IST-Africa

IST-Africa 2011 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2011
ISBN: 978-1-905824-26-7

The Corporate Incident Response Framework (CIRF)

Theron PIETERSE
University of Johannesburg, Corner Kingsway and University Road, Auckland Park, 2006, South Africa
Tel: +27 82 9070335, Email: theron.pieterse@kpmg.co.za

Abstract: There is a need for small and medium sized companies to cater for the investigation of internal and external computer incidences. This paper proposes a model that includes the important elements a company should have in place in order to effectively deal with incidences when they occur.

Keywords: South African incident response, forensic investigation, internal and external incidents, model for the small and medium sized company.

1. Introduction and objective

South Africa has undergone many changes with regard to how electronic information assets are managed, legally presented and distributed. The most important aspect of the ECT Act of (2002) is to ensure that an electronic document possesses the value of an asset. According to Jordan, Silcock (2005), the asset is used to generate the capacity to deliver value or benefit to a company. The computer has given a company the means of moving out of the brick-and-mortar stage of service delivery. Electronic information assets have become the life-blood of many companies, Von Solms (2008). These electronic assets can be both valuable and crucial to the company's existence. Companies protect information due to the valuable nature of this asset. The asset is valuable to the employees (internally) to ensure the flow of direct and indirect processes in a company, Jordan, Silcock (2005). Individuals who wish to exploit the company can attempt to steal, tamper or destroy the valuable company asset.

The Corporate Incident Response Framework (CIRF) is a methodology a company implements to ensure that incidents (internal and external threats) are appropriately planned for. Pro-active implementation of effective incident response procedures is important to the business continuity and disaster recovery of the company. The board of directors will be mindful of the fact that escalating incidents have dire consequences to the future of all those involved with the company and will seek to implement these methods in order to reduce the risk of failure.

This methodology includes the following aspects:

The People involved in the investigation;
The incident;
The legal considerations;
Internal processes and controls;
The formal risk analysis;
Digital evidence; and
The investigation.

Incidents have an effect on each of these areas and the aforementioned aspects can exclude many important portions that relate to effective incident response. The methodology will practically include all these aspects within the company's environment that is strategically implemented to deal with incidents. Therefore, the company seeks to reduce the risk of ineffective techniques that dealing with isolated issues. The CIRF is the foundation of business continuity and ultimately places the company in an advanced position to proceed legally and strategically.

There are obvious limitations to implementing a CIRF within any company and the list below provides more overview:

- The number of employees and workstations;
- The nature of the company's business and dealings;
- The extent to which information assets will need protection (the sensitivity of the information);
- The budget allocated to information protection;
- The need for investigation of internal and external incidents; and
- The cost/benefit of internal CIRF and external assurance.

2. The Problem Statement

The CIRF's objective is to give a company a strategic advantage when dealing with internal and external computer incidences. The problem the CIRF is solving is to ensure that the company:

- is legally prepared to deal with internal and external incidences;
- can initiate the first of many steps to investigate and solve internal and external incidences;
- is able to mitigate the risk of incidences occurring;
- is proving due diligence to the shareholders as per the King III report; and
- has the necessary controls, processes and people in place to shield against intrusion.

The digital Investigation is used to objectively identify, acquire, analyse and report digital evidence in a legally accepted manner. Internal and external computer incidences range from fraud and computer misuse to security breaches and industrial espionage. Internal and external computer incidences negatively affect a company and cause disruption to the daily workflow. The dilemma companies are facing is how to minimize the impact and probability of an incident whilst ensuring that digital evidence can be legally, efficiently and cost-effectively investigated and represented in court. Therefore, it is essential that the company should focus on foresight and proper planning. Formal Corporate Incident Response Frameworks usually do not exist in a company and this leads to inadequate or inappropriate actions once an incident has taken place.

