Digital Evidence Management Plan

CP Grobler
Department of Business IT
University of Johannesburg
Johannesburg, SA
tgrobler@uj.ac.za

CP Louwrens
Nedbank
South Africa

buksl@nedbank.co.za

Abstract—**The degree of the reliability, integrity, and availability of information in organizations can determine the credibility of the organization. As people and applications generate information, the information is stored in various places. It is vital for the organization to know where information is stored, what format it is, and how to access it. Not all information will be evidence but it is essential that organizations identify potential evidence proactively. Good evidence is a business enabler. Organizations require 'good' evidence to demonstrate due diligence with respect to good corporate and IT governance and to investigate and manage internal and external incidents. All internal and external forensic investigations hinge on 'good' evidence. Evidence in itself is not absolute, but is valuable when used to establish the truth about a particular incident. The paper will define digital evidence, propose a theoretical Evidence Management Plan (EMP), and briefly discuss potential benefits and constraints of the implementation of the proposed EMP.**

Keywords- Digital Evidence, Evidence Management Plan, Digital Forensics, Comprehensive Digital Evidence

I. Introduction

Organizations are experiencing pressure to have enough, relevant, complete, and admissible evidence available should an incident occur. Digital evidence is required for various reasons by organizations. The Human Resource department needs evidence to confirm misbehavior of an employee; auditors to prove fraudulent transactions; managers to determine if a control is effective and efficient to demonstrate due diligence with respect to good governance [1]; or to prove legal or regulatory compliance or non-negligence for an insurance claim; and the Information Technology department to investigate equipment misuse or to investigate incidents; [2].

The paper will consider digital evidence as 'any data stored or transmitted using a digital device that supports or refutes a theory of how an offence occurred or that addresses critical elements of the offence such as intent or alibi' [3] (Adapted from Casey, p 12). It means any digital data that can establish that a crime has been committed or that can provide a link between a crime and its victim or a crime and its perpetrator will be regarded as digital evidence.

Digital evidence is very volatile and can easily be contaminated or compromised when handled incorrectly. Failure to produce relevant, enough and admissible evidence very often leads to financial losses and failed investigations.

There are specific requirements for Digital Evidence to be admissible in a court of law. Various countries and judiciaries have different requirements. The Electronic Communications and Transactions Act of South Africa (ECT)[4] have the following requirements for determining the admissibility of a digital document or digital evidence in a court of law:

- The reliability of the manner in which the record was communicated and stored;
- how the integrity of the data was maintained;
- the manner in which the originator / author of the record is identified; and
- the evidence was legally obtained.

The paper will consider Comprehensive Digital Evidence (CDE) as '*digital evidence that will have evidentiary weight in a court of law and that contains all the evidence necessary (relevant and sufficient) to determine the root-cause of the incident, link the attacker to the incident and will result in a successful prosecution of the perpetrator'* [5]. By adhering to the requirements set out for evidence to be CDE, it is essential organizations have digital forensic sound processes and trained investigators.

From the literature studied, some authors propose to identify potential business scenarios that will require digital evidence. They suggest assessing all risks by considering vulnerabilities, threats, losses, and exposure and ensure that organizations have digital evidence in place when required. However, the focus is on evidence identification and collection after the detection of an incident. Other aspects to consider is the .development of policies to manage evidence in terms of storage and handling; a capability to gather evidence; and the systematic gathering of evidence with minimal disruption of business activities [6-10].

Rowlingson proposes to consider all types of evidence for example background evidence (evidence gathered for normal business reasons) and foreground evidence (evidence gathered by monitoring) [6]. The paper wants to add back-up information that can be potential evidence to background evidence. Venter and Olivier highlights the fact that log information is usually not tamperproof and can easily be modified or deleted [11].

