to under section 552a of title 5, US code (the Privacy Act), but which has not been specifically authorised under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defence or foreign policy". The US Computer Security Act of 1987 requires agencies to identify and recognise sensitive systems, conduct computer security training as well as developing computer security plans.
NIH [42]	"Information is considered to be sensitive if the loss of confidentiality, integrity or availability could be expected to have a serious, severe, or catastrophic adverse effect on organizational assets, or individuals".

Using the synthesis in Table 1, we define sensitive information as: Protected information that the owner does not want to reveal to others and not to be divulged outside the organisation as well as Information about an individual's racial or ethnic origin, Criminal Record, Sexual Preferences or Practices and other information that include Political Opinions, Membership of a Political Association, Religious Beliefs or Affiliations, Philosophical Beliefs, Membership of a Professional- or Trade Association, or a Trade Union.

3. FOSS INITIATIVES

Rafiq and Ameen [50] describe FOSS as computer software of which the source code is available under a license that permits users to use, change, and improve the software and to redistribute it in modified or unmodified form. The use of FOSS gained momentum in the last decade in both public and private organisations [65]. Internationally, governments see FOSS as a tool that can assist them to enhance affordable service delivery due to its low cost of implementation and maintenance [38].

3.1 South African Government Initiatives

The South African Cabinet accepted two FOSS policy submissions, one was by the National Advisory Council on Innovation (NACI) in 2002 and the other by the Department of Arts and Culture, Science and Technology in 2003 [66]. The Government IT Officers (GITO) Council FOSS Working Group compiled the 2003 FOSS policy for government (Cabinet Memorandum No. 29 of 2003) and this encouraged the use of FOSS in the SA Government [66].

A FOSS policy was approved by the South African Cabinet in 2007, stipulating that all future software should be based upon open standards and encouraged the migration of current government software to FOSS [19]. A project office that will oversee the implementation of this policy was established by the State Information Technology Agency (SITA) with the Council for Scientific and industrial Research (CSIR) [66].

The South African government started implementing FOSS within its departments since 2006 and has a target of 60% for back-end servers running FOSS [63]. However, the results of a survey conducted by Weilbach and Byrne [66] from November 2007 to March 2008 indicate that FOSS is not (yet) widely deployed within the SA government. They conclude that FOSS implementations in the SA government are rather few.

3.2 Foreign Government Initiatives

According to Miscione and Johnston [35], the Indian Government supports the use of FOSS and has clear policies in this regard. Sharma and Adkins [55] claim that India has implemented many projects in support of FOSS adoption. FOSS implementations have been carried out in many countries, e.g. China [70], Pakistan [50], and the South Americas [21].

The Malaysian government provided comprehensive implementation guidelines for FOSS adoption [58] and about 128 Malaysian state agencies migrated desktop users to FOSS by March 2008 as detailed in the Malaysian Public Sector Open Source Software Master Plan [57].

The Brazilian government also implemented and adopted FOSS [30] and has a large number of FOSS developers and contributors [36]. According to [54], almost 60% of state departments in Brazil were using FOSS in 2005. Shaw [56] pointed out that a group of Brazilian proponents of social change joined the FOSS communities and accelerated FOSS adoption by many Brazilian Government Agencies during the earlier part of the Lula Administration. The competence of IT professional's impacts on the Brazilian FOSS adoption and the use of FOSS in Brazil has sky-rocketed due to the fact that many Brazilian educated professionals are committed to FOSS.

The German government also implemented many FOSS projects: migration from MS Exchange 5.5 to KOLAB [39], migration of 14000 Windows desktop and laptop computers by the Munich Municipality in 2004 to Linux and OpenOffice.org [26], migration of 10,000 desktop machines by the German Foreign Office to FOSS across 300 sites in 2007 [44]. The central Administration of Germany signed an agreement with IBM to supply FOSS products based on Linux at a reduced price [38].

The US Government launched its recovery .gov Website known as Drupal and it was based on an Open Source Content Management System [53].

The British government adopted a policy on FOSS in 2002 [38]. The objectives of this policy include the use of products based on open standards, and avoiding problems of over-dependency on a specific supplier. The policy enhances the use of FOSS in all publicly funded British organisations (Central Government Departments and their Agencies), local governments, non-departmental public institutions, the National Health Service (NHS) and the Educational Sector.