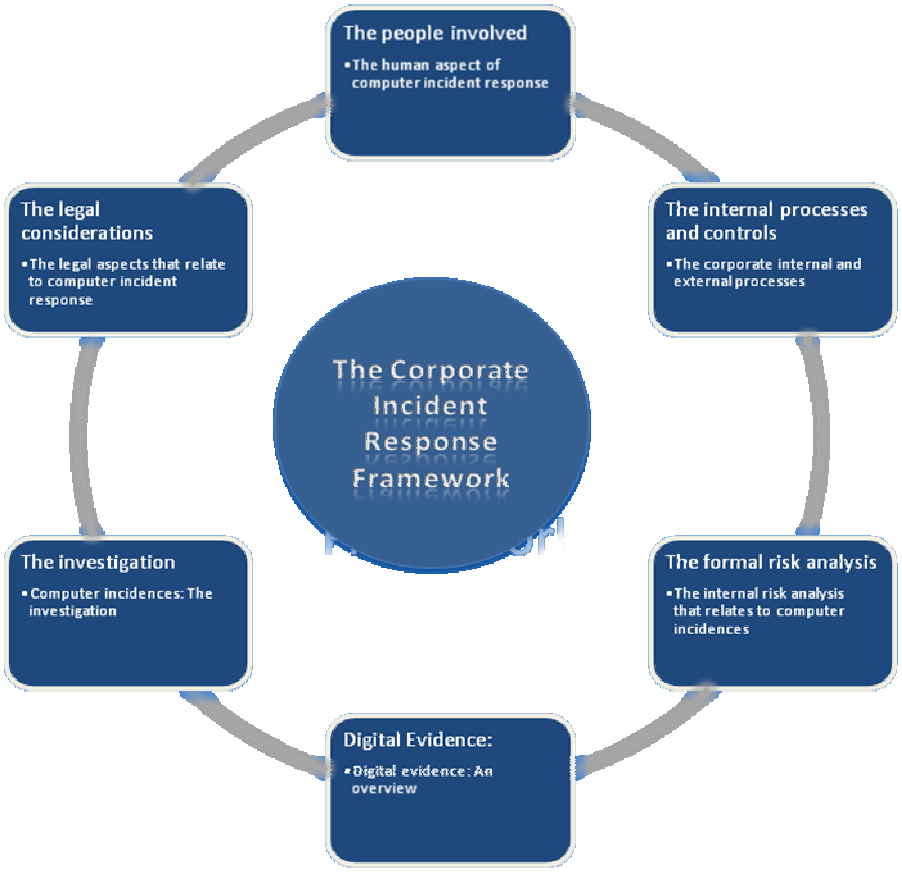
There are a wide variety of factors that affect the investigation of an incident and these include:

a) The size of the company;
b) The company's dependence on computer systems;
c) The size of the company's computer system and employees that manage these systems;
d) The effectiveness of the internal controls and procedures;
e) The inherent risks associated with computer systems;
f) The severity of the incident according to a formal classification scale.

The CIRF is the company's strategic plan to effectively deal with internal and external incidences.

3. Introducing the Corporate Incident Response Framework (CIRF)

The Corporate Incident Response Framework (CIRF) will affect a variety of fields and professions within an organisation in order to appropriately follow sound forensic practices. Any relevant incidents should be dealt with as though the incident will be tried in a court. The company's board of directors agree on the reason for implementing a Corporate Incident Response Framework, because this will determine the depth and extend to which the framework is implemented.



3.1 The people involved in the investigation

3.1.1 The corporate incident response committee

The Corporate Incident Response Committee reports directly to the board of directors. This committee is responsible for ensuring that the formal incident response framework is up-to-date and tested on a regular base. The formal leadership, support roles, responsibilities and reporting line must be identified. This will include the chain of command and eliminate any confusion during the investigation. Fraud and incidences must be formally reported (via the corporate reporting line) to the incident response committee. All personnel must know how to report any suspicious activities and be encouraged to do so (This can be kept anonymous if prompted).