The paper propose to classify evidence as physical evidence (flash disk) and digital evidence, where digital evidence consist of static digital evidence (e-mail, documents, log files) data objects (meta-data), live digital evidence (volatile RAM

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

content), legacy digital evidence, archived and post-incident digital evidence. It is essential that organizations identify the required CDE proactively before incidents occur so that when an incident occurs or evidence is required that CDE is available and accessible.

The next part of the paper will discuss the various components of the proposed Evidence Management Plan (EMP).

II. EVIDENCE MANAGEMENT PLAN (EMP)

It is essential that organizations put management measures and controls in place to manage the identified evidence. Beebe and Clark suggest to establish an information retention plan [7]. The authors are convinced that organizations need an EMP that is more comprehensive than the proposed information retention plan.

The authors have compared various frameworks and have combined the evidence handling, identification and managing concepts to propose the following steps [3, 6-8, 10, 12]. However, none of the frameworks researched evaluate the completeness of an evidence set linked to an incident or scenario. To manage the evidence in an organization, the EMP should

a. identify potential CDE proactively;

b. organize CDE by compiling an evidence index and establishing a network evidence map;

c. evaluate the evidence status of known assessed risks or scenarios in terms of the comprehensiveness of CDE; and

d. develop and augment evidence policies and procedures to ensure that evidence have the highest CDE rating.

The next part of the paper discusses each point.

A. Evidence identification

It is essential to define business scenarios that will require digital evidence. Beebe and Clark, Louwrens and Rowlingson suggest identifying potential evidence during the risk assessment process [6-8]. The paper suggests starting with evidence identification during Business Impact Analysis, when compiling the threat profiles for known threats / risks to the organization [13].

The threat profile includes general information about the identified risk for example the risk description or indications, controls applied and policies linked to the risk [13]. The paper suggests expanding the threat profile to include all risks and/or scenarios that may need evidence to compile a ‘complete threat profile’ or risk profile.

Another addition to the risk profile is to include the evidence elements that will be required to investigate the risk. This step will ensure that the evidence is relevant and enough for the identified risk or scenario. This will also address Louwrens et al’s requirement to ensure that monitoring and auditing is targeted to detect and deter major incidents as well as the systematic gathering of potential evidence [8].

The final addition is to add a CDE rating field to the risk profile. This field is an indication of the completeness and potential admissibility of the various evidence items related to the potential risk / scenario.

The adapted risk profile should include the

1. risk / scenario name;
2. the risk / scenario characteristics for example:
   a. Threat and probable threat agent;
   b. Known or possible vulnerabilities;
   c. Likely precursor activities or indicators;
   d. Likely attack activities or indicators of attack in process;
   e. Information assets at risk;
   f. Damage or loss from attack;
   g. Other assets at risk; and
   h. Damage or loss to other assets [13];
3. policy or controls set up for the identified risk or profile; and include a
4. CDE rating field.

Paragraph C will propose a method how to determine the CDE rating of the evidence collection for a proposed risk. The next step will be to organize the identified evidence.

B. Organising the evidence

It is inevitable that the same evidence elements are required for different scenarios / risks. It is essential to organize the evidence elements. Casey proposes to construct a digital evidence map that will contain all the information about the evidence i.e. category, location, retention time, reference procedures to collect and retrieve evidence [12]. The paper suggests expanding the map by adding certainty ratings and special requirements to the evidence map as proposed by Casey. This expanded map will be referred to as a digital evidence index. The following steps should be considered:

1) Classify / categorize the evidence element as being physical or digital evidence. If it is digital evidence, determine if it is static, live, archived or post investigation evidence. This classification is essential as different policies and procedures, technologies, legal requirements and investigation protocols are applicable to the different types of evidence;

2) Determine the technical requirements for the identified evidence element. The technical requirements can include who can access the evidence, what software are involved, is the evidence from legacy software or in a live format. This can determine what Digital Forensic (DF) tools will be required when it must be acquired;

3) Determine the legal and regulatory requirements for the identified evidence element to be acceptable in court and to have an evidentiary weight. This includes the legal and regulatory evidence collection, transport, storage requirements, retention time and privacy issues;

