Digital Investigations for Enterprise Information Architectures

Syed Naqvi, Gautier Dallons, Christophe Ponsard

Centre d'Excellence en Technologies de l'Information et de la Communication (CETIC)
29 Rue des Frères Wright, 6041 Charleroi, Belgium
{syed.naqvi; gautier.dallons; christophe.ponsard}@cetic.be

***Abstract*—This paper highlights the role of digital forensics in the enterprise information architecture. It presents a framework for embedding digital forensics analysis techniques at various stages of corporate information and communication technologies (ICT) lifecycle. A set of best practices for the corporate ICT security policy is also outlined to keep the operational costs of digital forensics at the optimal level. It also presents a detailed analysis of the risks to the competitive-edge of the companies that will not employ the forensics solutions to protect their business interests. This work also provides a high-level roadmap for the adaption of digital forensics in the emerging core business technologies such as cloud computing and virtualization infrastructures.**

Keywords - digital forensics analysis, ICT security architecture, enterprise information architecture

I. INTRODUCTION

Crimes involving computers started to occur as soon as the computers started sprawling across the various activities of everyday life in the 1980s. United States Federal Bureau of Investigation (FBI) launched its *Magnetic Media Program* [1] to address the growing needs of analyzing computers especially storage media for their investigations of high-technology crimes. The growth of networking technologies in the 1990s gave further impetus to the need for tackling crimes using sophisticated technological means. However, the overall scope of the digital forensics remained confined to the law enforcement agencies with the sole objective of collecting reliable evidences for the prosecution of the criminals involved in a court of justice.

The interest of performing digital forensics analysis at the enterprise level has significantly grown nowadays. This trend can be seen as a logical evolution of *white hat* or *ethical hacking* that is performed by the businesses to ensure that their ICT infrastructure is free from vulnerabilities. However, the major driving force behind this trend is the fact that growing number of *criminal offenses* using ICT is overwhelming the computer crime units. It is not so easy to involve law enforcement agencies in a commercial environment where there are some suspicious activities; but no explicit computer crime is committed. Moreover, their involvement casts shadows on the business interests notably on the reputation of the company.

Nowadays, enterprises are embracing considerable shift in their business approach where they have to not only adapt to non-traditional concepts such as virtualization, but also switch to more comprehensive security solutions to cope with the new security requirements as only pre-incidence measures, i.e., attack preventions is no longer be sufficient to protect their assets. They need to invest in the post-accident situation, i.e., digital forensics. It is evident that European enterprises can learn a lot in this area from their US counterparts who have acquired considerable experience of using digital forensic technologies in the business environment whereas digital forensics is still seen by a vast majority of Europeans as specialized tools for police to tackle cyber criminology.

This nascent trend of in-house digital forensics analysis in a relatively non-criminal context has to prove its worth by providing some competitive edge to the businesses. Major challenges include the demarcation of exact role of the digital forensics in the overall corporate ICT security operations; reducing its functional costs both in terms of monetary expenditures incurred in the acquisition of corresponding technologies; and in terms of the time consumed in the subsequent investigations especially when the operations of core business line are directly affected. This paper pragmatically identifies the role of digital forensics in the overall security architecture of an enterprise. We propose to implant the corresponding digital forensics analysis features in the various components of the corporate ICT infrastructure. This scheme provides better organization of the security functionalities with minimal impact on the overall performance of the ICT operations.

This paper presents a framework of digital forensics for enterprise information architectures and evaluates the scope of various methodologies and tools for these enterprise applications. It also presents a detailed analysis of the risks to the competitive-edge of the companies that will not employ the forensics solutions to protect their business interests. This work also provides a high-level roadmap for the adaption of digital forensics in the emerging core business technologies such as cloud computing and virtualization infrastructures.

This paper is organized as follows: Section II describes the role of digital forensics in the enterprise information architecture. A digital forensics analysis framework for enterprise information security policy is presented in Section III. Section IV highlights the impact of digital forensics on the competitive-edge of enterprises. Section V identifies a range of challenges of investigating the emerging paradigm of virtualized infrastructures. A discussion on the recent trends in the area of digital forensics and their positioning with our approach is presented in Section VI. Finally, some conclusions are drawn in Section VII.