The corporate incident response committee corresponds with the board of directors as to the objective of the investigation. The prosecution of personnel might be the agenda in one case but the tracing of funds in another.

3.1.2 The investigation team

Strategic management in a company will decide how an investigation team is constructed and to whom this team reports. The investigation of computer incidences is usually conducted by individuals with various skill levels and fields of expertise. A company can choose to conduct the investigation internally, externally or by means of law enforcement. The following are role players that can be used in different situations and organisations:

(1) The police (Public sector investigation)

The cost and benefit should be considered before reporting incidents to the police. This is due to the fact that the incident could have reputational damage to the company. Reputational damage can escalate from the clients to the shareholders in a company and cause much greater damage than the incident itself. Certain incidents (such as terrorism) are required to be reported to the authorities, seeing that these incidents affect the public well being.

(2) The internal investigation

Internal investigations are conducted by using the specialised skill of individuals that currently form part of a company's workforce. It is not always feasible to conduct an investigation in-house, (Vecchio-Flaim, 2001:1). This approach could prove to be the most cost effective for medium to larger organisations but smaller organisations lack the resources or structure to successfully complete such an investigation. According to Ryder (2002), it is appropriate to include the company's IT personnel in the investigation team, because these personnel know the system better than any external party. Improperly trained or inadequately educated personnel could potentially prove to be devastating. Depending on the incident type and severity, management should decide whether it is feasible to conduct the investigation internally.

It is management's duty to keep the following in mind:

a. The independence of the investigators;
b. The utilisation of technical personnel with knowledge of the computer systems; and
c. The integrity of evidence provided by internal personnel (impartiality).

In large organisations, it may be feasible to build a dedicated forensic specialist team. This could be both beneficial and cost effective when dealing with financial institutions or highly confidential electronic information (trade secrets).

(3) The external investigation (Private sector investigation);

A company can hire independent external consulting firms to investigate incidents that occur within the borders of a company. These external investigations are usually costly, time intensive and, due to experience and expertise, could provide the best quality of deliverables available. Private sector companies are equipped with the latest technology, training and insight into changes in legislation.

The most important aspect of an external investigator is independence (impartiality) and quality. These investigators are usually experienced in providing testimony in court and represent an unbiased opinion as to the validity of the evidence.

(4) The co-source option

External resources can be used as the primary investigation resource and company employees as support personnel. In other cases, only the expertise needed can be outsources to external companies in order to gain more in depth knowledge and experience. In order to

use the co-sourcing option, a company must have a superior understanding of the incident and the affected systems.

These four options can be used interchangeably depending on the size of the organisation, the affected computer systems and the severity of the incident itself. The most important aspect of a good forensic investigator is impartiality. The investigator must have no predispositions as to guilt or innocence during the investigation.

3.2 Roles and responsibility

Before conducting any investigation, the roles and responsibilities of each person on the team is well defined. Some roles are generic and can be fulfilled by the same individual. The Corporate Incident Response Team is required to fix the problem by utilising skill and knowledge to the situation, Tsoutsouris (2001). The following is a list of different roles and responsibilities that form a forensically sound investigation:

(1) The first to respond

The first responders are the company personnel that have identified a discrepancy or incident and have notified the appropriate management levels. The first to respond will start collecting evidence (usually from logs and traces). These personnel are trained and follow the internal procedures that dictate the chain of command when incidences occur.

(2) The Investigators

Internal and external investigators are the impartial individuals who identify, acquire, preserve, analyse, examine and report on digital evidence. These investigators work with the first responders and technical team to follow the forensically sound methods when investigating incidents.

(3) The technical team

The technical team understand the computer system and internal processes of the company. Technicians are crucial to the success and outcome of the forensic examination. These individuals report directly to the investigators and can comprise of internal and external personnel that are qualified the acquire evidence.