France set up the Agency for Information and Communication Technology (AICTA) in 2001 and it facilitates the use of FOSS by Public Agencies [39].

The Spanish Ministry of Industry, Tourism and Trade gave financial support for FOSS implementation to various government institutions and autonomous administrations [11]. Some FOSS implementations include GNU/Linux, Guaclalinux, Guadainfo, Linkat, Council of Zaragoza, MAX, etc.

4. SECURITY CHALLENGES IN FOSS

While FOSS offers a number of advantages, notably cost efficiency and reduced vendor lock-in [36], it does, however, bring along a number of security concerns.

According to the US National Security Agency (NSA), Linux security has been enhanced to cater for access controls, but they acknowledge that more work is still required to make SE Linux a trusted operating system that meets requirements of governments or corporate users [40].

Some security concerns regarding the migration from Proprietary Platforms to FOSS Platforms are phishing, stealing sensitive information e.g. account details, cookies etc. and getting hacked during the process.

According to the Danish Board of Technology Working Group [13], security in FOSS for e-government includes protection against breaches of secrecy in the content of data communication (e.g. sensitive personal data, members of the public and companies' economic circumstances) and protection against unauthorized access to computers (e.g. destruction of data, hacking of websites, etc.).

From an analysis performed by Mi2g, it was found that Linux-based web server systems were increasingly targeted by system hackers and it was found that in the first 6 months of 2002, there was a 27% increase in successful system attacks [34]. Subsequently, Fitzgerald and Bassett [18] suggested that Open Source Software should not be used by highly security sensitive users and also not for critical systems.

Fitzgerald and Bassett [18] pointed out that much of the debate around FOSS security is about software error fixes and is not about the security implications of the software architecture.

Hussain et al. [23] write that operating systems (Windows, UNIX, Linux, etc.) do not protect sensitive information that is not captured on the screen. Security is a key aspect and an integral part of any software development [61].

Arai and Tanaka [4] have highlighted the importance of information leakage for computer systems handling a company's sensitive information. They furthermore suggest that sensitive information should be encrypted and technology should make it possible to share the decryption key between the users dealing with the sensitive information. There has been an increase in the number of reported cyber frauds and attacks [1].

Rakers [49] stresses that (naturally) the management of sensitive information related to their business ought to be very important to all organisations.

According to Schryen [52], few quantitative models and empirical studies on open source security appear in the literature, e.g. [2], [41], [69]. Schryen [52] did a comprehensive empirical investigation of published vulnerabilities and patches of open source and closed source software packages. He claims that open source and closed source software do not significantly differ in terms of the severity of vulnerabilities, the types of vulnerability disclosures over time and vendors' patching behaviour.

5. ADDRESSING FOSS SECURITY

5.1 Standard Security Solutions

According to Hussain et al. [23], many IS security researchers have concentrated on the development of algorithms and protocols for the encryption, authentication and integrity of data. They maintain that since operating systems (Windows, UNIX, Linux, etc.) do not protect sensitive information by default, three security levels (Low/Medium/High) can be introduced to protect sensitive information.

According to Brin et al. [8], the copying of sensitive files to removable media can be blocked by some tools, also disallowing sensitive files to be included in email attachments by using copy detection techniques.

Ku and Chi [27] point out that a digital rights management system can be used to protect sensitive information by using encryption. Kurita et al. [28] propose a technique to track and control how programs read sensitive information by establishing security policies that grant or deny permissions to output devises, as well as the saving and protection of sensitive data in adherence to such policy.

Arai and Tanaka [4] propose an information flow control model for sharing and protecting sensitive information. They build and segregate program execution environments based on the type of information and grant privileges based on the execution environment.

This section briefly covered the standard ways of resolving security problems during FOSS migration; Section 5.2 motivates the use of a Management Framework in conjunction with existing solutions.

5.2 Properties of a Management Framework

Thompson and Kaarst-Brown [59] have specified the need for research to comprehend human conceptualisations of sensitive information and also to find the difference between sensitive information and other organisational information for security purposes. They maintain that much of the information that may be sensitive is not guided by technology. PoliVec [48] points out that some proposed security solutions need organisations to segregate information based on its sensitivity. Jones [25] stresses that more technology cannot resolve security problems; rather the basic models of security being employed by organisations need to be managed.