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

4) Assign a certainty rating to each evidence element. The paper proposes to use Casey's certainty scale (table 1) to evaluate the evidence [3];

TABLE I. CASEY'S SCALE OF CERTAINTY [3]

Certainty level	Description / Indicator	Commensurate / Qualification
C_0	Evidence contradicts the known facts	Incorrect / erroneous
C_1	Evidence highly questionable	Highly uncertain
C_2	Only one source of evidence not protected from tampering	Somewhat uncertain
C_3	The source of evidence are more difficult to tamper with, but there is not enough evidence to support a firm conclusion or there are unexplained inconsistencies in the available evidence	Possible
C_4	Evidence is protected against tampering Evidence is not protected, but multiple independent sources of evidence agree	Probable
C_5	Agreement of evidence from different independent sources that are protected against tampering, but small uncertainties exist (data loss)	Almost certain
C_6	The evidence is tamper proof and unquestionable	Certain

5) Include any special requirements as well as the location of the evidence element in the information architecture of the organization; and

6) Compile the digital evidence index. Table 2 is an example of a digital evidence index.

TABLE II. DIGITAL EVIDENCE INDEX

Column name	Description
Evidence number	E_I
Description/ Evidence element	
Category / type	Live / static/ / archived / physical
Technical requirements e.g. DF tools, How to retrieve Who, software. Legacy, live Format	Format Access requirements Encrypted? Format
Legal requirements	Retention Time, Privacy
Certainty rating / classification	Casey: C_0: incorrect $C_{6:}$ Certain
Special requirements	Classification in organisation e.g. confidential
Location	C:/kjskf/shfjkfhs

It will be useful to create a 'birds eye view' of the evidence elements in the information architecture. A useful way is to map the evidence to a network diagram of the organisation to provide a visual representation of the location of the evidence. Figure 1 is an example of a network diagram with evidence. The evidence element Ei is represented in the green blocks 🟩 as Ei.

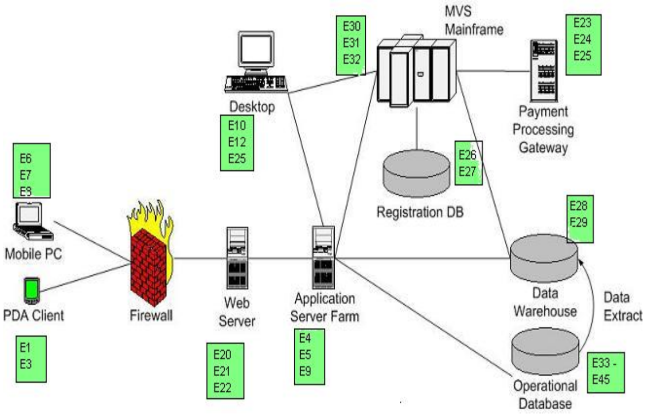

Figure 1 Network diagram with evidence

The next step will be to complete the risk profile determining the CDE rating for each risk or scenario.

C. Complete risk profile by calculating the CDE rating for each risk.

The paper proposes to use the Upgrader matrix as defined by Olivier and Venter to calculate the CDE rating and CDE flag color for and evidence set {E_1; E_2; …. E_n} associated with risk$_i$ or scenario$_i$ [11]. The risk management department should determine the specific evidence certainty combinations that will be acceptable for the organization. The authors propose to color code the Upgrader matrix.

The paper proposes the use of three colors:

- 🟩$_G$ Green (***C_5;C_6***) → Excellent CDE can result in a successful investigation;
- 🟧$_O$ Orange (***C_2 ;C_3;C_4***) → Average CDE; and
- 🟥$_R$ Red (***C_0; C_1***) → not enough or bad CDE.