II. ROLE OF DIGITAL FORENSICS IN ENTREPRISE INFORMATION ARCHETCTURE

The area of digital forensics analysis is considerably mature in the modern criminology; however, its scope in the commercial environment is still vague. Therefore, it is needed to precisely identify the role of digital forensics at various levels of the enterprise ICT operations so as to enhance the overall quality of protection without causing any substantial impact on the system's performance. This section outlines major blocks of a typical enterprise ICT infrastructure followed by the identification of those blocks where digital forensics analysis has a role to play. These roles are elaborated for individual blocks. These roles can eventually be harnessed together to constitute various digital forensics analysis functions.

Figure 1 shows a typical lifecycle of corporate ICT operations. These blocks are tagged to facilitate their subsequent usage. These operational blocks are subject to a number of internal and external requirements that have to meet in order to ensure the proper functioning of the overall business routines. We identify those blocks that require digital forensic analysis features for the improvement of the quality of protection offered by the corporate ICT security architecture. A magnified glimpse of these blocks is shown in the Figure 2.

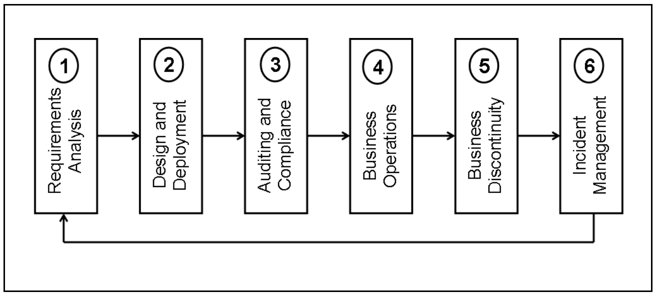

Figure 1. Various phases of corporate ICT operations

1) Design and Deployment

The design and development phase should ensure that the ICT infrastructure is globally *forensic-friendly* – this implies that both design specifications and deployment parameters should provide some sort of explicit checkpoints to facilitate digital forensics analysis at any time instant without causing major disruption to their operational routines.

The design and development phase also needs to ensure that *chronological documentation (chain of custody)* can be conveniently produced if deemed necessary. It can include some nonrepudiation techniques such as watermarking to justify that they are not tampered at any stage.

The design and development phase should also include *resilience planning* so that the forensic analysis will have minimal impact on the functioning of routine operations. This feature is particularly important for today's large-scale highly connected systems, such as Clouds, where disruption of entire ICT infrastructure in the aftermath of any incident will inflict huge damages. This feature also includes recovery time that is ideally kept at the minimum possible level.

2) Auditing and Compliance

The auditing and compliance is not only a prerequisite for launching a specific business but also a marketing tool to increase the customer base. Therefore, the auditing and compliance phase should provide means of justifying that the business is meeting all of its *legal obligations*. For example, the United States Sarbanes Oxley Act (SOX) [2] requires a formal process of using forensic analysis techniques for the investigation of incidents. This law has made significant impact on the security policies and incident management strategies of US based corporations [3].

Besides serving the compliance issues of the legal requirements, digital forensics can also play its role in the fulfillment of regulatory requirements that most of the corporations are required to comply with. For example, information security incidence management procedures are recommended by the ISO standard ISO27002 [4].

Likewise, the *quality assurance* practices can be improved by using digital forensics techniques such as analyzing the performance bottlenecks of network bandwidth, storage mediums, etc. They can be employed when some performance degradation is reported or they can be proactively used to ensure the execution of an optimal quality assurance plan.

