Information Assurance and Forensic Readiness

Georgios Pangalos[1] and Vasilios Katos[2]

[1] Aristotle University of Thessaloniki, Greece
pangalos@auth.gr
[2] Democritus University of Thrace, Greece
vkatos@ee.duth.gr

Abstract. Egalitarianism and justice are amongst the core attributes of a democratic regime and should be also secured in an e-democratic setting. As such, the rise of computer related offenses pose a threat to the fundamental aspects of e-democracy and e-governance. Digital forensics are a key component for protecting and enabling the underlying (e-)democratic values and therefore forensic readiness should be considered in an e-democratic setting. This position paper commences from the observation that the density of compliance and potential litigation activities is monotonically increasing in modern organizations, as rules, legislative regulations and policies are being constantly added to the corporate environment. Forensic practices seem to be departing from the niche of law enforcement and are becoming a business function and infrastructural component, posing new challenges to the security professionals. Having no a priori knowledge on whether a security related event or corporate policy violation will lead to litigation, we advocate that computer forensics need to be applied to all investigatory, monitoring and auditing activities. This would result into an inflation of the responsibilities of the Information Security Officer. After exploring some commonalities and differences between IS audit and computer forensics, we present a list of strategic challenges the organization and, in effect, the IS security and audit practitioner will face.

Keywords: Computer forensics, e-discovery, IS audit, compliance.

1 Introduction

Information Systems auditing (IS auditing) is a cornerstone function of Information Assurance. IS auditing is performed on all facets of the corporate IS, to ensure that the security controls placed within the system support IT governance which will allow the company to align its IT strategy with its enterprise objectives. The enterprise objectives in turn are reflected in the security policies which are the main means for communicating the *acceptable* behavior of all parties involved.

Recently the extroversion of the companies has been amplified with the facilitation of the Information and Communication Technologies. The speed of collecting, processing and disseminating information warranted a closer coupling between a company and its third parties and customers. However this setting posed additional challenges with respect to the protection of the data which in many cases involves third party personal information and as such regulatory compliance was mandated.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 181–188, 2010.

In addition, the overwhelming presence of ICT and the fact that the corporate IS has become the main instrument for conducting business, computer crime has enjoyed a proliferation in the recent years [1, 2]. As a result computer forensics not only have become the fastest growing market in information security [3], but also have become a centerpiece of the ICT infrastructure.

Currently the overlap between digital forensics and information security is acknowledged [4] and this is represented in Fig. 1a. It is advocated in this paper that the scope of forensics needs to be expanded in order to encompass the whole IS security domain as shown in Fig. 1b. This all-inclusive paradigm is primarily due to the expanding use of ICT and the substantial increase of user acceptance which is in line with the directions toward e-Governance in an Information Society. As such, it is anticipated that the term *user* will become synonymous to the term *citizen*. Consequently, strict corporate security policies will be challenged and could potentially conflict with the wider societal trends. A typical example is the policies prohibiting the use of corporate communication resources such as email for personal use, which could be viewed as an attempt to socially exclude the user who is already accustomed to using the email for accessing State services. This would create an environment where practices to detect security policy violations would need to be investigated in a legally acceptable way, regardless whether there is a civil or criminal offense committed or suspected. Naturally, this could lead to the need to incorporate digital forensics and incident response practices in the IS auditor's activities. Absence of formal forensic investigation processes could jeopardize the privacy and rights of the user as well as elevate the risk of the company facing lawsuits.

This paper is structured as follows. In Section 2 the audit process is outlined for the benefit of the reader who is unfamiliar with the area. Section 3 highlights the main aspects of digital forensics and forensic readiness. The material presented in Sections 2 and 3 is leveraged in Section 4 in order to highlight the challenges of the contemporary IS operating in a highly networked company placed in the information society. Finally the conclusions are presented in Section 5.