Organisations should be able to classify information based on its sensitivity and use such classification to protect sensitive information in their organisations [59]. Some authors e.g. [45], [15] and [47] also emphasised the importance of a classification system for information to perform a sensitivity assessment.

Farrell [16] writes that, despite the fact that some organisations may already have a rough idea of the different protection needs for information in both electronic and manual systems, a need for sensitivity assessment remains. Scholz [51] indicates that when new software systems are being designed and implemented, the security of the system and the network controls ought to be taken into consideration.

The British Standards Institute [9] indicates that organisations need to determine which information requires the most protection and which may require less protection based on the sensitivity of the information. They emphasise the importance of a classification system to realise this goal. Farrell [16] suggests that organisations must perform sensitivity assessments to elicit the different protection needs for information in both electronic and manual systems.

Liddy [31] indicates that business rules should be examined to provide a basis for information categorisation with respect to sensitivity.

Biot-Paquerot and Hasnaoui [6] indicate that confidentiality, integrity, identifying authorised uses, monitoring access and the flow of information and knowing where information is at any point in time are important aspects when dealing with the core of a security program that protects sensitive information.

Cate [10] suggests five steps for universities to manage their sensitive information: commitment to privacy and security; implementing protection tools and training; stopping collecting data for the sake of data collection; creation of executive leadership with resources to manage sensitive information and getting involved in the legal debate on privacy rights.

Augustinos [5] proposes the following to safeguard sensitive information: develop and implement policies and procedures to protect sensitive information; assess organisational data with a dedicated data security team; enforce hardware and software standards to eliminate unknown factors that assess sensitive information; educate employees, validate the people and systems and update the program with changes as needed; and mitigate risk by adopting insurance coverage.

Ma et al. [32] indicate four guiding principles to manage sensitive information: develop a clear objective; align the objective with organisational strategy; use multiple methods to accomplish the objective and understand and plan for change.

Rakers [49] highlights that managing sensitive information involves people, technology and information, but the people are the most critical component, yet it is the most neglected part when managing sensitive information. Lacey [29] argues that there should be a focus on policies, processes and technology when managing sensitive information.

Changes in employee awareness, attitude and behaviour should be facilitated. The view of Da Veiga [12] is that employee behaviour should be focused on when managing sensitive information.

Pearson [46] advises organisations to value accountability when handling data and build mechanisms for accountable and responsible decision-making. He maintains that obligations to protect data must be observed by all who process data, independent of where such processing occurs.

The overall goal is to decrease privacy risk and as with security, it is necessary to take this into consideration from the outset of the migration process and not just add privacy mechanisms at a later stage.

Thompson and Kaarst-Brown [59] suggest the use of a management framework for protecting sensitive information during software systems design and implementation. In this paper we argue the same case, but for the protection of sensitive information during platform migration. The building blocks of such a framework are presented next.

Table 2. Building Blocks for a Management Framework

Component in framework	Author(s)	Suggestion or Challenge Noted
Classify and Categorise sensitive data / Develop a Data Classification System.	Thompson and Kaarst-Brown [59]	Suggest that organisations should classify and categorise sensitive information based on the behaviours of people in organisations.
	PoliVec [48]	Suggests that organisations should segregate information based on their sensitivity.
	British Standards Institute [9]	A classification system is needed to address security issues.
Address the basic Models of Security within an organisation.	Jones [25]	Suggests more technology cannot resolve security problems but basic models of security employed by organisations ought to be addressed.