Organizations need to determine if the orange 🟧$_O$ rating is red 🟥$_R$ or green 🟩$_G$. If evidence is required for an internal hearing the orange 🟧$_O$ rating may be reclassified as green 🟩$_G$, but if it is for external investigation purposes the orange 🟧$_O$ may be red 🟥$_R$

The definition of CDE requires that the evidence must have an evidentiary weight, be complete and relevant. The linking of the evidence element to the scenario / risk makes it relevant, determining all the evidence elements for each risk in the risk-profile address completeness. The paper accepts that the evidence acquired will be admissible within the legal operating environment of the organization. The paper will use completeness and Casey's certainty rating (for admissibility) to determine the CDE rating for an identified risk / scenario.

The paper proposes to determine the weakest evidence element (C_{min}) and the strongest evidence element (C_{max}) in terms of the certainty rating. The weakest evidence element will have an influence and will lower the rating of the evidence set. C(E_i) is the certainty rating of evidence item E_i. The paper proposes the following steps:

- *Step 1:* If evidence set incomplete: CDE flag = 'RED'🟥$_R$ */ completeness of evidence set*/

  ELSE step 2;

- *Step 2:* Calculate C_{min} = min $\{C(E_1)_1; C(E_2)_2; \ldots; C(E_n)_n\}$ */ the lowest C rating of the evidence set $\{E_1; E_2; \ldots; E_n\}$ for risk / scenario$_i$;

- *Step 3:* Calculate C_{max}= max $\{C(E_1)_1; C(E_2)_2; \ldots; C(E_n)_n\}$ */ the highest C rating of the evidence set $\{E_1; E_2; \ldots; E_n\}$ for risk / scenario$_i$;

- *Step 4:* Determine the CDE rating by mapping C_{min} and C_{max} to determine the risk CDE rating and flag colour in Figure 2.

C_{max} across the top; C_{min} down the side:

C_{min} \ C_{max}	C_0	C_1	C_2	C_3	C_4	C_5	C_6
C_0	C_0	C_0	C_0	C_0	C_0	C_1	C_1
C_1		C_1	C_1	C_1	C_1	C_2	C_2
C_2			C_2	C_2	C_2	C_3	C_3
C_3				C_3	C_3	C_4	C_4
C_4					C_4	C_5	C_5
C_5						C_5	C_6
C_6							C_6

***Key:** $C_0; C_1$ → 🟥$_R$ $C_2;C_3;C_4$ → 🟧 $C_5;C_6$ → 🟩$_G$*

Figure 2 Color -coded Upgrader matrix

To demonstrate the calculation of the CDE rating, the paper will briefly discuss the following example in Figure 3 and table 3. Figure 3 contains the risk profile and the digital evidence index. The *risk profile* will contain a list of various identified risks / scenarios. The digital evidence index contains a list of all the evidence elements. Each evidence element E_i has a certainty rating C_i allocated to it during risk assessment or Business Impact Analysis of the scenario or risk. Table 3 is a demonstration of the calculation of the CDE rating and the flag.

Risk 1 / scenario 1 has 3 evidence elements with certainty rating from evidence index: $C(E_1) = C_4$; $C(E_5) = C_5$ and $C(E_6) = C_6$. Table 3 shows that $C_{min} = C_4$ and $C_{max} = C_6$. After consulting the Upgrader matrix in figure 2, the CDE rating = C_5 and flag = 🟩$_G$ Green.

After the calculation of the CDE rating, update the CDE rating field in the risk profile as indicated by the line labeled ❶ in figure 3 and table 3.

The organization can get a very good idea of their evidence status when they view the risk profile. There is scope for further research to expand this assessment to include more parameters to compute the CDE rating for example number of evidence items, admissibility rating (include relevance, legal, integrity, producible, etc. requirements) and certainty.