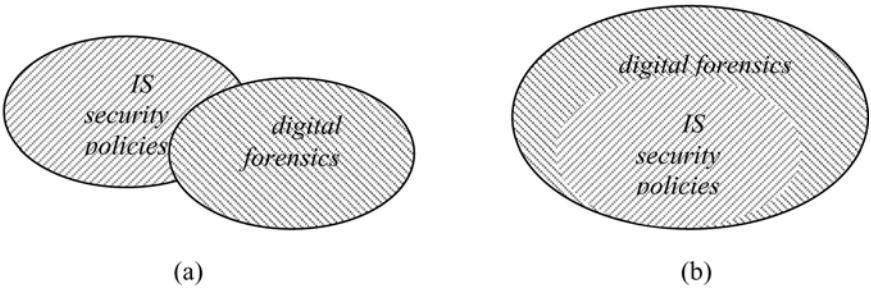

Fig. 1. The overlapping scopes between IS security and forensics

2 The Audit Process

IS audit is performed in order to assess the correctness of installation of the security controls aiming to reduce the risks to acceptable levels. Such exercise would imply

that a security assessment has been performed and the business owner and stakeholders together with the security consultant or security architect have agreed upon a number of security controls, but most important the business owner has agreed on accepting the residual risk. The Information Systems Audit and Control Association (ISACA) specifies the following five distinct tasks within the IS audit area [5]:

1. Develop and implement a risk-based IS audit strategy for the organization in compliance with IS audit standards, guidelines and best practices.
2. Plan specific audits to ensure that IT and business systems are protected and controlled.
3. Conduct audits in accordance with IS audit standards, guidelines and best practices to meet planned audit objectives.
4. Communicate emerging issues, potential risks and audit results to key stakeholders.
5. Advise on the implementation of risk management and control practices within the organization while maintaining independence.

The above tasks can be viewed as primitives for building an audit framework. An audit framework can be build upon a plethora of published standards, guidelines and procedures. Table 1 summarizes a small portion of known standards guidelines and procedures which are available to the IS auditor.

Table 1. Representative standards, guidelines and procedures

Short name	Title	Type
ISO 27002 (ISO/IEC 17799)	Code of practice for information security management	Standard
ISO 27005	Information security risk management	Standard
BS25999	Standard for Business Continuity Management	Standard
ISACA-S9	Irregularities and Illegal Acts	Standard
ISACA-S10	IT Governance	Standard
ISACA-G28	Computer Forensics	Guidelines
ISACA-G31	Privacy	Guidelines
ISACA-P3	Intrusion Detection	Procedures
ISACA-P8	Security Assessment – Penetration Testing and Vulnerability Analysis	Procedures

Of particular importance in this paper is the guideline G28, which relates to computer forensics. This guideline is further studied later on in Section 4.

Perhaps the most representative source of information is the material pertaining to the Certified Information Systems Auditor qualification. The CISA material consists of the following six domains [5]:

- The IS audit process, which encompasses the entire IS auditing process.
- IT Governance, which sets the context in which the controls are placed.
- Systems and Infrastructure Life Cycle Management, which relates to the key processes and methodologies adopted by organisations when creating and maintaining IS.

- IT service delivery and support, which is about service level expectations as derived from the organisation's business objectives.
- Protection of information assets, where the controls implemented are evaluated against the three security criteria of confidentiality, integrity and availability.
- Business continuity and disaster recovery, focusing on the controls that are responsible for ensuring the availability of the critical IS processes.

Other paradigms such as ISO and BS have a slightly different mix and definition of domains, but they all consent to the protection of the IS assets against confidentiality, integrity and availability threats.

3 Forensic Readiness and the Digital Forensics Process

Digital forensics is the examination of computer systems and digital storage media by the use of investigative and scientific techniques for the preservation, identification, acquisition, analysis, interpretation and documentation of the (digitally stored or encoded) information for evidentiary and/or root cause analysis and presentation of digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal [4,6,7,8,9]. Forensic readiness is the state of the organisation where certain controls are in place in order to facilitate the digital forensic processes and to assist in the anticipation of unauthorised actions shown to be disruptive to planned operations.

From the above definitions it should be evident that effective forensics cannot exist without security controls. Preservation for example is demonstrated with the use of cryptographic hashes [10], in the case of dead forensics [11]. The concept of preservation is also found in disaster recovery and business continuity practices. Analysis and interpretation of the findings highly depends on the ability to distinguish the malicious from benign activities, which is an area well studied in the domain of intrusion detection, whereas accountability and identification of a user/suspect suggests that acceptable user authentication is in place.

