Research Paper E-ISSN NO : 2455-295X | VOLUME : 9 | ISSUE : 8 | AUGUST 2023

STATISTICAL ANALYSIS OF CYBER SECURITY IN BUSINESS ORGANIZATIONS

DR. ABDULBASIT BANGA [1]

[1] ASSISTANT PROFESSOR, COLLEGE OF COMPUTING AND INFORMATICS, SAUDI ELECTRONIC UNIVERSITY, JEDDAH, KINGDOM OF SAUDI ARABIA.

ABSTRACT:

Many more corporate entities today are utilizing ICTs to identify opportunities for innovative and customer-centric, value-added products and services. Indeed, information systems have been key characteristics of any growing and successful business, as they utilize ICTs for business value creation. The key motivation for the huge investment in IT infrastructure is to ensure an upsurge in revenue and retention of a sizable market share. Computer usage policy is a document that provides guidelines that regulate the acceptable usage of these systems by end users. The provision of these guidelines also serves as benchmark metrics in assessing the abuse or misuse of corporate information systems. This misuse and/ or abuse are referred to as violations of computer usage in this study. 10 users selected randomly from within each unit of a multi-lateral company, were observed for violations. Live computer forensics techniques utilizing EnCase, Microsoft reporting tools, WinHex, etc. This paper further analyzes and addresses the causes and effects and offers measures to mitigate computer usage violations.

KEYWORDS:

LIVE COMPUTER FORENSICS, COMPUTER USAGE POLICY, CORPORATE POLICY VIOLATIONS, LIVE DIGITAL FORENSICS, DATA SHARING, AND USE.

I. INTRODUCTION

Numerous information technology managers strategically use information technologies to identify the opportunities associated with IT-enabled value-added products and services [1].

Interestingly, the study revealed that all end users that were monitored violated one policy or the other. This situation is of grave concern to all corporate entities if they must survive in this cyberspace or may be counted amongst the statistics of cyber victims who closed shop because of security breaches or compromises.

The key motivation for the huge IT infrastructure investment is to offer cutting-edge customer-centric products and services, whilst ensuring that the revenue is up, and a sizeable market share is retained. With this huge capital outlay, organizations are mindful of how computer and internet resources are used in the execution of corporate objectives or vision. Smith [2] asserts that information and data are economic drivers for business today and that the cost of lost data could be substantial. The author in [1] also alludes to that fact by indicating cyber threats to organizations could possibly lead to business closure as well as various costs due to vulnerabilities exploited. Corporate entitling various vulnerabilities, which can cause such debilitating disruption of their business infrastructures.

The end user is said to be the weakest link in the cyber security chain. About 43% of all data breaches are attributed to the negligence of end users [3]. This is partly due to several end users "unwittingly" choosing weak, often dictionary-based, passwords. The other part of the equation is strict adherence enforcement of appropriate corporate computer or internet usage policies. Admittedly, the security versus convenience curve is inversely correlated.

Corporate security policies are high-level statements that provide guidelines to end users for making appropriate business decisions. The object is to provide a framework for managing corporate cyber security resources. The policy, which is a living document, offers clear definitions, standards, procedures, and practices that must be complied with by all end users. Several issues are pertinent in enforcement and/ or ensuring compliance. What constitutes corporate policy violations? How do corporate entities assess, detect, and prevent violations? What mitigation measures are available to them? Obviously, non-compliance with the stipulated policy is deemed to be a violation. End users ought to be monitored to ascertain compliance or otherwise; the systems are thoroughly observed, anomalies must be detected and analyzed, and appropriate mitigation measures implemented to curtail any risks.

This research paper attempts to assess the extent of corporate security policy violations by employing live computer forensics data acquisition and analysis.