(4) The forensic examiners

Forensic examiners analyse and seek evidence from data that may be hidden, deleted or difficult to retrieve. Specialised tools and technology is used that help and guide the examiner to produce a forensically sound report.

(5) The legal advisors

Major incidents usually require the input of legal advisors. Pursuing a case to court will keep the company's legal team up to date and abreast of events surrounding the investigation. The legal team assists in ensuring that evidence will be defended against the scrutiny of a court case.

All individuals involved have to adhere to the strictest confidentiality clauses surrounding the incident. Reporting must be formally approved by the chain of command and independence should be kept in all situations.

3.3 The incident

3.3.1 Policies, agreements and confidential information

Incidents occur in all shapes and sizes. The company will provide certain security measures to lower the risk of fraud, copyright infringement and trade secrets leakage. The company realises that individuals and groups may cause harm to the company, and therefore tries to minimize the impact and likelihood of incidents occurring. Policies, non-disclosure agreements, trade secrets and copyright are used to keep the company protected from intellectual property and employment breaches.

3.3.2 Incident identification

Incidents are not always identified by means of unexpected behaviour of system such as input, output or processing discrepancies. The company encourages the use of the appropriate channels to create formal identification methods for employees that suspect fraud. There is no use for a security and response framework to be implemented in a company, if access of this framework is limited to the technical few.

Channels are created and implemented whereby an employee can anonymously voice any irregularity that may be classified as an incident. These channels are processes that can be the source of high profile incidents. High level management are usually not involved with the day-to-day tasks and can be out of touch with real problems that occur. Channels create a way for the person in the workplace to effectively communicate with senior staff members.

3.4 The legal considerations

3.4.1 Legal Introduction

Investigations are required to adhere to South African legislation and therefore the company seeks legal assistance before, during and after the incident investigation life cycle. It is within the company's best interest to keep certain incidents confidential and out of the public domain, however legislation states that certain incidences are required to be reported (e.g. terrorism).

South Africa has one legal system that extends into two mediums: The physical world and the electronic world. The difference between these mediums is that one is tangible with human role players, and the other is intangible with computers as role players. Therefore, South Africa has Information and Communication Technology law comprising of three pieces of legislation that govern the use of computers:

(1) Electronic Communications and Transactions Act 25 of 2002;

This law promotes certainty regarding electronic communications and transactions and covers a wide variety of issues such as electronic signatures. This law states that any electronic version carries the same value as a physical version and promotes liability in terms of supplier security. All electronic technology and communications are governed by this act and the digital investigator will seek to abide by these regulations to ensure that evidence is admissible.

(2) Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

The RIC Act governs the use and distribution of surveillance regarding workplace and government methods. Monitoring, interception, data retention and encryption form part of

this Act. This is very important for a forensic investigator who intends to monitor the workplace and suspected criminals.

(3) The Communications Act

The Communications Act regulates intellectual property, limited monopolies and competition.

3.4.2 Intellectual Property concepts in the forensic framework

Intellectual Property is intangible property that is derived from creative, intellectual activity in the literary, artistic, industrial, scientific and Information and Communication Technology (ICT) field. The forensic examiner will work with intellectual property as part of the investigation. Incidents that occur in the electronic environment have a stringent impact on the Intellectual Property that the company owns. According to Tsoutsouris (2001), the employee initiates most of the intellectual property theft within a company, because it is usually part of an employee's job to have easy access to such information. There are different types of Intellectual Property namely:

(1) Copyright Act of 1998

Copyright protection gives the owner of intellectual property exclusive right to prevent others from copying the work. Copyright is automatic in South Africa and computer programs fall under the copyright protection. During a crime investigation, copyright may be infringed by reverse engineering computer programs.

(2) Trade secrets

Trade secret involves information which has independent economic value and reasonable measures have been taken to secure this information. The company enforces strict rules to ensure that trade secrets remain safe. Computer related incidents leave trade secrets exposed or are the reason individuals try to exploit the company.