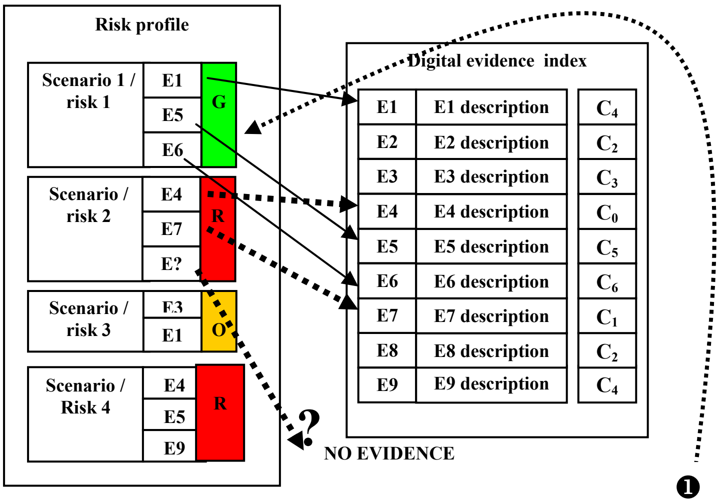

Figure 3 Example of completion of risk profile

TABLE III. CALCULATION OF CDE RATING AND FLAG

Risk / Scenario	Evidence	C_{min}	C_{max}	CDE rating	Flag
1	$E_1 = C_4$, $E_5 = C_5$, $E_6 = C_6$	C_4	C_6	C_5	🟩$_G$
2	Evidence is missing			C_0	🟥$_R$
3	$E_2 = C_2$, $E_3 = C_3$	C_2	C_3	C_2	🟧$_O$
4	$E_4 = C_0$, $E_5 = C_5$, $E_9 = C_4$	C_0,	C_5	C_3	🟥$_Y$

The next step is to create, update, or augment policies and procedures related to evidence.

D. Establish evidence management policies and procedures

Policies and procedures guide behavior and actions in the organization. Typical policies and procedures to consider are evidence identification, acquisition, handling, preservation, authentication, transport, post investigation evidence handling (retention, returning or archiving). This may not be a complete list but serves as an example of typical policies and procedures to consider.

The Incident Response, Business Continuity and Disaster Recovery plans contains policies and procedures for example incident detection, confirmation, containment, escalation and recovery. The policies must recognize the importance of CDE preservation and the procedures should be forensically sound. All the policies and procedures must ensure the preservation of the chain of evidence and chain of custody.

Intrusion detection technologies do not consider any evidence requirements as it is focused on detecting incidents [14]. It is also vital to review technical and people related policies and procedures for example time synchronizing of equipment and the content of training and awareness programmes.

The authors anticipate the following benefits, but also potential constraints for the implementation of the EMP.

III. BENEFITS AND CONSTRAINTS OF THE IMPLEMENTATION OF THE EMP

If an organization invests in the implementation of the EMP, they can expect the following benefits:

- The availability of quality CDE. The digital evidence index contains a list of all identified evidence elements in the organization. The index will contain all physical, live and static evidence with relevant information about the evidence for example how to recover, access requirements and format of the evidence;
- Organizations will be prepared for investigations of known incidents. The organization should consider all risks and scenarios that may require evidence;
- CDE will be available to enable organizations to demonstrate due diligence by being able to prove effectiveness of controls implemented;
- Well defined policies and procedures to preserve the chain of evidence and chain of custody;
- Availability of acceptable tools and technologies to acquire the evidence;
- Minimum business interruption during investigations as evidence and processes will be in place when required;
- Provide a way to gain an overview of the CDE status for all risks by using the color status of each risk or scenario; and
- Reduced costs for an investigation or to retrieve evidence as the organization will be prepared;

However, there are some problems or constraints that one can encounter when considering the implementation of an EMP for example:

- The impact of additional information (evidence) on the information architecture of the organization;
- Additional storage capacity and cost to store identified CDE;
- Adjustment of current systems to make evidence tamperproof or admissible;
- Organizations can only prepare for known incidents or scenarios;
- Currently no application exists to implement the EMP as it requires dynamic updating of the evidence index and risk profile. There is a need to develop an application;
- It will be essential to update the content of the risk profile and evidence index frequently; and
- There may be an initial high setup cost;

The benefit of CDE availability and well-defined policies and procedures can be justified when considering reduced investigation costs, the prevention of the loss of reputation of the firm, legal and regulatory compliance and prompt response and action to incidents. Organizations will be Digital Forensic ready and therefore prove due diligence with respect to good corporate governance [5].