A. The Issues at Stake

As many more corporate entities use information systems for business functions and production, various infractions or violations occur which are often overlooked or pass unnoticed. Though not all such incidents lead to catastrophic risks, they could, nevertheless, impact

production in the long run. Since security or cyber risk is a business concern, appropriate measures ought to be instituted to monitor, report, analyze, and mitigate the survivability of the entity. Due to data proliferation and dynamics of usage and processing, lots of corporate data resides on employee-owned devices or media. The conventional norm of cyber security policies that control and managing organizational data is now inadequate. The risk of end users sharing data outside the confines of the corporate intranet poses serious concerns with the possibility of data leakage or unauthorized access, modification, or even usage. The issue is some organizations do not have policies to deal with such security breaches, let alone to correct them and/ or prevent a future occurrence. Where the policies exist, constant monitoring could facilitate the mitigation mechanisms. The object of this study is to examine the extent and severity of corporate security violations. From a computer forensics perspective, live analysis is more plausible to unearth the violations and their root causes as some evidence could be lost with a dead analysis. This paper is organized as follows: this preamble deals with the background, and it's followed by the literature review on security policy and computer forensic analysis. The methodology is presented next, followed by the results and analysis, and the extent of violations, causes, and effects are discussed in the conclusion.

II. LITERATURE REVIEW

This section discusses the related works and state of the art in cyber security policy initiatives and what constitutes violations.

1) Cyber Security: In the algorithm of approaches to secure organizations, the initial step is establishing the security policy. Incidentally, most organizations put this all-important step at the end of the flow, if any. Essentially, a cyber-security policy is a set of rules that govern how the organization manages, protects, and controls access to its information assets, as well as administers end users. Usually, these rules are specified to safeguard the Confidentiality, Integrity, and Availability (CIA) security objectives.

End users are guided by the policies to make present and future decisions. The policy serves as a guidance that defines and classifies the mission-critical assets, and the extent of protection measures required. It must be noted that the policy is periodically reviewed, with re-classification of assets thus, the security policy is said to be a" living document".

The policy also specifies the systems that can be installed on the network, as well as the procedures to be followed. A variety of issues are raised: what traffic data is collected and monitored? How is it carried out? Who has access to which systems? What determines a violation or an incident? How is it addressed and reported?

In summary, a cyber-security policy is a set of rules defining the roles and responsibilities, which provides strategic directions for decision-making and the appropriate use and level of protection of information assets. It also stipulates the measures to be taken in the event of violations, such as reporting and correcting violations in conformity with the policies.

A violation is a cyber-incident that breaches laid down security policies or poses a threat, which has the possibility to compromise computer best practices [4]. Indeed, a cyber-security violation is any breach of rules, policy statements, procedures, processes, or guidelines, whether intentional or inadvertent, irrespective of the extent and severity of the damage. For this study, we categorized security violations into three key themes namely computing resources usage, network resources usage, and data sharing.

2) Computing Resource Usage: Here, we discuss computing resources or account usage. This policy establishes the essential guidelines and rules that govern end users' behavior regarding the use of computers and computing resources. These are variously referred to as computer-acceptable usage, internet acceptable use, electronic resource use, or computing resources usage policy, etc. Typically, computing resources are not to be used for the conduct of private business or any activities that are illegal by governing laws.

Every computer policy enjoins end users to be the custodian of their accounts [5] [6]. It also makes all end users directly responsible for transactions carried out with their user accounts. In this regard, creating generic user accounts for sharing by a host of users is prohibited. Generic accounts are not permitted in most security-conscious organizations. In the event of cyber incidents, it may be very difficult to trace and establish the causes and culprits. In cyber security, it is necessary to guarantee that an entity initiated or originated a transaction; this property is known as non-repudiation.

Accurate tracing and identification of transactions originating from generic accounts are paramount in reducing any ambiguity- ties and thus, mitigating associated risks. The author in [7] posits that the use of generic or service accounts is a blatant violation of the non-repudiation dimension in cyber-security policy. He recommended that generic account usage could be curtailed by assigning high-level access rights to responsible system administrators. The weak password could be used as a "vulnerability bridge" for intrusion into corporate networks. In this regard, the password should not be easily guessed; the user's name or objects or activities that are easily associated with a user should never be used to create a password.

3) Network Usage: The network usage policy stipulates the regulations for the use of corporate network facilities and resources. The essence of the network resources policy is that usage is deemed a privilege accorded to end users and so they must act responsibly.