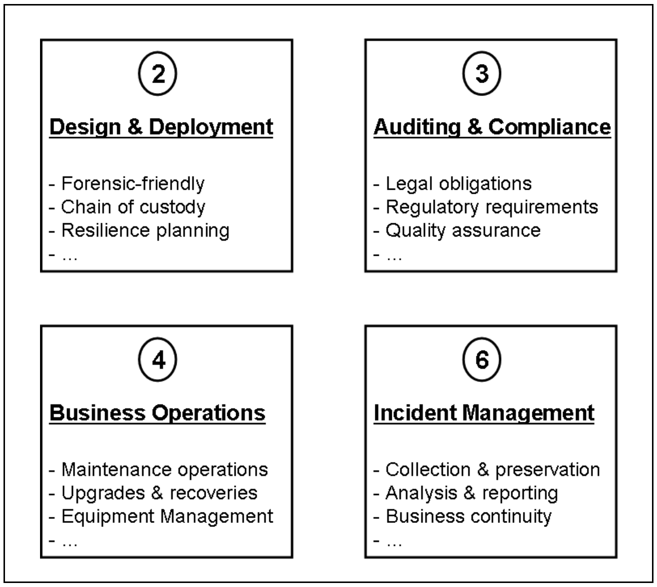

Figure 2. Corporate ICT phases that can be improved by Digital Forensics

3) Business Operations

The business operations phase is crucial for meeting the company's targets within the allocated resources. Therefore, it is important to explore newer techniques to improve this phase not only to facilitate the targets achievements, but also to provide a competitive-edge in this core operational phase.

Several *maintenance operations* of corporate ICT infrastructure, such as disk cleaning operations, require reliable analysis solutions. Digital forensics analysis tools can be employed to efficiently provide these maintenance operations.

With the ever increasing evolution and expansion of the ICT scope in everyday life, the *upgrades* have become a routine activity. Moreover, *data recovery* from the obsolete, faulty, or broken equipment requires some reliable solutions. Digital forensics techniques can be employed for recovering data in these situations.

Managing the ICT inventories in a corporate environment also requires efficient sorting solutions before discarding the useless lot. Digital forensics techniques can assist in securely disposing of equipment.

4) Incident Management

This is the privileged phase for employing digital forensic techniques as the general perception of the *forensics* is the post incident analysis. Digital forensics can be used by the administrator of a corporate ICT infrastructure to gather the digital traces and consequently analyze them to determine the causes of incident. All these actions should be carried out within the given legal framework. Another important role of the incident management team is to ensure business continuity ideally even during the incident phase. In real terms, it should at least ensure the continuation of core business operations during the adverse situations.

III. A Digital Forensics Analysis Framework for Enterprise Information Security Policy

Corporate security policy can play the pivotal role in outlining best practices for their ICT security teams. We suggest that organizational security policy of a modern enterprise should explicitly reflect the role of digital forensics as described in the section II of this paper.

Figure 3 presents a placement of *security and forensics team* in a corporate ICT infrastructure where it interacts with the different phases that can benefit from various digital forensics analysis techniques.

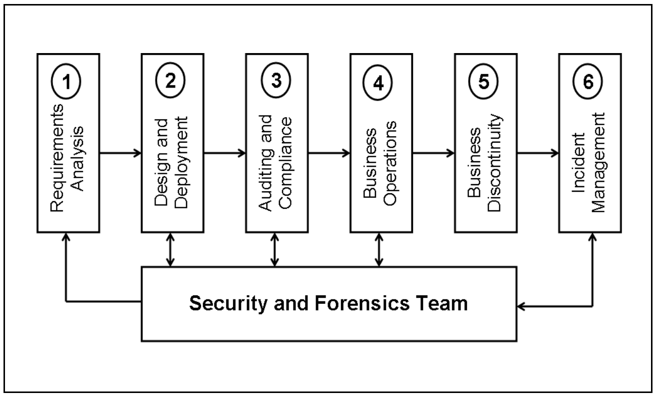

Figure 3. Security and Forensics Team in a Corporate ICT Infrastructure

It is essential that security and forensics team should be equipped with *fine-grained forensics policy* that can handle the peculiar requirements of the contemporary ICT infrastructures especially their complexities, scale, and decentralization. It is understood that highly dynamic environments such as *Open Clouds* give rise to enormous challenges of localization and demarcation of their boundaries that keep on changing in an amoeboid style. While research and development initiatives are needed to effectively address these specific challenges, ICT security teams of corporate sector can handle the digital forensics tasks by having clear vision and strategy of achieving the security goals. The current state of the tools support for the digital forensics activities is quite sparse. We therefore recommend using a set of tools for different tasks instead of looking for a comprehensive framework or toolkit that can provide a silver bullet kind of solution.