Commit to Privacy and Security by the organisation / Deploy Protection Tools to protect sensitive data / Assign Executive Leadership to manage sensitive information.	Cate [10]	Points out the 5 steps to manage sensitive information: commitment to privacy and security; protection tools; no unnecessary data collection; executive leadership to manage sensitive information and participation in legal debates.
Assess the Organisational Data / Enforce Hardware and Software Standards.	Augustinos [5]	Suggests ways to protect sensitive information: Policies and Procedures; organisational data assessment; hardware and software standards enforcement
Train users on how to handle sensitive information.	Da Veiga [12] and Augustinos [5]	Focuses on employee behaviour, employee training; systems/people validation and risk mitigation.
Perform a sensitivity assessment.	Farrell [16]	Suggests organisations ought to perform sensitivity assessment to identify different protection needs for information.
Understand the business rules.	Liddy [31]	Indicates business rules should be examined to provide a basis for information classification with respect to sensitivity.
Consider confidentiality, integrity, identifying authorized uses, monitoring access and the flow of information.	Biot-Paquerot and Hasnaoui [6]	Indicate that confidentiality, integrity, identifying authorised uses, monitoring access and the flow of information and knowing where information is at any point in time.
Guiding principles	Ma et al. [32]	Indicate 4 guiding principles to manage sensitive information: develop a clear objective; align the objective with organisational strategy; use multiple methods to accomplish the objective and understand and plan for change.
Focus on policies, processes, technology, a change in employee awareness, attitude and behaviour.	Augustinos [5] Lacey [29] Rakers [49]	Suggests 5 ways to protect sensitive information and one of them is Policies and Procedures. Argues there should be a focus on policies, processes, technology, a change in employee awareness, attitude and behaviour. Points out that there are 3 primary aspects when managing sensitive information and these are people, technology and information.
Value accountability and build mechanisms for accountable and responsible decision-making.	Pearson [46]	Advises organisations to value accountability when handling data. Build mechanisms for accountable and responsible decision-making.

To protect sensitive information during the Migration from a Proprietary- to a FOSS platform, we suggest the development of a Management Framework with building blocks as indicated in Table 2: Develop sensitive information policies and procedures; Know what sensitive information you have to migrate [17]; Classify the information to be migrated [59]; Encrypt sensitive information stored or transmitted electronically; Keep only the sensitive information you need and comprehensively destroy sensitive information when no longer needed [17]; Train users (Managers/Developers/Analysts etc.) who will migrate the sensitive information; Use Privacy-Enhanced Technologies; Develop a response plan to a security breach of sensitive information [17].

6. CHALLENGES DURING THE MIGRATION FROM PROPRIETARY TO FOSS PLATFORM

Van Belle et al. [62] identified the following obstacles in migrating to FOSS:

(a) Non-availability of (little) published guidance on how to migrate from proprietary to FOSS.
(b) Difficulty in getting qualified staff to support and maintain FOSS.
(c) Availability of very few resellers of FOSS, especially in developing countries.
(d) Lack of technical support due to the availability of very few OSS certification programs for Information Technology support professionals.

The following Challenges during the Migration from a Proprietary Platform to a FOSS platform have been highlighted by ElHag and Abushama [14] (continuing the above list):

(e) Usability: FOSS Development might not use user-centred design or established Software Engineering methods.
(f) Security: Security risks and errors in FOSS are detected rapidly and because the source code is open to the public, the process of eliminating errors is also rapid. However, metrics for measuring software security for real time and mission critical software may be hard to come by.
(g) Data Migration: Data should be divided into categories of critical importance and according to the cost involved in collecting, organising and maintaining it.
(h) Software Development Service and Support: Naturally, the success of a FOSS development project is not guaranteed. Such FOSS implementations depend on the type of the software development service required and also the vendor providing the software development support.
(i) Interoperability and Integration: The new FOSS software may need to integrate with other, already installed, operational software and this might not be feasible due to vendor independence of FOSS. The FOSS implementation might not have taken into consideration the interoperability with other, already installed, operational software.
(j) FOSS Code Maintenance and Management: Fault detection and correction might not have been performed and finished in the FOSS development environment before the software is ported to a live environment. This might lead to developers not using their resources efficiently to deliver higher quality products in a timely manner, making FOSS Code Maintenance and Management expensive. Organisations should invest in fine-grained comparison and versioning tools to track changes carefully to facilitate knowing the impact of upgrading to a future release.

Bleek and Finck [7] discovered the following challenges during FOSS Migrations (continuing above list):

(k) Organisational frame: In some FOSS developments, developers are paid for their contributions while others are not paid. This has led to some ill-feelings amongst participating developers. They suggest that a new development rhythm should be found and communicated fast enough to meet outside expectations but still accommodate everybody willing to contribute.
(l) Team structure: Since both external and internal contributors want to be recognised, the team has to be integrated and all contributors must be equally valued according to their levels of contribution.
(m) Culture: Cultural values need to be shared by both long-standing and new team members. Paid and unpaid contributions could create a natural divergence and unpaid work has to be clarified and justified beforehand.
(n) Coordination: The challenge resides in communicating with large numbers of users and developers. All work has to be well coordinated and the development process should be transparent to these stakeholders.