The corporate network has interfaces with the internet, and these could be conduits for intrusions. In view of that, organizations regulate network usage policies to, for

instance, restrict certain websites that are most likely susceptible to hacking activities. Porn sites and P2P links could be possible targets. These regulations are meant to ensure that end users focus on corporate business and not unnecessary pleasurable visits. Strict use of the network is documented, and several privilege levels are created to maintain decent access to the network. It is important to have a hierarchy of access to various network resources in an organization [8]. Certain internet sites are restricted from access for security reasons and others to keep employees focused on work during business hours. Unauthorized access to such websites is considered a policy violation and may be subject to sanctions such as entire denial of access to the internet, or some punitive measures, as the policy may prescribe.

4) Data Sharing and Usage: The data sharing and use policy stipulates and manages the permissions granted to providers and end users, for usage and transmission of data across the organization. The policy entails the conditions of use and processing of data, as well as acknowledgment of the data sources. Data used in the organizations are the legal assets of those entities. So adequate steps are usually put in place to ensure that only authorized data is shared and with only authorized users on a need-to-know basis. Carrying corporate data off-side without express permission is considered theft and a violation of computer security policy. As part of the policy, USB ports are usually blocked to prohibit the copying of files onto external storage media. Data sharing amongst authorized entities is carried out via the corporate internet and/ or through protected file servers, using FTP. Some employees could argue that they needed to continue with a particular task, outside of the office. Unless appropriate permission is sought, copying such data would be deemed a violation of corporate security policy. Audit with the registry keys such as would reveal any such data sharing, with some details on the time stamp and device ID [9], [10]. Computing devices can be tracked, whenever they are mounted or previously attached using the registry keys [10]. Records are logged into appropriate registry keys. In a live forensic analysis, the "Regedit" command can be executed on a computer with these registry keys and then saved as text files for readability and ease of analysis [10]. Detailed analysis of these logs will reveal the timestamps of when the device was attached or mounted.

A. LIVE DIGITAL FORENSICS

The essence of digital forensics is to acquire evidence; to recover and examine the incidence for digital evidence. Typically, it involves evidence acquisition and examination of both hardware and software, such as PCs, laptops, servers, databases, storage media, deleted files, unallocated clusters or sectors, emails, web browser cookies, etc.

A key concern in digital forensics is about the integrity of the evidence gathered and the admissibility of the analysis in a court of competent jurisdiction [11], [12]. Besides a credible chain of custody, amongst others, the volatility of the memory contents is very paramount, as valuable evidential data could be lost because of rebooting or shutting down the systems. So, live forensics acquisition is meant to ensure the integrity of the evidence, to acquire vital data that could have been otherwise lost, and to secure the suspected crime scene.

In this study, we delimit the discussion to live network forensics, whereby traffic data are collected and analyzed to ascertain the occurrence of incidents or attacks [13]. Network processes and logs are monitored, and traffic data are examined for any anomalies and/ or violations of policies.

III. METHODOLOGY

This study is delimited by the accessibility to live corporate data. To assess a representative network, the head office was used as the case example, and every effort is made to conceal its identity. We realized that the case company had 10 departments with almost 100 computers. So, we randomly sampled one computer per department, constituting 10 samples for the assessment.

A. RESEARCH DESIGN AND APPROACH

This study assessed the violations of corporate computer policies using live computer forensics data acquisition analysis. This technique is appropriate for the types of violations being investigated. We employed forensics tools such as EnCase, WinHex, and MS logs, and associated reporting tools for the study. This warrants the research design to use both quantitative and qualitative approaches.

During the study period, the sample computer resources were monitored, and the logs collected were scrutinized for possible violations. Based on the data acquired, strategic interviews were conducted with end users, especially the identified violators to ascertain their motivations.

B. ETHICAL AND VALIDITY CONSIDERATIONS

This study assured the policy violators of their confidentiality and so, we anonymized their user credentials as well as the departments or units investigated. In accordance with [14], we were guided by both normative and descriptive privacies of the samples. Here, normative privacy ethics is concerned with efforts to ensure that the users' privacy is not violated in any form under this study. Similarly, descriptive privacy is concerned with ensuring that a user's privacy is kept intact, even with this study.

Reliability and validity are said to be the foundational pillars of any viable scientific inquiry. The reliability of the study ensures that the findings are repeatable. Whereas the validity of the study ensures that due process was followed in selecting the samples and in carrying out the data acquisition and analysis. This is key in all computer forensics assessments since the digital evidence adduced must be admissibly accepted by stakeholders.