We now present different phases of standard forensics analysis and their efficient implementation in businesses. They are presented in the context of incident management; however, we have already shown that these techniques are equally useful in a number of other ICT operations.

A. Preparation phase

Preparation phase mainly involves adequate planning by envisioning the security threats and the contingency plans followed by the deployment of necessary tools and procedures. This is a management task that requires regular re-evaluation and assessment as the threats picture changes rapidly especially in the dynamic environments such as virtual infrastructures.

B. Detection phase

Detection phase often includes collection mechanism as well. This phase requires up to date set of tools to monitor the company's ICT resources and capture the various events followed by the identification of some abnormal activity that should be logged and the security manager be notified.

C. Preservation phase

Preservation phase generally involves the production of copies of the ICT resources being investigated. The original resources are preserved so that they can no longer be altered. The integrity of the original resources is indispensable in the follow-up procedures in the court of justice or even in the disciplinary action board.

D. Analysis phase

Analysis phase traditionally employs human interventions to note the sequence of events leading to a particular incident. However, the ever growing scale and scope of the digital data now necessitates the use of some semantic tools for the analysis of log files and traces. This phase also involves some artificial intelligent mechanisms for performing good quality analysis to avoid human errors.

E. Recovery phase

Recovery phase is generally not seen as an integral part of the forensics task. However, any emergency or incidence response cannot be completed if the system is not restored to its original functioning state. This situation is especially desirable when the core business of a company is halted due to some incidence and therefore there is immense pressure to restore the routine activities.

F. Reporting phase

Reporting phase is not necessarily the preparation of legal case against the attackers. A simple report of incidence for the line manager can also constitute this phase. The objective is to produce a record of the incidence that took place in the corporate ICT infrastructure. It can also be used as a feedback for the preparation phase, so that the reasons leading to the incident can be taken into account by the company's security team.

IV. IMPACT OF DIGITAL FORENSICS ON THE COMPETETIVE-EDGE OF ENTERPRISES

There are genuine ICT security concerns for enterprises especially when the scope of virtualization brings several challenges for its deployment including a lot of uncertainty as to how and where to implement security [5]. Security and dependability issues are a gauging factor for measuring the success of business endeavors. Classical security solutions and practices are getting obsolete in the face of the peculiar security requirements of virtualization infrastructures where physical resources are dynamically mapped to address the spontaneous business needs. The inherent nature of virtualization requires totally different security provisioning approach than the classical one developed decades ago.

This section covers a set of threats mitigation techniques that can be employed by using digital forensics techniques and the risks of not using digital forensics in the enterprise environments. We maintain that it is becoming indispensable for the businesses to integrate digital forensics in the security architecture of their enterprise information architectures otherwise there could be devastating impact both in terms of security breaches and in the loss of business prospects.

A. Threats Mitigation Techniques using Digital Forensics

This section summarizes a set of major security challenges that can be addressed by using appropriate digital forensic technologies.

1) Access Control

Enterprise virtualization infrastructures offer promising features for the enterprises. However, virtual ICT resources are lot more vulnerable to malicious activities than the classical ones. Smart solutions for the monitoring of the access logs of an enterprise have become indispensable to know if its resources are the target of some malicious activity. It also includes insider threats such as frequent remote access to the company's resources outside the routine office hours.

2) Steganalysis

The ever-growing demand of bandwidth capacity for the contents rich applications is driving the conception of high speed internet backbone to enable seamless access to the applications using bulk of data. However, this capacity exposes enterprises to *steganography* where important corporate data can easily be stolen. The enterprises need to incorporate efficient steganalysis tools to protect its intellectual properties.

3) Multi-tenancy

Multi-tenancy is quite new concept [6] that refers to the architectural principle, where a single instance of the software runs on a software-as-a-service (SaaS) vendor's servers, serving multiple client organizations. Assuring data isolation on a node is a challenging task for the security designers that include complete isolation of their execution environments and data storage including temporary storage of the execution data. Enterprises need to employ some analysis tools to trace the software instances for being assured of the protection of their data in the multi-tenant applications.

B. Risks Analysis for Computing Impact on the competitive-edge of Enterprises

The ISO27001 [7] standard defines the way to establish an Information Security Management System. Considering this standard, a company has to monitor its security in order to adapt the security policy to new threats. This standard considers not only IT security but also Information system security that is broader than the IT infrastructure. In this paper, we only consider IT security of the infrastructure used to operate the enterprise information system.

ISO27001 requires enterprise to monitor its *security state* in order to monitor security breaches and to react accordingly. Security monitoring implies tracking of the security traces left by an attacker. Digital forensics analysis techniques and tools can facilitate this task. This standard requirement has the objective of reducing the risk linked to security for companies. If we consider a company with a set of computer business asset A = {a1, …, an}, each asset is concerned by security following four properties : Confidentiality (C), Integrity (I), Availability (D) and Legal force (L) (legal force is the ability of an asset to be used as a proof in the case of lawsuit). Each asset has some requirements concerning these properties. The risks are to loose one or more of these security properties. The risk of a particular enterprise can be summarized by $\sum(Ic(ai)+ Ii(ai) + Id(ai) + Il(ai))$, where Ic is the financial impact function of confidentiality lose, Ii is the financial impact function of integrity lose , Ii is the financial impact function of integrity, Id is the financial impact function of availability and Il is the financial impact function of legal force lose. We can argue that a company that doesn’t use forensics techniques is exposed to a financial risk of $\sum(Ic(ai)+ Ii(ai) + Id(ai) + Il(ai))$. Now, the question is how digital forensics can reduce this risk. Digital forensics will be used as a curative tool. Forensics techniques will be used after the attack when an impact has been detected. In this scope, it will be only useful to demonstrate legally the cybercrime and to try to obtain compensation accorded by a court of law. If we consider our maximal financial risk will be reduced by an amount equal to the compensation obtained through a court of law; but some fees must be paid to the lawyers. We can therefore express this risk by of $\sum(Ic(ai)+ Ii(ai) + Id(ai) + Il(ai))$ – compensations + fees. This financial risk formula is interesting:

- More $\sum Il(ai)$ is high, more compensations will be important due to difficulties to demonstrate the cybercrime
- If fees are higher than compensations, the forensics analysis won't be useful

So, optimizing the benefit of forensics investigation implies to reduce the risk of losing legal force of an asset and its traces (ideally $\sum Il(ai)$ must be closer to 0). It is also important to reduce the lawyers' fees by contracting a legal insurance. Legal insurance is marginal compared to cybercrime compensation. In this situation, our risk can be evaluated to $\sum(Ic(ai)+ Ii(ai) + Id(ai))$ – compensations.

Compensations are relative to security incident of some assets and are at less equivalent to direct damages. In this case, the security impacts of these assets are at least covered. The risk equation becomes $\sum_{i<>j} (Ic(ai)+ Ii(ai) + Id(ai))$ - |delta| where delta is the difference between compensation and the impacts of assets aj.

This formula demonstrates that forensics reduces significantly the financial risk by suppressing the risk of the assets that can be fully covered by forensics. And an extra reduction is induced by compensations. In an ideal and idyllic situation, each asset can be traceable and all the legal demonstration of cybercrime can be produced in this case forensics can generate an extra benefit equal to |delta|.

V. Challenges of Investigating Virtualised Corporate Infrastructures

The concept of *virtualization* is not new in the field of ICT. It dated back to the inception of programming language compilers that virtualizes the object code [8]. However, the concept of *virtualization infrastructures*, where physical resources are dynamically mapped to address the spontaneous business needs, is relatively new. Moreover, the scale and scope of this novel concept brings several challenges for its deployment including a lot of uncertainty as to how and where to implement security [5]. The inherent nature of virtualization requires totally different security provisioning approach than the classical one developed decades ago.

Classical digital forensics techniques and solutions require precise information of the underlying infrastructure to perform investigation and conceive the sequence of events. They cannot be applied to these emerging infrastructures due to the intrinsic characteristic of virtualization that provides abstraction to the underlying resources and infrastructures. This section examines the challenge of investigating virtualized corporate infrastructures that will have to be addressed to ensure smooth and secure transition from the classical enterprise information architecture towards virtualized one.