In modern organizations the vast majority of documents are in a digital form. The term Electronically Stored Information, ESI refers primarily to storage and retention of electronically generated documents. As such, the digital forensics process when invoked must deal with the acquisition of documents from a variety of sources and states and the forensic analyst is burdened with the task to identify and correlate the digital evidence. The term which encompasses the above forensic tasks is referred to as e-discovery. Consequently, the effectiveness as well as cost of e-discovery would depend on the capability and maturity of the attained forensic readiness. In addition when there is a litigation involved, there may be compliance and other legislative issues. This is already reflected in the US with the enactment of the new amendments to the US court system's Federal Rules of Civil Procedure, FRCP [12], which emphasizes on the timeliness of serving electronic documents in court. A representative example is the case of General Motors being fined $700,000 by the Alabama Circuit Court of Appeals for delaying a discovery process by 98 days [13].

The attribute which differentiates forensic investigations from other type of investigations such as network monitoring, is due diligence and the ability to demonstrate this.

The investigator needs to take care in order not to harm or offend the interests of all parties involved as well as their properties, and the forensics procedures are built around these considerations. As an example, due diligence is shown in the case of a suspect hard disk acquisition, if reasonable effort is invested to preserve the state of a hard disk, and the cryptographic hashes are calculated against the whole disk at the earliest possible stage of the e-discovery process. As we will present below, due diligence is not necessarily one of the objectives in information security led investigations.

4 Analysis and Discussion

ISACA's G28 guideline on computer forensics [14] aims to introduce the forensics process to the IS auditor practitioner and also provides a list of audit considerations. The very fact that the reference to forensics is in a form of a guideline, shows a weak coupling between the IS audit practice and the domain of computer forensics. Provided that the need for compliance is gaining ground, digital forensics will become a core and established practice in the corporate. Thus, integration between the two disciplines must be targeted on an epistemological level.

Against the above, a number of issues are becoming apparent which are detailed below.

4.1 The Security Auditor Needs to Revisit the Risk Analysis Paradigm

Typically on a risk assessment exercise the auditor and the stakeholders agree on the company's risk exposure. More analytically, the auditor assesses the risk and if this is found to be acceptably high, then security controls are introduced in order to lower the risk to an acceptable level. The acceptable risk is the so called residual risk and the auditor is not normally concerned with this quantity. We subscribe to the view that the presence of the residual risk is the very reason for the need and existence of forensics. By accepting the residual risk, we also accept that the security controls will at some point fail. Security breaches, no matter how low risk may be, must be treated as potentially criminal activities due to the lack of the *a priory* knowledge of the nature of the security event. The tunnel vision of risk analysis which focuses primarily on financial losses does not provide information on the long term impact of an event which may exhibit low losses during its genesis.

Risk assessment seems to be the common denominator between IS auditing and forensics, as it is emphasized in [7] that the need for forensic readiness can be established via a risk assessment. However, if the scope of forensics is to be expanded to include all aspects of information security, the auditors need to adapt there practices to the forensics paradigm.

4.2 Redress

The limited dimensions of risk assessment can also be understood if one examines the goals of the security controls. More analytically, information security controls serve three goals, namely prevention, detection and recovery. Detection in security does not necessarily include the goal of identifying the perpetrator, or as colorfully mentioned in forensics to "put fingers on keyboards". In [15] the synonyms of resistance, recognition,

recovery are used to describe the components of what the authors equivalently call a survivable system (that is an IS with security controls). In the same paper the authors recognize the need for a fourth goal, redress [15]:

> *Redress is the ability to hold intruders accountable in a court of law and the ability to retaliate.*

It can be seen that accountability is a subset of redress. Again, due to the need for compliance and risks of litigation, the traditional accountability solutions may not be sufficient in the modern organization, but should be enriched with computer forensics techniques and processes for legal remedies and active defense. It should be highlighted that the traditional accountability processes should not become obsolete, but be enriched instead with the above aspects.

4.3 Business Continuity and Forensic Readiness

The domain of business continuity and disaster recovery can be a valuable source of information to support forensic readiness and incident response respectively. Business continuity includes processes for data backup and recovery. These processes can form the specification documents for developing forensic readiness processes. Disaster recovery may in turn benefit from incident response practices which can run in parallel in the event of a security breach.