7. TOWARDS A RUDIMENTARY MANAGEMENT FRAMEWORK

Our rudimentary Management Framework is synthesised from the building blocks in Table 2 and is illustrated in Figure 1.

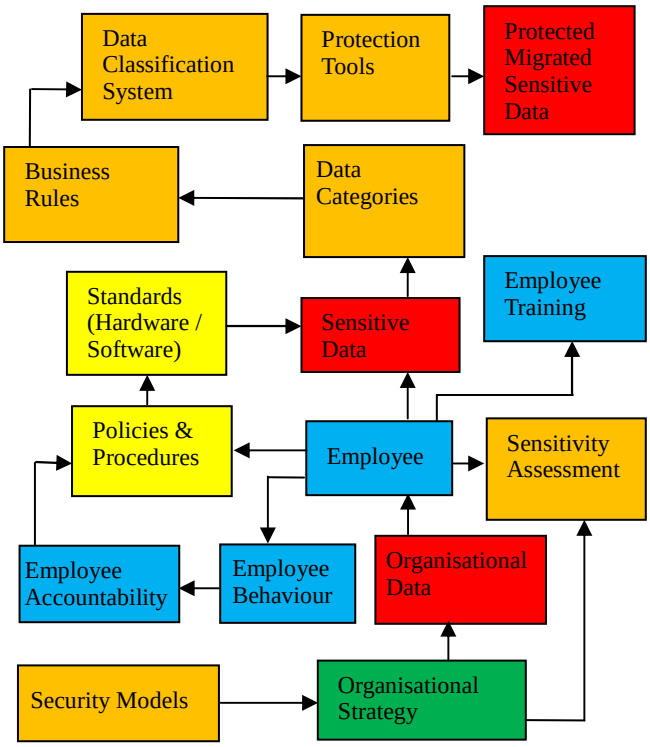

Figure 1. Rudimentary Management Framework

Organisations migrating sensitive information should develop security models to support their organisational strategy. The organisational strategy will incorporate how organisational data will be protected and handled. Organisations ought to develop clear objectives to manage sensitive information through a dedicated Data Security team. Employees handling organisational data should be trained on how to handle sensitive information and the changes in employee awareness, attitude and behaviour ought to be facilitated. Employees need to perform sensitivity assessment as part of the organisational strategy on the protection of their organisational data.

Policies and Procedures on sensitive information need to be developed and enforced by management. Employees should be made accountable to ensure that sensitive information protection is in line with the Policy and Procedures governing sensitive information. Such policies and procedureses should be used to enforce hardware and software standards in order to eliminate unknown factors that assess sensitive information. Data should be categorised into Data Categories using Business Rules and Data Classification System. Data should be categorised into categories of critical importance and in accordance to the cost involved in collecting, organising and maintaining the data. Organisations need to examine Business Rules in order to provide a basis for information categorisation with respect to sensitivity. The information to be migrated need to be classified using the Data Classification System. Sensitive information need to be encrypted using the Data Protection Tools and Privacy-Enhanced Technologies. Organisations need to develop a Response Plan to a security breach of sensitive information.

8. CONCLUSIONS

Although many researchers claim that FOSS platforms have increased security, due to their openness [68], [64], [67], [22], this paper argued in favour of a Management Framework to address the protection of sensitive information in migrating from a Proprietary Platform to a FOSS Platform.

Sensitive information was defined, based on definitions from researchers in the literature. Understanding and being able to identify sensitive information will necessarily facilitate the development of a comprehensive Management Framework to protect such information during system migrations. The desirable properties and the building blocks of such a framework were noted and on the strength of these, a preliminary and high-level framework for sensitive information protection was defined. The standard Information Security approaches to sensitive information protection will form part of, and will be managed by the proposed framework.

Future research should seek to develop several layers of the framework and interactions with the standard, technical processes will be established. A Case Study approach, using multiple case studies in different organisations will form part of the research. It is anticipated that the principles derived from this study could be extrapolated to general migrations in future. The validation of the proposed framework should also receive attention. This framework will be implemented in a governmental organisation as part of future work.

9. ACKNOWLEDGEMENTS

Our thanks go to the University of South Africa for providing funding to undertake this research.

10. REFERENCES

[1] Acello, R. (2009**). Feds ready to tackle Cybercrime**, ABA Journal, 95(2), 37.

[2] Alhazmi, O., and Malaiya, Y., Ray, I. (2007). **Measuring, analyzing and predicting security vulnerabilities in software systems**, Computers & Security, 26(3), pp. 219 – 228.

[3] ALRC (2000). **ALRC Report 108**. Available on www.alrc.gov.au.

[4] Arai, M., and Tanaka, H. (2009). **A Proposal for an Effective Information Flow Control Model for Sharing and Protecting Sensitive Information**, Australasian Information Security Conference (AISC), Wellington, New Zealand. Conferences in Research and practice in Information Technology (CRPIT), Vol. 98. Ljiljana Brankovic and Willy Susilo, Eds.

[5] Augustinos, T. (2009). **Preventing and reacting to a data breach**, Risk Management, 56 (10), 45.

[6] Biot-Paquerot, G., and Hasnaoui, A. (2009). **Stakeholders Perspective and Ethics in Financial Information System**, Journal of Electronic Commerce in Organisations, 7(1), pp. 59 – 70.

[7] Bleek, W., Finck, M. (2011. **Migrating a Development Project to Open Source Software Development**. Available from www.flosshub.org/system/files/bleek10-14.pdf

[8] Brin, S., Davis, J., and Garcia-Molina, H. (1995). **Copy detection mechanisms for digital documents**, Proceedings of the 1995 ACM SIGMOD International Conference on Management of Data, San Jose, CA, USA, May 22 – 25, ACM, pp. 398 – 409.

[9] British Standards Institute (2000). **Information Technology Code of practice for information security management (Standard 0-580-36958-7)**. London: British Standards Institute.

[10] Cate, F. H. (2006). **The Privacy and Security Policy Vacuum in Higher Education**, EDUCAUSE Review, 41(5).

[11] CENATIC, (2008). **Open source software for the Development of the Spanish Public Administration, An overview**. Available from: www.cenatic.es

[12] Da Veiga, A. and Eloff, J. (2010). **A framework and Assessment Instrument for information Security Culture**, Computers & security, 29(2), 196.

[13] Danish Board of Technology Working Group, (2002). **Open Source Software in e-government, a Report on the analysis and recommendations drawn up by a working group under the Danish Board of Technology**.

[14] ElHag, H. M. A., Abushama, H. M. (2009). **Migration to FOSS: Readiness and Challenges**

[15] Eloff, J. H. P., Holbein, R., and Teufel, S. (1996). **Security Classification for documents**, Computers and Security, 15 (1), 55 – 71.

[16] Farrell, G. (2002). **Former Anderson executive to testify**. USA Today, April 10, p.B1.

[17] Federal Trade Commission (FTC) (2009). **Protection Personal Information: A Guide for Business**. Available from: http://www.ftc.gov/infosecurity. Accessed: 2012/02/23.

[18] Fitzgerald, B., and Bassett, G. (2003). **Legal Issues Relating to Free and Open Source Software, Essays in Technology Policy and Law**, vol. 1, Queensland University of Technology, School of Law.

[19] GCIS (2007). **"Cabinet Statement", Feb 22**, available at www.gcis.gov.za/media/cabinet/2007/070222.htm Accessed: 2 February 2012

[20] Gennotte, G., and Trueman, B. (1996). **The strategic timing of corporate disclosures**. Review of Financial Studies, 9 (2), 665 – 690.

[21] Hedgebeth, D. (2007). **Gaining competitive advantage in a knowledge-based economy through the utilization of open source softwar**e, VINE: The Journal of Information and Knowledge Management Systems, Vol. 37, No. 3, pp. 284 – 294.

[22] Hoepman, J., and Jacobs, B. (2007). **Increased Security Through Open Source**, Communications of the ACM, Vol. 50, No. 1

[23] Hussain, K., Addulla, N., Rajan, S., and Moussa, G. (2005). **Preventing the capture of sensitive information**, 43rd ACM Southeast Conference, March 18 – 20, Kennesaw, GA, USA.

[24] Johnston, K. A., and Seymour L. F. (2005). **Why South Africans don't floss?** Proceedings of the International Business Information Management Conference (IBIMA), 438 – 446, July, Lisbon, Portugal.

[25] Jones, A. K. (2002). **Network Security. Paper presented at the Critical Infrastructure and Information Assurance Symposium**, Syracuse, NY.

[26] Kovacs, G. L., Drozdik, S., Zuliani, P., and Succi, G. (2004). **Open source software for the public administration**. Proceedings of the 6th International Workshop on Computer Science and Information Technologies, Budapest, Hungary.

