Case Report

Open Access CrossMark

Digital forensics in the audit of public private partnerships - a case study

Volume 4 Issue 6 - 2017

Israel Sadu
Auditor, OIOS, United Nations, Jordan

Correspondence: Israel Sadu, CIA, CISA, CFE, CRMA, CCSA, CRISC, CIPSFR, MBA, Msc, Phd,, OIOS, United Nations, 2, Abdul Fattah Al May street, Al Jandaweel area, Amman, 11194, Jordan, Tel 962 796798712, Email isadu@unog.ch

Received: May 13, 2017 | **Published:** June 01, 2017

Introduction

Information Technology has revolutionised all walks of human life and their business processes are no exception. Information technology and business are becoming inextricably interwoven. I don't think anybody can talk meaningfully about one without the talking about the other.[1] Sadly, the same technology once considered being a boon to cover more ground and provide economic and social services through enhanced efficiency is turning out be a bane due to its misuse and abuse. Today cybercrime is possibly the most frequent crime the nations all over the world face. According to a survey[2], cybercrime jumped to the second highest crime and only 37 per cent of the respondents of the survey had an appropriate incident response plan. If the trend persists , it is estimated that cybercrime damages are expected to cost $6 trillion by 2021, up from $3 trillion in 2015![3] With over $78 trillion of public sector expenditure world over, the organisations spend colossal amounts of their resources to establish effective and efficient deterrence measures to ensure that they provide the intended quality services seamlessly. The statutory audit organisations, known as the Supreme Audit Institutions (hereinafter referred to as 'SAIs'), have the mandatory responsibility to ensure that accountability of every penny spent through the tax payers money regardless of the modalities of their clients' operations. Broadly, their objectives, among others, are to ensure:

a. Control against the abuse or misuse of the authority entrusted to the Executive by the Legislature;

b. Provide assurance if the activities were being performed with due adherence to the canons of the financial propriety; and

c. Report on the performance on the programmes and policies through the established reporting mechanism to facilitate accountability.

Due to the constantly evolving changes in the operational environments of the public sector, the traditional accountability methods, including the oversight procedures and practices followed have come under pressure. The sources of pressure included, changing partnering arrangements, funding patterns, innovative technologies used, among others. These changes necessitate the statutory audit arrangements to remain aligned/ and or abreast with the changing business practices and constantly reinvent and reinforce their auditing methodologies. One such challenge is their ability to operate in situations that warrant a thorough understanding of the key business risks in the IT environment and competence to obtain and analyse evidence applying the digital forensic principles.

[1]https://www.brainyquote.com/quotes/quotes/b/billgates173262.html
[2]https://www.pwc.com/gx/en/services/advisory/...crime-survey/cybercrime.html
[3]www.csoonline.com/.../security/cybercrime-damages-expected-to-cost-the-world-6-tri...

Auditing public private partnerships

The financial crisis of 2008 brought about renewed interest in Public Private Partnerships (PPAs) in both developed and developing countries. Facing constraints on public resources and fiscal space, while recognizing the importance of investment in infrastructure to help their economies grow, governments are increasingly turning to the private sector as an alternative additional source of funding to meet the funding gap. The United Nations defines PPP as "*innovative methods used by the public sector to contract with the private sector who bring their capital and their ability to deliver projects on time and to budget, while the public sector retains the responsibility to provide these services to the public in a way that benefits the public and delivers economic development and improvement in the quality of life*".[4] Depending on the adequacy and nature of the statutory mandate given by the respective Legislatures, the SAIs may involve a review of the service provider's data and records as a part of the audit of the PPP projects. In the given case, the mandate of the SAI had an enabling provision towards this end. However, there were no clear provisions if the SAI's Auditors could search and seize the resources used in committing the crime if such a requirement arises during the course of the audit.[5] The world over, there are three types of arrangements: One, SAIs have specialised forensic audit teams with a clear mandate to search and seize the evidence in the crime scene. Second, SAIs may share the preliminary evidence in the crime scene with the state investigating authorities to investigate it further. Third, SAIs, in coordination with law enforcement agencies, form joint forensic teams who would investigate and report through appropriate legal proceedings to determine the quantity of loss, and perpetrators, among others. This paper, with the help of a case study, traverses through some distance in forensic investigation using the third approach.

Followed by a competitive bidding process, a particular Ministry in a country, entered into a PPA with a contractor (service provider)

[4]https://www.unece.org/fileadmin/DAM/ceci/publications/ppp.pdf
[5]Sadu Israel (2010) Forensic Auditing-Issues and Challenges for Auditors, Indian Journal of Public Audit & Accountability, Vol-III, No. 4 and 5, July-December 2010, p.81

to build, operate, and transfer to the Government (after 15 years) a toll bridge at a particular site owned by the Government. In return, according to the conditions of the PPA, the service provider was required to share 40 per cent of the revenue collected from the vehicular traffic that used the toll bridge with the Government on a monthly basis. Audit of this PPA formed a part of the annual work plan of the SAI of the country. The overall audit objective was to provide an assurance that the Ministry/Department responsible for implementing the PPA had established appropriate controls and procedures to ensure that the project was planned, executed and monitored in accordance with the PPA, with a focus on the adequacy of the revenue sharing arrangement. According to its mandate, SAI's auditors were allowed to access the service provider's premises, including the arrangements for the revenue collection and the records maintained for this purpose.

Red flag-mismatch between the expected and the actual revenue

The SAI's audit team noted during the field audit, among others, that the information on the traffic volume and the revenue shared with the Government from time to time appeared to be far lower than the expected volume. The team decided to compare these details with the expected traffic volume as indicated in the initial project feasibility study conducted by the service provider. A comparison of the given volume grossly (up to 50 per cent) deviated from the actual traffic. During its project visit, the team reviewed the adequacy of arrangements over key process such as toll collection at the entry site, cash management, and revenue sharing. The results were generally satisfactory, but the reason for the gross variation between the expected volume of traffic and the actual remained unanswered. After several rounds of discussion with the service provider's operating and managerial staff, the team decided to involve the State Forensic Unit to search and review the service provider's server room and other resources used in this activity. Comparison of the data for a randomly selected month indicated that the data matched in terms of the number of vehicles plied, revenue collected and the revenue due/shared. Nevertheless, considering the magnitude of the volume of revenue involved and the unanswered question about the reason for the huge variation, a joint investigation team was formed consisting of SAI's Auditors and the State Forensic Unit's Investigators to undertake a full-fledged investigation. This exercise involved a carefully planned and complex evidence collection process as explained below.

Digital evidence gathering, analysis and reporting

Digital evidence is fragile, prone to errors and manipulation and therefore it was required to be handled carefully which is commonly known as 'maintaining the chain of custody'. Digital Forensics, therefore, is the art and science of identification, collection, preservation, analysis, documentation and presentation of the digital evidence in a legally acceptable manner collected at the crime scene. In the given case, to start with, the team encountered two types of data at the crime scene. First, volatile data such as login sessions, network connections, cache, running processes, open files, the contents of the Random Access Memory (RAM) and other pertinent data. Second, non-volatile data maintained on the hard drive. In the given case, after obtaining the authorisation to 'search and seize' the team decided to seize the disk for further analysis. In order to take out the hard disk from the running system, the system needed to be shut down or power plug pulled, but on shutting down all the volatile data could be banished. Therefore, the team was fully equipped with the required tools to preserve the volatile data by taking the RAM dump, which consisted of the passwords of the browsers, files, encrypted disks/volumes and other information. After taking the RAM dump, the hard disk was removed and a mirror image of the disk taken as it is a cardinal rule of computer forensics that one not work on the original media. The team used the mirror image (not copy) of the hard disk that contained historical and current data on traffic volume and revenue shared for further analysis. Before proceeding further, it is necessary to clarify here, why a clone or a copy of the hard disk was not taken and what is the difference between the copy of the hard disk and image of the hard disk. Copying is nothing but making a copy of active files from one disk to another where the deleted files are not copied and left in the original disk only. Additionally, media access control timings of the files also change from the original media access timings to the date of copying. The clone is a direct disk-to-disk method for creating an exact copy of the original disk which is executable from any system. Conversely, the mirror image is an exact replica of the original image including the unallocated space and the data that can be seen only through the forensic tools like encase, Forensic Tool Kit, Autopsy etc. As the mirror image also contains the unallocated space and image is viewed through specialised forensic software, the deleted files also will be visible and they can be retrieved.

After imaging and documentation, the team had transported the original (sealed) and the mirrored hard disks to the State Forensic Laboratory for further analysis on the mirrored disk. Adequate precaution was taken to avoid excessive pressures, humidity and temperatures during transportation and storage. While there were several tools and procedures followed for the forensic investigation process,[6] the team followed the following processes as felt appropriate in the given situation. Verifying the integrity of the data: Verification of data integrity is essential to confirm at a later stage that the data was not tampered with during the evidence collection process. The team verified the data integrity using the Message Digest Hash 5 functions. The hash function is a mathematical algorithm that map data of arbitrary size to a bit string of a fixed size (a hash function) which is designed to also be a one-way function, that is, a function which is infeasible to invert. This was the most crucial stage of the investigation process as there were several cases rejected during the court proceedings as the hash generated after seizing and the hash generated during the hearing process did not match. As such, most of the imaging devices/software available in the market these days have the inbuilt hashing function which create the hashing of the entire disk/volumes/files as per the users' choice and it is reflected in their logs.

Analysis and reporting phase

The team used an online specialist free tool to analyse the data in the imaged hard disk. The team was surprised to note that the disk had two billing programmes running in a particular pattern. Further analysis of the software lines indicated that one programme was set to record all the transactions while the other was set to record revenue collected from every 15th vehicle which was being shared with the Government. This demystified the reason for the gross variation between the expected and the actual revenue. The team had completed the remaining stages of the investigation process which involved extensive documentation of the process, analysis of the evidence gathered, and interview responses and finalisation of the

[6]https://en.wikipedia.org/wiki/Digital_forensic_process

report for prosecuting the accused. The report contained the actions of the suspect during the crime, a full description of the investigation process, and the conclusions made. The report also contained the digital evidence, photographs taken, methodology used, and the chain of custody documents.

Lessons learnt

a. The fast changing landscape in the business processes, accelerated by the new technologies, poses a serious challenge to the traditional paper-based audit and forensic methodologies; and the auditors should be vigilant of such risks.

b. In auditing PPP projects, auditors should list all the risks at the planning stage, keeping in view the nature, the magnitude and complexity of the PPP arrangement. It should also be ascertained whether all the relevant risks were considered at the project design stage and adequately reflected in the request for proposal document.

c. Auditors should ascertain how each of the risks would impact the public sector participants as also on the consumers at large in the medium and long run. It should also ascertain whether the risk allocations have been judicious and fair for the sustained operation and management of the project.

d. One should carefully look for any possible ambiguities and pitfalls in the fixation of tariffs which could be recovered by the private partners as per the terms of the contracts and for this purpose, Auditors should carefully scrutinise the contract conditions.

e. A question to be addressed up front is whether the auditors could access documents of private partner for review. This was because the private sector partners are likely to resist the move on the plea of commercial confidentiality. This depends on the nature and the adequacy of the audit mandate the SAI had to undertake such projects.

f. There is a need to train the selected SAI staff for PPP audit, so as to equip them with the required skills and expertise for audit applying the forensics principles and above all, the required skill and competence to co-ordinate with the Statutory Forensic Units and other law enforcement agencies.

Acknowledgments

None.

Conflicts of interest

None.

Citation: Sadu I. Digital forensics in the audit of public private partnerships - a case study. *Forensic Res Criminol Int J.* 2017;4(6):195–197.
DOI: 10.15406/frcij.2017.04.00138