4.4 Well Established Roles in Forensics

Roles such as Chief Information Security Officer, Security Architect and Security Administrator are well established in many organizations. The expanding scope of security and forensics though necessitates a dedicated role relating to forensics. A Security Architect for example is not responsible and does not maintain the key skills for conducting forensics and setting forensic readiness requirements. Depending on the organization, its size and the industry it is in, a Forensic Consultant type of role will most likely be required. At the time of writing there is no established body of knowledge in digital forensics and there is a plethora of professional certifications. It is expected that the computer forensics discipline will undergo a lifecycle similar to that of information security.

4.5 Forensics on the Security Policies

The security policies can be found to be exposed and the need for applying computer forensics practices. For example, firewall and intrusion detection policies do not usually include forensic considerations within their incident response processes. Since one would not know *a priori* if a suspected action (e.g. obtained by detecting abnormal network activity) will result to a criminal offense being committed, monitoring should incorporate live forensics practices in order to secure the potential evidence from spoliation. On the other hand, forensic acquisition of evidence normally includes safeguards to protect the privacy of the users on the corporate network.

Consequently, the security policies would also need to be assessed for their forensic readiness status. A deliverable for this exercise could be a metric for forensic readiness.

5 Conclusions

The challenges faced by the corporations and the auditors with respect to compliance and forensic readiness need to be addressed in a systematic way. Although a corporate policy violation will not necessarily lead to court (in fact about a third of the violations do lead up in court [16]), the actual severity and legal implications of a security event cannot be established beforehand. Consequently, forensic practices seem to be departing from the niche of law enforcement and are becoming a business function and infrastructural component. This migration will pose challenges to the security professionals and may require the establishment of the role of a computer forensics analyst.

It is argued that the two main components of information assurance is security auditing and forensics. The former is a mature discipline in IS and can provide some of the primitives to both incorporate and facilitate the computer forensics processes within the organization. The need for synergy between forensics and IS auditing can be justified with the compliance restrictions which are regularly introduced in the corporate environment. This synergy in turn would trigger further integration practices between the two disciplines and in this paper we exposed some of the reasons that the integration may lead to research intensive directions, as well as the challenges an audit practitioner will face.

The issues raised in the discussion section essentially require a methodology for integrating the disciplines. This is an ongoing area of research.

References

1. Antiphishing Working Group. Phishing Activity Trends Report Q2, 2008 (2008), http://www.antiphishing.org/reports/apwg_report_Q2_2008.pdf
2. Parliamentary Office of Science and Technology. Computer Crime. POSTNOTE, 271 (2006)
3. Harris, S.: To Catch A Thief: Bringing Forensics In-House And The Necessary Tools To Succeed. Amazines (2008)
4. Grobler, T., Louwrens, B.: Digital Forensic Readiness as a Component of Information Security Best Practice. In: Venter, H., Eloff, M., Labuschanc, L., Eloff, J., von Solms, R. (eds.) New Approaches for Security, Privacy and Trust in Complex Environments. IFIP, vol. 232, pp. 13–24. Springer, Boston (2007)
5. Information Systems Audit and Control Association: CISA Review Manual 2008 (2007)
6. Kruse II, W., Heiser, J.: Computer Forensics: Incident Response Essentials. Addison Wesley, Reading (2004)
7. Rowlingson, R.: A Ten Step Process for Forensic Readiness. Int. Journal of Digital Evidence 2(3) (2004)
8. Sinangin, D.: Computer Forensics Investigations in a Corporate Environment. Computer Fraud & Security 8, 11–14 (2002)

9. EDRM, The E-Discovery Reference Model, http://edrm.net
10. Chen, L., Wang, G.: An Efficient Piecewise Hashing Method for Computer Forensics. In: 2008 Workshop on Knowledge Discovery and Data Mining, pp. 635–638 (2008)
11. Kotze, D., Olivier, M.: Patlet for Digital Forensics First Responders. In: 18th International Workshop on Database and Expert Systems Applications, pp. 770–774 (2007)
12. US Court, Amendments to the Federal Rules of Civil Procedure (2006), http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf
13. Marcella, A.: Electronically Stored Information and Cyberforensics. Information Systems Control Journal 5, 44–48 (2008)
14. Information Systems Audit and Control Association, Guidline G28: Computer Forensics (2000)
15. Endicott-Popovsky, B., Frinke, D.: Adding the 4th R: A Systems Approach to Solving the Hackers Arms Race. In: Proc. of the 2006 Symposium 39th Hawaii International Conference on System Sciences (2006)
16. Computer Security Institute CSI Survey 2007 (2007), http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf