Digital Forensic Readiness as a Component of Information Security Best Practice

CP Grobler[1], CP Louwrens[2]
1 University of Johannesburg, Department of Business IT, Bunting Road Auklandpark, Johannesburg, South Africa
tgrobler@uj.ac.za,

2 Nedbank, South Africa
buksl@nedbank.co.za

Abstract. In a world where cyber crime is constantly increasing, pervasive computing is on the rise and information is becoming the most sought after commodity making an effective and efficient Information Security (IS) architecture and program essential. 'With this improved technology and infrastructure, ongoing and pro-active computer investigations are now a mandatory component of the IS enterprise' [16]. Corporate governance reports require that organizations should not only apply good corporate governance principles, but also practice good IT governance and specially IS governance. Organizations develop their security architectures based on current best practices for example IS017799 [21] and Cobit [12]. These best practices do not consider the importance of putting controls or procedures in place that will ensure successful investigations. There is a definite need to adapt current Information Security (IS) best practices to include for example certain aspects of Digital Forensics (DF) readiness to the current best practices to address the shortcomings. Whilst IS and DF are considered as two different disciplines, there is a definite overlap between the two [29]. The aim of this paper is to examine the overlap between DF and IS, to determine the relevance of DF readiness to IS and propose the inclusion of certain aspects of DF readiness as a component for best practice for IS.

1 Introduction

The Information Security (IS) program of an organization is only as strong as its weakest link. Incidents will occur, but it is essential to link the attacker or source of

Please use the following format when citing this chapter:

Grobler, T. and Louwrens. B., 2007. in IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer), pp. 13–24.

the attack to the attack so that management can make the appropriate decision as to what action to take.

Most of the security incidents do not proceed to legal action, as companies want to proceed with normal business activities as soon as possible [9]. Statistics from the CSI/FBI computer crime survey of 2006 [7] indicate that only 25% of all cases were reported to law enforcement, 15% to legal or regulatory authorities and 70% of the respondents deal with security incidents by patching the holes. Although the ratio is still very high, there has been an improvement in the way organizations deal with the breaches [7]. Reasons for this are that companies want to prevent negative publicity and do not want their competitors to use the incident to gain a competitive advantage.

According to von Solms [28], we are experiencing the fourth wave of IS: Information Security Governance. He defines it as the 'process of the explicit inclusion of IS as an integral part of good Corporate Governance and the maturing of the concept of Information Security Governance'. The result of this wave is that management must take the responsibility and are personally responsible for the security health of their IT systems. These IT systems are the foundation which provide accurate information that managers use to substantiate their every day decisions. There is therefore a need to prove that the IS systems are healthy and should an incident occur, that management must deal with the incident in an appropriate way.

The CSI/FBI 2006 computer crime survey [7] indicates that more than 60% of the respondents have indicated the need to improve the IS posture of the organization as a result of the Sarbarnes–Oxley [26] report. The report has changed the focus of IS from managing technology and people to Corporate Governance and specifically IS Governance.

Many organizations have an Information Security (IS) strategy in place to protect the information and information assets of the organization. This strategy will determine how the organization manages all IS activities in the organization. Computer crime is a very lucrative activity that continues to grow in prevalence and frequency [14]. More and more commercial organizations are using DF technologies to investigate for example fraud, accessing pornography or harassment.

The increase in cyber related criminal activity places a strain on law enforcement and governments. Courts no longer require only document-based evidence but also digital/electronic-based evidence. Criminal investigations require solid, well documented, acceptable procedures and evidence. Normal forensic investigations are no longer suitable or applicable and digital forensic investigations need to be undertaken.

Digital evidence is becoming increasingly prominent in court cases and internal hearings. Network administrators and system administrators want to analyze activities on the networks and applications. Organizations should look at the evidence required so that security programs and architectures can be adapted to provide the evidence when required.

The format of the paper will be to

1 define IS and DF;
2 discuss the overlap between IS and DF;
3 discuss DF readiness;

4 discuss the overlap between DF readiness and IS and
5 propose DF readiness as a best practice for IS.

The next part of the paper will define IS and DF and discuss the overlap between DF and IS.

2 Digital Forensics and Information Security

Information Security can be defined as the process of protecting information and information assets from a wide range of threats in order to ensure business continuity, minimize business damage, maximize return on investments and business opportunities by preserving confidentiality, integrity and availability of information [21].