[27] Ku, W., and Chi, C. H. (2004). **Survey on the Technological Aspects of Digital Rights Management**, Proceedings of the 7th International Conference, ISC, Palo Alto, CA, USA, Sept 27 – 29, Springer Berlin / Heidelberg, pp. 391 – 403.

[28] Kurita, H., Shioya, R., Irie, H., Goshima, M., and Sakai, S. (2007). **Dynamic Information flow control for preventing information leakage**, Proceedings of the IPSJ SIG Technical Report, HOKKE, Hokkaido, Japan, March 1 – 2, ARC- 172, IPSJ Press, pp. 227 – 232.

[29] Lacey, D. (2010). **Understanding and transforming organisational security culture**, Information Management & Computer Security, 18(1), 4-13.

[30] Lewis, J. A. (2007). **Government open source policies**. Available from: http://www.csis.org/media/csis/pubs/070820_open_source_policies.pdf. Accessed: 2012/01/29.

[31] Liddy, E. D. (2001**). Information Security and Sharing**. Online Magazine, 28 – 30. Available from: www.cnlp.org/publications/pub.asp

[32] Ma, Q., Schmidt, M., and Pearson, J. (2009). **An integrated framework for Information Security Management**, Review of Business, 30(1), pp. 58 – 69.

[33] Mc Cullagh, K., (2007). **Data Sensitivity: resolving the conundrum**, British & Irish Law, Education and Technology Association Annual Conference, Hertfordshire 16 - 17 April.

[34] Mi2g Report, (2002). **Press report** at http://www.zdnet.com.au/newstech/os/story/0,2000024997,20266696,00.htm

[35] Miscione, G., and Johnston, K., (2009). **Free and Open Source Software in developing contexts, From open in principle to open in the consequences**, Journal of Information, Communication & Ethics in Society, Vol. 8, No. 1, pp. 42 – 56.

[36] Mtsweni, J., and Biermann, E. (2008). **An investigation into the implementation of open source software within the SA government: An emerging expansion model**. SAICSIT, 6 – 8 October, Wilderness Beach Hotel, Wilderness, SA.

[37] Mtsweni, J., and Biermann, E. (2010). **A Roadmap to proliferate Open Source Software Usage within SA Government Servers**, IEEE Computer Society.

[38] Mutula, S., and Kalaote, T. (2010). **Open source software deployment in the public sector: a review of Botswana and South Africa**, Emerald, Vol. 28, No. 1, pp. 63 – 80.

[39] Nagler, M. (2005). **Open Source adoption of the German Federal Office for Information Security**. Available from: http://ec.europa.eu/idabc/servelets/Doc?id=21394. Accessed: 2012/01/25.

[40] NSA (National Security Agency), (2001). **Response #19** at www.nsa.gov/selinux/faq.html

[41] Neuhaus, S., Zimmermann, T., Holler, C., and Zeller, A. (2007). **Predicting vulnerable software components**, In Proceedings of the 14th ACM Conference on Computer and Communications Security, Alexandria VA, Oct. pp. 529 – 540.

[42] NIH (2008). **Guide for identifying sensitive information**. Available on http://irm.cit.nih.gov/security/NIH_sensitive_info_Guide.doc

[43] NIST (2008). **An Introduction to Computer Security, The NIST Handbook**. Text from: http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter1-printable.html. Accessed on 09/03/2012.

[44] Otter, A. (2007). **SA government gets serious about ODF, IOIL Technology**. Available from: http://www.ioltechnology.co.za/article_page.php?iArticleId=4126700&iSectionId=2888. Accessed; 2012/02/21.

[45] Parker, D. B. (1996). **Classification of information to protect it from loss**. Information systems security, 5 (2), 9 – 15.

[46] Pearson, S. (2009). **Taking Account of Privacy when Designing Cloud Computing Services**, CLOUD '09, IEEE, May 23, Vancouver, Canada.

[47] Peltier, T. R. (1998). **Information Classification**. Information Systems Security, 7 (3), 31 – 43.

[48] Polivec, (2002). **Security policy development process**. Colorado Springs, CO: PoliVec Inc.

[49] Rakers, J. (2010). **Managing Professional and Personal Sensitive Information**, SIGUCCS, October 24 – 27, Norfolk, Virginia, USA.