IV. DATA ANALYSIS AND FINDINGS

This section deals with the results and findings of the study.

A. ACCOUNT USAGE - EVIDENCE OF VIOLATION AND ANALYSIS

Account usage policies usually inform the user on how to use the computer account. These policies usually state parameters such as password complexity, restrictions on account sharing, password disclosure to colleagues, user data security, etc. Typical policies that can be violated under this category will be password complexity requirements. The selection of passwords spans around the type of password and the complexity requirements that ought to be met when choosing them. A thorough review of the corporate account usage policy enjoins users to set passwords that meet certain complexity measures, as well as comply with the number and type of characters used. Typically, a chosen password must not be something that is easily associated with the user. The key concern is that the password must be safeguarded against both external and internal attacks. The password must be unique,

TABLE I. RANDOM QUERY FOR ACCOUNT USAGE VIOLATION - PASSWORD

Department	OS	User Privilege	Pass Recovery	Pass Strength
Customer Service	Win XP	Standard	avad1	59%
Accessories Sales	Win 7	Standard	guyguy4u	55%
Equipment Sales	Win 7	Local Admin	mylord24	42%
Power Supply	Win 7	Standard	123india	39%
Executives	Win 7	Local Admin	stive1	25%
Human Resource Management	Win 7	Standard	apple-2013	62%
Technology	Win 7	Admin	CR@ admin. pat.2694@henry	100%
Finance	Win XP	Standard	guj.123	37%
Main ProductSales	Win 7	Standard	1india	37%
Installation	Win XP	Standard	my@2012	97%

FIG. 1. PASSWORD STRENGTH FOR VARIOUS DEPARTMENTS

hard to guess and must meet the set complexity requirements. The author [15] explains scenarios where password stays in memory, which could be exploited even when the user has logged off.

Using a memory image, such passwords could be detected. WinHex was used to capture passwords used by users on the sampled computers from RAM. The data acquired were assessed using Meta Beta Geek's password meter to

ascertain their strengths; the results are tabulated in Table-I and illustrated in Figure-1.

Thus, the average password strength for the sample computers is 54.5%, as computed in Equation-1. It is observed that some administrative accounts fell below the average and had weak passwords. There's a high risk of being compromised, possibly using an opportunistic password-guessing algorithm. Weak passwords may be exploited by both external and internal attackers, especially insiders with nefarious motivations. According to the author in [15] accounts with password strength of about 60% are cracked within 4 days, implying that 54.5% may be cracked in a shorter period.

B. NETWORK USAGE - EVIDENCE OF VIOLATIONS

Due to the wide scope of possible violations in this investigative category, we categorized violations into 2 parts, i.e. email and internet usage violations.

1) Evidence Gathering - E-Mail Violations: Our focus for this study, however, will be on email violations per the company's policy based on an email client system where an email application is installed on the user's PC such as Outlook, lotus, etc.

The sample organization uses MS Outlook, the client application. Using live analysis techniques, violations regarding using corporate emails for personal communications were investigated. A look through the company's policy about emails revealed that company emails are not to be used for personal communications. This investigation was carried out by examining the email header information.

- Email Header - Evidence Gathering: The email header holds a lot of valuable information from which the sender of a message, the recipient address, and the protocols used in communication can all be recovered from. With modern protocols such as SMTP protocols, the IP address used in communication can also be obtained [?]. Cognizant of the ethical considerations of confidentiality, certain details pertaining to the corporate ID of the sample entity are purposefully suppressed using asterisks; i.e. IP address and Domain Names.
- The information gathered from the header shows that the mail was sent to a webmail account and had an attachment. The subject of the mail also suggests that this mail was business correspondence. Further analysis can be carried out using EnCase for which the results are as follows. The aim of this investigation was to gather emails sent to webmails and querying through them to disclose which ones were related to business and which ones were not. Using EnCase keyword search, the results are tabulated in TABLE-2.
- Total E-Mails = 335
- Total Personal E-Mails = 95

$$\text{Average} = \frac{\text{Total Valu}}{\text{Total Entities}} = \frac{545}{10} = 54.5 \quad (1)$$

$$\text{Ratio of Personal Communication} = \frac{95}{355} = 26.76 \quad (2)$$

Using basic arithmetic, the average password strength for these computers is calculated as the sum of these passwords' strengths divided by the number of computers under investigation.

This means that about 27% of emails were meant for personal communications, rather than business-oriented, and thus constitutes violations.

TABLE II. AIL EVIDENCE GATHERING E-M

Department	Mail to/from Gmail	Mail to/from Yahoo	Mail to/from Rediff	Personal	Business Related
Customer Service	3	5	0	8	0
Accessories Sales	20	35	0	5	50
Equipment Sales	26	19	2	7	40
Power Supply	5	16	6	7	20
Executives	8	0	7	5	10
Human Resource Management	20	20	8	10	38
Technology	14	14	10	25	13
Finance	8	9	3	10	10
Main ProductSales	20	29	15	10	54
Installation	15	16	2	8	25

TABLE III SER-WISE INTERNET USAGE BANDWIDTH			
User	**Bandwidth Kilo Byte**	**Requests hits**	**Browse Time hh:mm:ss**
User-J	14804690456	9756	29:38:21
User-I	8509139196	2214	32:15:23
User-H	6713034282	11521	19:35:41
User-G	3452305719	51967	61:50:01
User-F	2853295676	145688	10:18:25
User-E	2466633710	8256	14:05:53
User-D	2394599774	33032	49:05:13
User-C	2244390171	9493	28:18:07
User-B	2212931800	14978	29:35:09
User-A	2043057307	18212	95:27:25
Total Usage	**47694078091**	**305117**	**370:09:38**

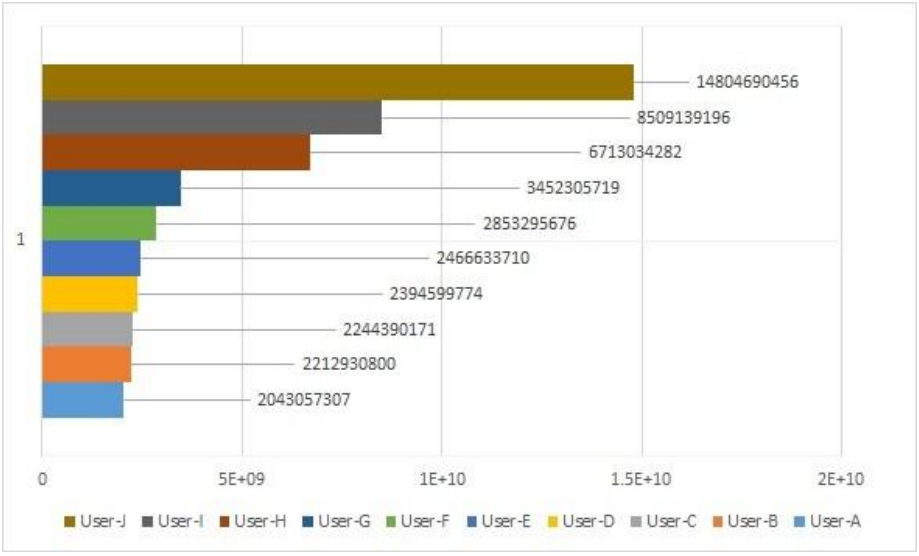
TABLE IV AVERAGE INTERNET USAGE - DAILY USAGE-PER-USER			
User	**Total Browse TimeMinutes**	**Average Browse Time Minutes**	**Approximate Browsing PeriodHours**
User-J	1778	88.9	1.48
User-I	1935	96.75	1.61
User-H	1175	58.75	0.97
User-G	3710	185.5	3.09
User-F	618	30.9	0.52
User-E	845	42.25	0.70
User-D	2945	147.25	2.45
User-C	1698	84.9	1.41
User-B	1775	88.75	1.48
User-A	5727	286.35	4.77

The total allowable browse period stipulated in the case sample organization's policy was 40 minutes during working hours. There were also allotted user quotas. So, computing the total allowable monthly browse quota is 800 minutes, given 20 working days per month. It is apparent that 200% of sample users had all violated the internet usage policy as they have all exceeded the allowable time given. High data usage constitutes an outright violation. It is also possible for a user to download a large volume of data for a short period. Probing further, in respect of lengthy browsing periods constituting violations, it also meant that users had spent a chunk of their working period accessing the internet instead of attending to scheduled work. In accordance with ethics, we have modified the actual first names of culprits to disguise any semblance of their identity and that of the company.

- User-A's Browsing Time per Month = 95:27:00

2) Internet - Evidence of Violations: The Internet usage policies of our sample organization strictly stipulate the website that should not be accessed. Attempting to access and/ or accessing those sites are considered violations. Reports from the websense server show internet usage statistics for users over the study observation period of 1 month and are depicted below.

FIG. 2. USER-WISE INTERNET USAGE BANDWIDTH



- User-A's Browsing Time in Minutes =5727
- User-A's Average Browsing Time per Day = 286.35

But expected working minutes is given by 8*60*20 = 9600 per month considering 8 hours per day. This culminates into 4.77 hours of browsing time per day, constituting almost 60% of working hours used to access the internet. Obviously, this is a violation of internet usage. This table below depicts the extent of internet usage violations by the samples.

About 69% of the violated internet access was associated with streaming sites and general internet web surfing. These web access were not related to business operations in any way. The high percentage value indicated that a lot of production time was used to access the internet rather than contributing to productivity. Records from the reports also showed high periods of access for these sites.

EnCase was also used to further probe other forms of internet usage violations. Some users with a good sense of IT skills deleted internet history or disabled caching altogether in their internet browsers. Assuming that the user accesses these websites in a way and manner that makes his/ her internet usage for these sites minimal, his logs can or may never be captured in these reports. The rationale behind querying for this report from the websense is usually used to find out the extreme usage of sites by users, thus a user's minimal usage may be tampered with. As the policy clearly prohibits access or attempts to access certain prohibited sites, his/ her minimal access is still considered a violation and should be detected using forensic techniques.

V. CONCLUSION

Firstly, the objective of this research has been to determine possible corporate computer usage violations for this organization. This study set off with an extensive review of some related works on corporate computer policy violations as the basis for the research design. Policies are said to be guidelines for corporate computer usage and enforcement. Violations such as password complexity requirements, email usage, account usage, Internet usage, etc. were observed to have been violated by the sample computer users sampled in the study. This goes to show that corporate policies violation could be seen to a larger extent if the research was performed using more computers and the policies investigated more thoroughly.

A. IMPLICATIONS OF VIOLATIONS ON THE ORGANIZATION

Discovering the policies violated had practically no meaning without identifying the possible effects it may have on the organization's network and operations. For instance, users who have spent enormous periods on the Internet tend to contribute little to productivity. The time required of them to perform corporate duties is used for non-business-related surfing and/ or entertaining themselves on these sites. Weak passwords also meant that company information could easily be accessed by internal and/ or external attackers alike. Sensitive corporate assets, such as trade secrets and designs could be leaked out to malicious and unscrupulous entities. Companies have had to shut down because of lost trade secrets; corporate executives lose their jobs due to data leakage; the extent of reputational damage is unimaginable, etc. These are some of the implications that violations of computer usage can have on the company.

B. CAUSES AND EFFECTS OF CORPORATE VIOLATIONS

One of the main reasons for the various violations was the weak enforcement schemes used in the organization. Since the complexity measures for passwords set up were not properly enforced, users we allowed to set weak passwords on the domain. From the interviews with some of the violators and members of the Technology department, it was admitted that some of the users were not properly inducted into the computer usage of the

organization which was seen as a major vulnerability. Another cause deduced was what appears to be unprofessionalism on the part of some technical staff. It was realized that certain users were given elevated unwarranted privileged access. Finally, the policy document was not updated regularly and at the time of this research, the policy document has been used for 6 years without any review. Certain do's before were now a violation and they had not been properly documented.

C. SUGGESTIONS AND RECOMMENDATIONS

The creation of Group Policy Objects (GPOs) with set-defined responsible servers could be used to set and define explicit conditions that will affect users in a more brute manner when selecting passwords. Defining precisely what encompasses password complexity will help prevent the formation of seemingly weak passwords by users. Users should be given the right induction and appropriate briefing on the policies. Users may not fully understand the essence of the policy document and sometimes implementing or honoring such policies may become burdensome for users. Especially with little or no orientation to ITIIS systems. The Technology team should be refreshed in their role and essence in the organization as the custodian and law enforcers for IT/ IS usage. Professionalism is thus key to all their functions in any organization. The policies governing IT/ IS usage for the organization should have an expiration period which can be subject to change before its expiration depending on the changing trends in IT usage. Also, the organization's operation should be aligned with the reclassification of computer assets and reviewed policies that govern computer and network usage. Furthermore, there should be clearly defined sanctions for policy violations. This will represent the last layer of policy enforcement. Violation of policies could be assumed to be forever existent, minimizing it or eradicating it could depend on the sanctions tied to these violations. Users will be more cautious in using IT resources knowing the possible consequences they may encounter after its abuse. This will present a more rational use of IT/ IS infrastructure.

In conclusion, we have endeavored to address the key issues raised at the beginning of this study. Several policy violations were identified and critically examined, and some solutions were preferred. The possible causes and implications were duly dealt with.

VI. FUTURE WORKS

Computer forensics presents vast diversified areas of research for various questions. Currently, a host of several mobile platforms are used in place of computers for business operations in organizations. Employees nowadays may push corporate email onto their phones, tablets, and other mobile platforms. Company data can be stored on these platforms for ease of access. Further work will therefore include mobile forensics investigations into policy violations on these devices and their impact on data leakage.

REFERENCES

1. Ezer Osei Yeboah-Boateng," Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability", Ph.D. Thesis, Institute for Elektroniske Systemer, Aalborg Universitet, vol.1, ed.1, ISBN: 978-87-7152-038-5, 2013.

2. David M Smith," The Cost of Lost Data-The importance of investing in that 'ounce of prevention", Graziadio Business Review, Pepperdine University, vol.6, no.3, 2003

3. " An Information Resource for Data Breach Prevention and Response", Data Breach Statistics, IBM Security Services, 2014

4. " Report Cyber Risks", Cybersecurity and Communications External Affairs, Homeland Security, December 2013. [Accessed 01st Feb 2015] www.dhs.gov/report-cyber-risks

5. B Ruppert," Protecting Against Insider Attacks" - White Paper, SANS Institute, 2009

6. Deb Shinder," Protecting Against Insider Attacks in Todays Network Environments" - White Paper, WindowsSecurity.com, March 2011

7. Garo Doudian," Generic Accounts and Non-repudiation," SANS/ GIAC Practical Assignment for Glssal Information Assurance Certification, Version: 1.4b, June 2004.

8. " Active Directory Domain Services Overview," Microsoft Corporation, February 2012 [Accessed 01st Feb 2015] www.technet.microsoft.com/en-us/library/hh831484.aspx

9. " USB Device Registry Entries," Microsoft Development Center - Hardware, Microsoft Corporation, [Accessed 01st Feb 2015] www.msdn.microsoft.com/en-us/library/windows/hardware/jj649944(v=vs.85)

10. John J Barbara," Windows 7 Registry Forensics: Part 6," Forensic Magazine-On the Scene and In the Lab, October 2012 [Accessed 01st Feb 2015] www.forensicmag.com/articles/2012/windows-7-registry-firebsucs-part-6

11. S Yadav," Analysis of Digital Forensics and Investigation," International Journal of Computer Science and Information Technology, vol.01, no.03, 2011

12. Rayan Jones," Safer Live Forensics Acquisition" - A Research Report, Computer Science Laboratory, University of Kent at Canterbury, United Kingdom, 2006

13. Bill Nelson, Amelia Phillips, and Christopher Steuart," Guide to Computer Forensics and Investigations," edition. 04, Course Technology, Cengage Learning, 2010.

14. Roux and Falgoust," Ethical Issues Raised by Data Acquisition Methods in Digital Forensics Research," Journal of Information Ethics, vol.21, no.1, pp.40-60, 2012.

15. A Kumar," Discovering Passwords in the Memory," Paladion Networks,2003

16. B Schneider," The Home Computers Security Center," Feb 2009 [Accessed 01 Feb 2015] www.lockdown.co.uk

17. V V Riabov," SMTP - Simple Mail Transfer Protocol," River College,2005