3.4.3 Evidence in court

Evidence is required to be legally admissible. Therefore the evidence is identified, preserved, analysed and reported in certain a forensically sound manner. Monitoring of personnel within a company and random computer scans should adhere to the legal standards of the RIC Act. When dealing with computer related incidences, the company's legal team should be consulted. According to Marcella et al. (2002), any information is theoretically admissible in court if it has relevance. The guarantee of trustworthiness, that sound forensic techniques provide, is what makes evidence unquestionable.

3.4.4 Chain of custody

When an incident is being investigated, evidence is gathered as the investigation continues. All evidence must follow an unbroken chain of custody in order to be admissible in court. The company may wish to pursue a criminal or civil case against and individual or institution and therefore all evidence is required to be correctly handled.

3.5 Internal processes and controls

3.5.1 Internal processes and controls introduction

Companies have certain processes and controls that are used in to perform daily, monthly and yearly tasks within the company. These controls are usually generic and apply to the processes that the entire company follows. It is the company's responsibility to maintain, update and enforce the processes and controls within the company to effectively prevent, detect and investigate incidences.

3.5.2 The purpose of internal processes

Technical internal processes ensure that the frequencies of errors are reduced by using effective and enforceable rules. These rules are used to guide the data capture, administration and throughput of data from one point to another and correct errors that may have occurred. Most companies rely solely on the computer systems that drive the company. These internal processes and controls are used to ensure the completeness, accuracy and integrity of the input data (Krauss et al., 1979)

These processes and controls are also used to detect anomalies in the system and inputs, outputs and processes that may be abnormal. These processes and controls are usually a good indicator of an incident occurring or incidents that may have occurred.

3.5.3 Applying internal processes and controls.

Designing adequate controls can not only save a company money and man hours, but also contribute to detecting, preventing and investigating incidences. These controls can be used to create multiple points where unauthorized and fraudulent activities can be detected. In essence, there controls are used to prevent fraud from occurring by flagging any unusual uses of the system. This section will address the following categories:

1) Input Controls;
2) Output Controls;
3) Processing Controls; and
4) Correction Controls.

There are certain generic activities that form part of each of these categories. These activities, such as segregation of duties, administration and documentation, will be discussed under each of the categories.

3.6 The formal risk analysis

3.6.1 Risk analysis introduction;

It is the company's responsibility to conduct a formal risk analysis of crucial or all computer systems in order to ensure that appropriate measures have been taken to protect the company. Striving to provide excess security measures are economically unfeasible and will drain company resources.

3.6.2 Cost estimation

Every incident countermeasure will have certain costs to the company. These costs are implementation costs and maintenance costs. The Corporate Incident Response Framework (CIRF) is seen as a countermeasure to fraudulent activity and computer incidents. Therefore, the company must estimate the cost of implementing this framework relative to the size of the company and the factors that are included in the introduction.

3.6.3 Estimating the benefits

The costs of implementing countermeasures are usually measured in terms of the benefit the company will gain in the future. The primary benefit is the reduction in the risk that an incident might occur, and that the company will not be prepared (financially or otherwise) to counter it.

3.6.4 The cost-benefit and risk analysis

This section will deal with the risk and the cost-benefit analysis of not only the incident itself, but the implementation of a formal Corporate Incident Response Framework. The goal will be to have absolute certainty as to the extent and feasability of implementing the framework within the company. Each and every company is different and therefore the implementation of this framework will focus on generic aspects of most companies.

3.6.5 Incident classification

Every incident that occurs within the borders of a company is required to be classified by impact and severity. Major incidences will require a formal investigation whilst minor incidences can be classified as mere housekeeping issues. Incidences that severely impact the business will also get higher priority and therefore all incidents have to be informally classified in a timely manner. A formal risk assessment needs to be completed on major incidences in order to formally investigate as needed.