[50] Rafiq, M., and Ameen, K. (2009). **Issues and lessons learned in open source software adoption in Pakistani libraries**, The Electronic Library, Vol. 27, No. 4, pp. 601 – 610.

[51] Scholz, C. (1990). **The symbolic value of computerized information systems**, In P. Gagliardi (Ed.) Secrecy (pp. 161 – 177), New York: Human Sciences.

[52] Schryen G. (2011). **Is Open Source Security a Myth? What does vulnerability and patch data say?** Communications of the ACM, May, Vol. 54, No. 5.

[53] Scola, N. (2009). **Why the White House's embrace of Drupal matters**. Personal Democracy Forum techPresident.

[54] SERPRO (2005). **Fast move to Free Software in Brazil**. Available from: http://ec.europa.eu/idabc/en/documents/5131/528. Accessed: 2012/01/20.

[55] Sharma, A., and Adkins, R. (2006). **OSS in India**, in DiBona, C., Cooper, D. and Stone, M. (Eds.), Open Sources 2.0, O'Reilly Media, Sebastopol, CA, pp. 189 - 196.

[56] Shaw, A. (2011). **Insurgent expertise: The politics of free/live and open source software in Brazil**, Journal of Information Technology & Politics, 8, 253 – 272.

[57] TMPSOSSMP (2008). **The Malaysian Public Sector Open Source Software Master Plan: Phase II – Accelerated Adoption**. Available from http://www.mampu.gov.my/seminar%20ict/kk2-OSS.pdf Accessed: 2012/02/19

[58] Thomas, J. (2007). **Malaysian public sector OSS program phase II: Accelerated Adoption**. Available from: http://www.oscc.org.my/documentation/phase2_launching/OSS-Phase-2Strategy-Plan-Launch.pdf [Accessed: 2012/02/18].

[59] Thompson, E. D., and Kaarst-Brown, M. L. (2005). **Sensitive Information: A Review and Research Agenda**, Journal of the American Society for Information Science and Technology, 56(3), 245 – 257.

[60] TJNAF (2007). **Security Plan for protection of sensitive information**, Thomas Jefferson National Accelerator Facility.

[61] Vadalasetty, S. R. (2009). **Security Concerns in Using Open Source Software for Enterprise Requirements**, SANS Institute InfoSec Reading Room.

[62] Van Belle, J., Brink, D., Roos, L., Weller, J. (2006). **Migrating to OSS-on-the-Desktop: Lesson Learnt and a Proposed Model**, Proceedings of the 38th Southern Africa Computer Lecturers Association Conference, Somerset West, South Africa, pp. 94 – 107.

[63] Vital Wave, (2006). **The South African adoption of open source**: a white paper created by Vital Wave Consulting available online from www.vitalwaveconsulting.com/insights/South-African-Adoption-of-Open-Source.pdf accessed on 20 February 2012.

[64] Walker, T. (2004). **The future of Open source software in government.** Available from: http://www.oss-institute.org/newspdf/walker_oss_white_paper_2292004.pdf. Accessed 2012/01/24.

[65] Weber, T. (2004). **The Success of Open Source**, Harvard University Press, New York, NY.

[66] Weilbach, L, and Byrne, E. (2010). **A human environmentalist approach to diffusion in ICT policies – A case study of the FOSS policy of the South African Government**, Journal of Information, Communication & Ethics in Society, Vol. 8 No. 1. pp 108 – 123.

[67] Wheeler, D. A. (2005). **Why open source software/free software? Look at the numbers!** Available from: http://www.dwheeler.com/oss_fs_why.html. Accessed: 2012/02/11.

[68] Witten, B., Lanwehr, C., and Caloyannides, M. (2001**). Does open source improve system security?** IEEE Software, Sept – October, pp. 57 – 61.

[69] Woo, S. W., Alhazmi, O. H., and Malaiya, Y. K. (2006). **An analysis of the vulnerability discovery process in Web browsers**. In Proceedings of the 10th International Conference on Software Engineering and Applications, Dallas, TX, Nov. 13 – 15.

[70] Yeo, B., Liu, L., and Saxena, S. (2006). **When China dances with OSS**, in DiBona, C., Cooper, D. and Stone, M. (Eds), Open Sources 2.0, O'Reilly Media, Sebastopol, CA, pp. 197 – 210.