A. Conducting Security Audit Investigation of Future Internet-based Virtualization infrastructures

Security audit assess the security of the networked system's physical configuration and environment, software, information handling processes, and user practices. While it is similar in terms of investigation, it is carried out before commissioning of a system and then on regular basis to ensure the desired functioning of a system. Whereas the investigations carried out by the digital forensics team is the post incident activity where a malicious activity successfully carried out its nasty action. However, in terms of *investigating* an ICT infrastructure, both have similar challenge of dealing with virtualization paradigm. We have therefore used our previous work on security audit [9] to leverage the work on applying digital forensics in the virtual infrastructures.

B. Case-study: Payment Card Industry Data Security Standard (PCI-DSS)

Various security audit standards such as Payment Card Industry Data Security Standard (PCI-DSS) require audit of the physical controls [10]. The virtualization infrastructures provide an abstraction layer to the underlying lower-level details. This situation raises several security concerns such as multitenancy; lack of security tools [11]; and disparity with the classical IT security audit practices.

There exist a number of generic monitoring tools such as hardware monitoring (e.g., HP Insight Manager, Dell Open Manage, VMWare Virtual Center, etc.), performance monitoring (e.g. VizionCore, Veeam Monitor, Vmtree, Nagios, etc.), machine state monitoring (e.g. Virtualshield, Logcheck, etc.), and security monitoring (e.g. intrusion detection, honeypots, etc.). However, these tools may not be suitable for security audit controls of virtualization infrastructures as physical controls can be distributed that will require onsite checks by the local controllers. There is a strong need of a new set of matrices for measuring security strength. With more reliable matrices, new check-pointing models need to be developed. Besides these technical requirements for carrying out security audit of the virtualization infrastructures, there is also a need of new regulations/legislations for the cross-border deployment of resources used in virtualization infrastructures. This work is the continuation of our previous work on analyzing the overall security requirements of deploying virtual infrastructures [12].

VI. Discussions

The scope of digital forensics outside the criminology sphere was hardly explored in the past. However, the broadened scope of corporate ICT infrastructures and the reliance of core businesses on these infrastructures are pushing the paradigm shift in this domain. Some recent literature shows the exploration of digital forensics in the corporate sector [13,14]. However, these efforts are mainly focused on the philosophical possibilities. They do not provide any concrete model or design approach towards the inclusion of digital forensics practices in the routine operations of corporate ICT infrastructures. Likewise, a set of best practices for computer forensics is proposed in [15] that describe some effective ways of carrying out the digital forensics analysis in the post-incident situations without any specific link to the commercial side of employing these techniques in the business environments.

There are the genuine predictions that near future cybercrimes will be driven by the *clouds* and virtualization infrastructures [16]. We believe that businesses and law enforcement agencies won't be able to cope with this wave of contemporary crimes with the classical digital analysis approaches. Digital forensics is often a very painstaking task that consumes enormous resources and takes considerable time to develop a sequence of events that is acceptable by the courts. An example is the FBI investigation of ENRON scandal [17] where FBI gathered and analyzed 31 terabytes of digital data from 130 computers; thousands of e-mails; and more than 10 million document pages. The entire investigation took five years while the total monetary costs incurred remained largely unknown. With the proliferation of computing through virtualization infrastructures and the evident increase of related crimes, the law enforcement agencies will simply be overwhelmed with the demand of providing digital forensic analysis requests. Therefore, there is a strong need for the businesses to include digital forensics in their corporate security strategy. They should use these technologies within the legal framework covering their activities.

We have carried out a risk analysis to show the impact of not using the digital forensic solutions by the enterprises. We proved that loss of clientele and sanctions from the regulatory bodies might severely harm the business interests of those enterprises who will not employ the digital forensics technologies for the protection of their business interests. A similar concern is reported in [18] that predict *fall of forensic research behind the market* in the next ten years if various disjoint research efforts are not harnessed together in a systematic way.

VII. Conclusions and Perspectives

We have presented a non-classical approach towards the digital forensics analysis in this paper. We argue that enterprise information architectures can improve their overall quality of protection if digital forensics technologies are made their integral part. We presented a framework for embedding digital forensics analysis techniques at several stages of enterprise information lifecycle followed by a set of best practices for operating an enterprise information security policy together with the digital forensics techniques and tools.

There are a number of open issues that we plan to address in the near future. The foremost is the use of digital forensics solutions in the virtualization infrastructures such as *open clouds*. Major challenges of virtualization infrastructures are the absence of a fix perimeter of the ICT resources; and the unknown details of the underlying physical infrastructure.

Acknowledgment

The research leading to the results presented in this paper has received funding from the Walloon Region of Belgium through the project CE-IQS (Centre d'Expertise en Ingénierie et Qualité des Systèmes) and the European Union's seventh framework programme (FP7 2007-2013) Project PONTE under grant agreement number 247945.

References

[1] K. S. Rosenblatt, High-Technology Crime: Investigating Cases Involving Computers, KSK Publications, ISBN 0-9648171-0-1, 1995

[2] The United States Sarbanes Oxley Act 2002 – http://uscode.house.gov/download/pls/15C98.txt <retrieved: Nov. 2011>

[3] J. Mullis, The Impact of the Sarbanes-Oxley Act of 2002 on Computer Forensic Procedures in Public Corporations, University of Oregon, July 2009 – https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/9480/Mullis-2009.pdf <retrieved: Nov. 2011>

[4] International Organization for Standardization, Standard ISO27002: Code of practice for information security – http://www.27000.org/iso-27002.htm <retrieved: Nov. 2011>

[5] R. Adhikari, The Virtualization Challenge, Part 5: Virtualization and Security, TechNewsWorld, March 2008

[6] F. Chong, G. Carraro, and R. Wolter, Multi-Tenant Data Architecture, Microsoft Corporation, June 2006

[7] International Organization for Standardization, Standard ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements

[8] J. Bloomberg, Building Security into a Service-Oriented Architecture, ZapThink Whitepaper, ZapThink LLC Publisher, May 2003

[9] S. Naqvi, G. Dallons, C. Ponsard, and P. Massonet, Ensuring Security of the Future Internet-based Virtualization Infrastructures (Position Paper), IEEE Symposium on Security and Privacy 2010, Oakland, CA, USA, May 16-20, 2010

[10] Payment Card Industry Data Security Standard (PCI-DSS) https://www.pcisecuritystandards.org/ <retrieved: Nov. 2011>

[11] E. Haletky, Virtualization Security – Security and Compliance within the Virtual Environment, DABCC online article 08 April 2009 http://www.dabcc.com/channel.aspx?id=279 <retrieved: Nov. 2011>

[12] S. Naqvi, P. Massonet, and J. Latanicki, Challenges of Deploying Scalable Virtual Infrastructures - A Security Perspective, CESNET Conference on Security, Middleware and Virtualisation, Prague, Czech Republic, September 25-26, 2008

[13] B. Nikkel, The Role of Digital Forensics within a Corporate Organization, IBSA Conference, Vienna, Austria, May 2006 – http://www.digitalforensics.ch/nikkel06a.pdf <retrieved: Nov. 2011>

[14] J. Heiser, Digital Forensics and Corporate Investigations, Gartner, November 2005 – www.gartner.com/teleconferences/attributes/attr_144863_115.pdf <retrieved: Nov. 2011>

[15] Scientific Working Group on Digital Evidence (SWGDE) Best Practices for Computer Forensics V1.0, 2004 – http://swgde.org/documents/swgde2005/SWGDE%20Best%20Practices%20_Rev%20Sept%202004_.pdf <retrieved: Nov. 2011>

[16] Trend Micro Report: The Future of threats and Threat Technologies – How the Landscape is Changing, December 2009 – http://affinitypartner.trendmicro.com/media/34716/trend_micro_2010_future_threat_report_final.pdf <retrieved: Nov. 2011>

[17] Federal Bureau of Investigations (FBI), Digital Forensics: It's a Bull Market, July 2007 – http://www.fbi.gov/page2/may07/rcfl050707.htm <retrieved: Nov. 2011>

[18] S. Garfinkel, Digital forensics research: The next 10 years, Elsevier Science Directi Magazine Digital Investigation vol. 7, pp 64-73, 2010 – http://www.dfrws.org/2010/proceedings/2010-308.pdf <retrieved: Nov. 2011>