Forensics is the use of science and technology to investigate and establish facts in criminal and civil courts of law [1]. The goal of any forensic investigation will be to prosecute the criminal or offender successfully, determine the root cause of an event and determine who was responsible.

The environment in which digital crimes are committed has changed drastically with the emergence of digital devices e.g. digital fax, the internet and wireless devices. It is no longer sufficient to only investigate the hard drive of the victim's PC (computer forensics), as there will be additional evidence required for a successful prosecution. With the emergence of new technologies e.g. wireless communications, PDA's, flash disks and the internet, computer forensics has become a subset of DF. DF is more comprehensive than computer forensics. Cyber-trained defense attorneys require the chain of evidence that must link the attacker to the victim [24].

DF can be defined as the efficient use of analytical and investigative techniques for the preservation, identification, extraction, documentation, analysis and interpretation of computer media which is digitally stored or encoded for evidentiary and / or root-cause analysis and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations [14, 4, 18, 23, 20].

DF is a new discipline that will become more relevant and essential as it becomes the vehicle for organizations to assess the effectiveness of controls implemented and to determine the root-cause of an incident. These controls can be typically security controls.

Traditionally an organization will conduct a DF investigation once a security breach is encountered, but DF can be conducted in a pro-active as well as a re-active manner. Re-active forensic investigations will occur after an incident has taken place. Most of the current investigations are re-active. Typically an investigation will focus upon the legal and law enforcement aspects of an incident or it will be used to determine the root-cause that instigated the incident [24].

Pro-active DF will enable an organisation to become DF ready. DF readiness can be defined as the ability of an organization to maximise its potential to use digital evidence whilst minimising the costs of an investigation [20].

It is essential to determine what evidence is required should an incident occur. The authors propose that organizations have pro-active evidence. Pro-active evidence can be defined as evidence that will have evidentiary weight in a court of law and contain all the evidence necessary (relevant and sufficient) to determine the root-cause of the event, link the attacker to the incident and will result in a successful prosecution of the perpetrator.

The Electronic Communications and Transactions Act of South Africa (ECT) [25] have the following requirements for determining the admissibility of a digital document or digital evidence in a court of law: The reliability of the manner in which the record was communicated and stored, how the integrity of the data was maintained, and the manner in which the originator / author of the record is identified.

IS can also be pro-active and re-active. Pro-active IS will ensure that appropriate controls e.g. policies are in place to prevent attacks or security breaches. Re-active IS will ensure that organizations can resume operations as soon as possible whilst minimising the damage.

The authors have compared IS and DF in

Table 1. The aim of this comparison will be to identify potential areas where DF and IS overlap.

Table 1 Comparison of IS and DF

	Information Security	**Digital Forensics**
Pro-active	**Purpose:** Prevent damage to information and information resources by applying the most effective and efficient controls for the identified threats by the organization	**Purpose: (two fold)** Ensure that all processes, procedures, technologies and appropriate legal admissible evidence is in place to enable a successful investigation, with minimal disruption of business activities Use DF technology to determine the 'holes' in the security posture of the organization
	How: IS policies, e.g. incident recognition, Implement IS procedures and mechanisms Determine legal requirements IS Awareness and training	**How:** DF policies, e.g. evidence preservation DF readiness, e.g. prevent anonymous activities, secure storage of logs, hashing etc. Determine legal requirements DF awareness and training
Re-active	**Purpose:** Ensure that the damage that has occurred from a breach is minimised and prevent further damages	**Purpose:** To investigate an event in a way that the evidence gathered can used to determine the root-cause of an event and successful prosecution of the perpetrator
	How: Incident response plan (IRP) Disaster Recovery Plan (DRP) Business Continuity Plan (BCP)	**How:** Incident response plan (IRP) Disaster recovery plan (DRP) Business Continuity plan (BCP)

	Fix security loophole	Adequate DF processes and techniques

From

Table 1 the authors have identified similar areas between the two disciplines e.g. IRP's, policies and staff training. Both disciplines demonstrate the need for policies, but it may not be the same policy. DF policies may augment some IS policies for example the IS policy for the identification of an incident will be influenced by the DF policy for the preservation of evidence.

DF awareness training will link with IS awareness training for example with first incident response training.

During the IR, DRP and BCP of organizations, the DF process and procedural requirements will influence the way IS plans (IRP, DRP, BCP) are developed. The main aim from a IS perspective will be to resume business as soon as possible and minimise the damage, whereas the DF requirement is to capture and preserve all relevant evidence for prosecution. This can cause a conflict, as normally business does not want to wait for evidence gathering before they resume the operations. Pro-active evidence can allow business to continue with minimal interruption.

DF will influence all stages of the IS management lifecycle: planning, developing, implementing, monitoring and assessing the security posture of the organization. DF techniques are currently used to assess the security posture of the organization, by using for example penetration testing and audits. DF readiness will add the missing controls and procedures to perform a successful investigation to the security posture of the organization.

The relationship between IS and DF is also identified by a study done by Endicott-Popovsky [5]. According to the authors a survivable system consists of 3 R's: *Resistance, Recognition and Recovery.*

- Resistance is defined as the ability to repel attacks. It will deal with firewalls, user authentication, diversification;
- Recognition is defined as the ability to detect an attack coupled with the ability to react or adapt during an attack. It will deal with IDS and internal integrity tests;
- Recovery is defined as the ability to provide essential services during an attack and restore services after an attack. It will deal with incident response, replication, back-up systems and Fault tolerant designs. All 3 R's should be taken care of by the ISA of an organization.

Endicott-Popovsky [5] suggests that a fourth R, *Redress* must be included in the IS Security strategy:

- Redress is defined as the ability to hold intruders accountable in a court of law and the ability to retaliate. It will consider DF techniques, legal remedies and active defense.

The outcome of a 3R strategy will be to recover from the incident as soon as possible by for example applying a suitable patch, whereas the outcome of a 4R strategy will be to gather evidence, restore the system and pursue legal consequences. The 4R strategy therefore includes DF, as you will not be able to take legal action without following the appropriate DF processes.

There is a definite overlap between IS and DF from the discussion above and studies done by Louwrens and von Solms [29]. IS architectures concentrate on

preventing incidents from happening and should an incident occur, the incident response, disaster recovery and business continuity plans focus on recovering as quickly as possible from the incident so that the interruption is minimized and the business can continue. IS will concentrate on confidentiality, integrity and availability of information and information assets and does not consider the preservation of evidence.

DF will ensure that the organization will have the adequate evidence, processes and policies in place to ensure that a successful investigation can be done with minimal disruption in business processes.

DF investigations will enable the organization to find the source of the attack, preserve the evidence and to take appropriate action. DF is concerned with the integrity of the information and processes of the investigation. The result of a DF investigation should be used as input into the security strategy of an organization so that the security posture can improve.

DF must have an influence on the way security is planned, implemented and measured in an organization. DF is perceived as a very expensive exercise [20], but thoughtful planning can combat the costs, for example: an inexpensive way will be to define adequate policies and processes to capture applicable evidence [30, 17].

DF is not only important for the IS management of the organization, but also vital for good Corporate Governance and specifically IS Governance. Corporate Governance reports such as Sarbarnes-Oxley and King II as well as best practices for example ISO17799 and Cobit [27] requires that adequate controls are in place. DF tools and techniques are being used to assist with the assessment of controls.

In the next part of the paper the authors will define DF readiness and discuss the role and importance of DF readiness for an organization.

3 Digital Forensic Readiness

As discussed in the first part of the paper, DF consists of pro-active and re-active components. DF is transforming from an investigation and response mechanism to include a powerful pro-active measure. DF tools are currently used to: collect digital evidence in a legally acceptable format, audit an organization's networks and structure, validate policies and procedures, assist in identifying major risks, prioritize protection of and access to an organization's most valuable data during and investigation and provide training in first response to avoid the contamination of evidence [11].

Management is often wary of the cost implication to become DF ready in an organization. It is essential to convince them of the benefits of DF processes in the organization. These benefits can include the demonstration of due diligence for good corporate governance, useful for data retention and provide protection for the organization against litigation risks.

Pro-active DF management must ensure that all business processes are structured in such a way that essential data and evidence will be retained to ensure successful DF investigations, should an incident occur. Proper pro-active DF management

should minimize interruption to the business processes while conducting an investigation. It is essential that the organization become DF ready.

DF readiness was defined in paragraph 2 of the paper. Another definition is the 'art of maximizing the environment's ability to collect credible evidence' [6].

The organization must identify all possible evidence sources and ways to gather evidence legally and cost-effectively. It will not help just to identify and capture the evidence, but organizations must implement a digital evidence record management system and electronic document management system. The ECT Act [25] prescribes the following conditions for electronic records retention:

- The retained records should be accessible;
- the electronic version should accurately represent the original format and
- meta-data such as author and date should be retained with the record.

The digital evidence management system must enable organizations to identify and manage applicable evidence in an organised way.

According to Rowlingson [20] the goals of forensic readiness are as follows:

- To gather admissible evidence legally and without interfering with business processes;
- To gather evidence targeting the potential crimes and disputes that may adversely impact an organization;
- To allow an investigation to proceed at a cost in proportion to the incident;
- To minimize interruption to the business from any investigation;
- To ensure that evidence makes a positive impact on the outcome of any legal action [20].

The authors want to add the following goals to DF readiness:

- To ensure that the organization practices good corporate governance, specifically IS governance;
- To 'enrich' / augment the security program of the organization to ensure that adequate evidence, processes and procedures are in place to successfully determine the source of an attack;
- Use of DF tools to enhance the IS management of an organization, for example to recover data from a crashed hard drive and
- To prevent the use of anti-forensic strategies for example data destruction or manipulation and data hiding.

The above discussion has indicated that DF readiness is a business requirement in any organization.

4 The overlap: DF readiness and IS

According to Rowlingson [20], DF readiness will concern itself with incident anticipation - instead of incident response - and enabling the business to use digital evidence. Information security will concern itself with ensuring the business utility of information and information assets is maintained – excluding the requirement for digital evidence.

From the discussion in paragraph 3 and Rowlingson's activities for DF readiness [20], the overlap of DF readiness and IS will be in:

- IS and DF awareness training. All IS training programs must be revised to include aspects of DF training. Caution must be taken on what should be included in the IS awareness training, as the curriculum must maintain a balance between necessary awareness and unnecessary information sharing. The result of badly planned curriculums can result in criminals manipulating or tampering with evidence to prevent successful investigations ;
- IS and DF policies. Determine all the IS policies that will need inputs from DF – for example: evidence identification and preservation;
- IS Risk Management where it will include:
    - Assessing the risks by identifying all the business scenarios that will require digital evidence;
    - Determine the vulnerabilities and threats during risk assessment, but also determine what evidence will be required to determine the root–cause of the event, also for more unlikely threats;
    - Determine what information is required for evidence (the format and exactly what is required);
    - Determine how to legally capture and preserve the evidence and integrate it into the legal requirements for the organization. Consider the other legal requirements for example monitoring of activities, interception of communications and privacy;
    - Ensure that monitoring is targeted to detect and deter incidents;
    - Augment the IRP to specify when to escalate to a full investigation;
    - Define the first response guidelines to the IRP to preserve evidence and
    - Determine when and how to activate DRP and BCP;
- Establish an organizational structure with roles and responsibilities to deal with DF in the organization. There should be a clear segregation of duties between the DF and IS teams;
- Establish a digital evidence management program;
- Incorporate DF techniques in the IS auditing procedures, this will enable a more accurate audit that can for example determine the efficiency of a control;
- Access controls should be reviewed to prevent anonymous activities;
- Establish a capability to securely gather admissible evidence by considering technology and human capacity.
- Use DF tools and processes to demonstrate good corporate governance so that for example management can prove that they have tested the adequacy of IS controls;
- Use DF tools for non-forensic purposes to enhance the ISA, for example data recovery if a hard disk crashes;
- Developing a preservation culture in the organization to preserve all processes and activities should an investigation arise;
- Design all security controls to prevent any anti-forensic activities. Typically no password crackers, key-loggers, steganography software etc. should be allowed in the organization and
- Removable / portable devices must be monitored and preferably controlled so that potential cyber crimes can be minimized, for example Intellectual Property theft.

In this part of the paper the authors have identified that there is a big overlap and coherence of activities of DF readiness and IS. This overlap is not necessarily the same activity that takes place, but the way 'how' and 'what' should be done from an IS perspective is influenced by the 'what' that is required of the DF perspective. For example: when setting a policy on first incident response, the policy should not only include the elements to identify an incident and what should be done, but the preservation of evidence must be included in the policy so that no contamination of evidence can take place.

In the next part of the paper the authors will propose DF readiness as a component of an IS best practice.

5 DF Readiness as a component if of IS Best Practice

A best practice is defined as the 'most broadly effective and efficient means of organizing a system or performing a function' [3]. Von Solms et al [19] conclude that 'best practice can possibly serve as a reference to the care that an ordinarily reasonable and prudent party should apply in the case of the protection of valuable company information resources' [19].

IS governance and management models, must include a way to prove that the controls in place are the most broadly efficient and effective for the specific organization. According to the CSI/FBI computer crime survey 2006, 82% of organizations assess their security posture by performing internal audits and 62% using external audits [7]. Other means of assessing is penetration testing, e-mail monitoring and web activity monitoring tools. Assessing the security posture of the organization will not be sufficient as the IS architectures do not consider the requirement for the preservation of digital evidence. Organizations will not be able to determine the source of an event in a legally acceptable way as admissible evidence is not in place.

By including some aspects of DF readiness into the IS architecture of the organization, it will be possible to link the source of the attack to the incident and the perpetrator. It will also enable management to assess the current controls so that they have proof that the controls in place are efficient and effective.

The following Sarbarnes–Oxley [26] sections require DF readiness in an organization:

- Section 302 stipulates that CEO's and CFO's (CIO's) are responsible for signing off the effectiveness of internal controls. DF readiness can assist by looking at information on the corporate network as part of compliance. CIO's will be able to use DF processes to prove that regular checks have been performed;
- Section 802 indicates that there are criminal penalties if documents are altered. DF procedures adhere to legal requirements for evidence, therefore it will be possible to prove that the information is original and not altered;
- Section 409 requires rapid response and reporting. DF readiness will enable rapid response and
- Finally, the report also requires a whistle blowing policy. Remote network forensics is good at doing an analysis without tipping off the perpetrator [9].

In a study done by Spike Quinn [17] in New Zealand he has proved that:

- internal policies and procedures for dealing with evidence recovery is often insufficient for admissible evidence in court;
- management can also not plan for events that may need forensic investigation as they often do not sufficiently comprehend the requirement for admissible evidence required for successful prosecution and lastly;
- where management expect IT staff to deal with events that may require DF investigations, often the evidence will not be admissible in court as the staff are not properly trained [17].

This is not a country specific example, but many organizations are still not ready for successful prosecution of a perpetrator should an event take place [11].

It is therefore clear that DF and specifically DF readiness can not be treated as a separate issue from IS. DF readiness should also not only be included in the security awareness programs and incident response plans of the organizations, but in all aspects of planning, implementing, monitoring and assessment of IS in an organization. DF readiness must therefore be included as a component of best practice for IS.

6 Summary

Most organizations have accepted IS as a fundamental business requirement. Protecting the information and information assets is no longer sufficient as corporate governance reports require full responsibility and accountability from management, also in terms of IS governance.

This paper has indicated that the current IS architectures, strategies and best practices are lacking in the sense that successful prosecution of an event can seldom occur due to the lack of admissible evidence and poor procedures. Management will not be able to prove that the security controls are effective and efficient.

DF readiness will demonstrate due diligence and good corporate governance of a company's assets. It will provide guidelines of the legal admissibility of all processes and evidence, identify the misuse or illegal use of resources, and provide guidance on the legal aspects of logging data and monitoring of people's activities using IT systems in an organization

DF readiness as discussed in the paper will enhance the security strategy of an organization by providing a way to prepare an organization for an incident, whilst gathering sufficient digital evidence in a way that minimizes the effect on normal business processes. This can help to minimize system downtime and the cost of the investigation if an incident occurs.

DF readiness is a component of an IS best practice, as it will provide the IS manager and top management the means to demonstrate that reasonable care has been taken to protect valuable company information resources.

References

1. American Heritage Dictionary (4th Edition), (New York, NY: Houghton Mifflin, 2000).
2. Cullery A, *Computer Forensics: Past Present And Future, Information Security Technical Report,* Volume 8, number 2, (Elsevier, 2003), p 32-35.
3. Dictionary.Com, (June 31, 2006), http://dictionary.reference.com.
4. Digital Forensic Research Workshop, *A Roadmap for Digital Forensics Research,* (2001), www.dfrws.org.
5. Endicott-Popovsky B, Frincke D, *Adding the 4th R: A Systems Approach to Solving the Hackers Arms Race*, Proceedings of the 2006 Symposium 39th Hawai International Conference on System Sciences, (2006).
6. Garcia J, 2006, *Pro-Active and Re-Active Forensics,* (September 5, 2006), http://jessland.net.
7. Gordon La, Loeb M, Richardson R, Lucyshyn W, 2006 *CSI/FBI Computer Crime and Security Survey,* (Computer Security Institute, 2006).
8. Grobler CP, Von Solms SH, *A Model To Assess The Information Security Status of an Organization with Special Reference to the Policy Dimension* , Master's Dissertation, (2004).
9. Hilley, 2004, *The Corporation: The Non-Policed State*, (September 24, 2006), http://www.infosecurity-magaqzine.com/features/novdec04/corp_novdec.htm.
10. Hoffman T, 2004, *Sarbanes-Oxley Sparks Forensics Apps Interest,* (March 29, 2004), http://www.computerworld.com/action/article.do?command=viewarticlebasic&articleid=91676.
11. Inforenz, 2006, *Are You Ready For Forensics*?, (September 14, 2006), http://Inforenz.com/press/20060223.html.
12. Cobit: Control Objectives for Information and related technologies, (IT Governance Institute, 3rd edition, 2000)
13. King II Report on Corporate Governance, (August, 2003), http://iodsa.co.za/lod%20draft%20king%20report.pdf.
14. Kruse II, Warren G, Jay G Heiser JG, *Computer Forensics Incident Response Essentials*, (Addison Wesley, Pearson Education 2004).
15. Louwrens B, Von Solms SH, Reeckie C, Grobler T, *A Control Framework for Digital Forensics*, Advances in Digital Forensics, (Springer, 2006).
16. Patzakis J, *Computer Forensics as an Integral Component of Information Security Enterprise*, Guidance Software, (October 24, 2005), www.guidancesoftware.com.
17. Quinn S, *Examining The State of Preparedness of IT Management in New Zealand for Events that may require Forensic Analysis*, Digital Investigation, December 2005, Volume 2, Issue 4, (Elsevier, 2005), p. 276-280.
18. Reith M, Varr V, Gunch G, *An Examination of Digital Forensic Models.* International Journal Of Digital Evidence Volume 1, Issue 3, (Elsevier, 2002), (February 15, 2005), http://www.ijde.org/docs/02 art2.pdf.
19. Rosseau Von Solms, SH (Basie) Von Solms, *Information Security Governance: Due Care*, Computers And Security, (August 13, 2006), doi:10:1016/Jcose.
20. Rowlingson, *A Ten Step Process for Forensic Readiness*, International Journal of Digital Evidence, Volume 2 Issue 3, Winter 2004, (Elsevier, 2004).

21. SABS ISO/IEC17799. SABS Edition 11/iso/iec Edition1, South African Standard, Code of Practice for Information Security Management, (South African Bureau of Standards, 2001).
22. Sheldon A, Forensic Auditing, *The Role of Computer Forensics in the Corporate Toolbox*, (March 25, 2004), http://www.itsecurity.com/papers/p11.htm.
23. Sinangin D, *Computer Forensics Investigations in a Corporate Environment*, Computer Fraud and Security Bulletin, Volume 8, p.11-14, June 2002, (Elsevier, 2002).
24. Stephenson P, *Conducting Incident Post Mortems*, Computer Fraud and Security, April 2003, (Elsevier, 2003).
25. The Electronic Communications and Transactions Act, (2003), http://www.gov.za/gazette/regulation/2003/24594a.pdf.
26. Sarbarnes-Oxley Act of 2002, (October 20, 2006), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf.
27. Von Solms SH, *Information Security Governance: Cobit or ISO17799 or both,* Computers and Security, Volume 24, Issue2, March 2005, (Elsevier, 2005).
28. Von Solms SH, *Information Security: The Fourth Wave*, Computers and Security, Volume 25, Issue3, May 2006, (Elsevier, 2006), p. 165-168.
29. Von Solms SH, Louwrens CP. *Relationship between Digital Forensics, Corporate Governance, Information Technology and Information Security Governance* ,(Information Security Of South Africa Conference 2005 Proceeding , 2005).
30. Wolfe H, *The question of organizational forensic policy*, Computer Fraud and Security, Volume 6, June 2004, (Elsevier, 2004), p. 13-14.