IV. SUMMARY

Organizations have an ever-growing need for CDE. Technologies such as the Internet and intelligent cell phones are becoming a necessity to live as we communicate, do banking, and business transactions using technology. However, criminals exploit the technologies to commit crimes. Corporate governance reports for example King 3 and Sarbanes-Oxley also require evidence to prove that controls are effective and efficient [1, 15].

The paper has defined and briefly discussed the concept of Comprehensive Digital Evidence. There is a need for an evidence management plan that will enable organizations to proactively identify digital evidence, create a risk profile with a CDE rating per risk or scenario, create an evidence index, create and augment evidence related policies and procedures as well as training programs. The last part of the paper discusses potential benefits and constraints of the EMP.

The authors are convinced that the potential benefits derived from the implementation of an EMP will outweigh the mentioned constraints.

REFERENCES

[1] *King 3 Report on Corporate Governance*. 2009, Institute of Directors of Southern Africa.http://www.iodsa.co.za/downloads/documents/King_Code_of_Governance_for_SA_2009.pdf

[2] Sommer, P. (2005) *Directors and Corporate Advisors' Guide to Digital Investigations and Evidence*. Information Assurance Advisory Council, http://www.iaac.org.uk/Portals/0/Evidence%20of%20Cyber-Crime%20v12-rev.pdf3 June 2007

[3] Casey, E., ed. *Digital Evidence and Computer Crime*. 2 ed. 2004, Elsevier Academic Press.

[4] *Electronic Comminications Act*. 2003: South Africa.http://www.gov.za/gazette/regulation/2003/24594a.pdf

[5] Grobler, C., C. Louwrens, and S.v. Solms. *A framework to guide the implementation of Proactive Digital Forensics in organizations*. in *Workshop for Digital Forensics 2010*. 2010. Krakow, Poland.

[6] Rowlingson, R., *A ten step Process for Forensic Readiness*. International journal of Digital Evidence, 2004. **2**(3).

[7] Beebe, N. and J. Clark, *A hierarchical, objectives-based framework for the digital investigations process* Digital Investigation, Elsevier, 2005. **2**: p. 147-167.

[8] CP Louwrens, et al. *A control Framework for Digital Forensics*. in *IFIP11.9 International Conference on Digital Forensics*. 2006. Orlando Florida: Springer.

[9] Carrier, B. and E. Spafford, *Getting physical with the digital investigation process.* International journal of Digital Evidence, 2003. **2**(2).

[10] Barayumureeba, V. and F. Tushabe. *The enhanced digital investigation process model*. in *DFRWS 2004*. 2004.

[11] Venter, H. and M. Olivier, *Applying the BIBA integrity model within a forensic evidence management system.*

[12] Casey, E., *Digital Evidence maps - A sign of the times.* Digital Investigation, Elsevier, 2007. 4: p. 1-2.

[13] Whitman, M.E. and H.J. Mattord, *Princilples of Information Security*. 3rd Edition ed. 2009: Thompson Course technology. 560.

[14] Sommer, P., *Intrusion Detection Systems as Evidence.* Computer Networks: The International Journal of Computer and Telecommunications Networking 1999. Volume 31 **,** (I23-24 (December 1999)): p. 2477 - 2487

[15] *Sarbanes-Oxley Act*, in 2002: USA.http://frwebgate .access.gpo.gov/cgiin/getdoc.cgi?dbname=107_cong_bills &docid=f:h3763enr.txt.pdf.

[16]