3.7 Digital evidence

3.7.1 Tools and equipment

Tools and equipment are very important to any investigation that will be fully or partially conducted within the company. Acquiring the necessary tools and equipment will require careful and precise planning, depending on the range of the computer systems in the company.

Provisioning for portable equipment is feasible in larger diverse organisations. This section provides formal motivation of why expensive tools and equipment are a crucial factor of a computer forensic investigation.

(1) The variety of tools and equipment required

Digital forensic teams are equipped to deal with a variety of different incidents. According to Kruss II *et al.* (2002), investigators require a variety of tools in order to be successful. Computer forensics encompasses identification, extraction, preservation and documentation and the tools the investigator uses will determine how effective the investigation concludes.

(2) The preparation

The formal risk analysis performed on the electronic environment of the company is used by the Corporate Incident Response Committee to gain a high level technical understanding of the systems and software that the company utilises. Depending on the findings of the risk analysis, the Corporate Incident Response Committee will decide which tools and equipment will be necessary in order to conduct a forensically sound investigation.

(3) Reliable output

Forensically sound methods coinciding with industry trusted and certified tools guarantee the best results. This section focuses on the tools and equipment that is well known in the

South African legal circles. These include drive imaging, network monitoring software and forensic programs.

(4) Focussing on the company need

The majority of tools and equipment are built for specific purposes. Therefore, the Corporate Incident Response Committee will ensure that the purpose for which the company is implementing a Corporate Incident Response Framework (CIRF) is in line with the tools that the company will acquire. Network-based tools, protection tools, analysis tools are all available and used for different purposes (Marcella *et al.*, 2002). Each tool should be evaluated to ensure the appropriate usage and implementation.

3.7.2 The laboratory

An effective and secure laboratory is needed as part of the investigation. This laboratory requires formal standards and controls in order to be forensically sound. Access and security procedures are strict due to the sensitive nature of the information being analysed and stored. (This includes physical and logical access controls and procedures). According to Vecchio-Flaim (2001), the investigation team will acquire tools and equipment as a variety of investigations is conducted. Tools and equipment, examinations and properly securing evidence is all part of the function of the forensic laboratory.

3.7.3 The rules of digital evidence

According to Ryder (2002), there are five rules to digital evidence:

(1) Admissible

The evidence must be able to withstand the scrutiny of the court system and be admissible as appropriate. Evidence collected must always be admissible in court, or the cost of not being able to do so will be too high.

(2) Authentic

The evidence must prove that an incident has taken place, or that an individual has committed the incident. The evidence must be proven authentic to be of any value to the company or court.

(3) Complete

The investigator must use all the evidence available to create a complete picture of the incident that has taken place. Evidence is also used in this way to eliminate certain suspects or incident theories.

(4) Reliable

The evidence that is collected is required to be regarded as reliable. There can be no doubt as to the source, methods or investigation team that collected the evidence.

(5) Believable

The evidence will be presented in the future and is required to be clear, easy to understand and simplistic or logical. The investigator must be able to explain the technical and relationship of different types of evidence.

3.8 The investigation

3.8.1 The investigation introduction;

If an effective Corporate Incident Response Framework is present, the company will have the benefit of investigating immediately, without any delay from external parties. According to Kuchta (2002), the investigation program provides the needed structure and consistency that will prove due diligence on behalf of the investigation team. The company will focus on minimising losses and gaining enough evidence to make an informed decision as to the steps to follow. Major incidences will usually result in bringing the responsible parties to justice.

3.8.2 The investigation procedures;

The investigation team will work toward gathering the evidence that should ultimately lead to the root of the incident. This involved planning and organising the investigation to successfully see the investigation through. The investigation will strive to use trusted methods to be as discrete and effective as possible, gaining knowledge such as motive, modus operandi and total loss for the company. The goal of any investigation is to make a successful case for prosecution.

(1) Clues to the existence of an incident;

The network and data administrators usually detect problems on the technical level of a company. These signs and indications are that of unexpected behaviour, irresolvable exceptions or unusual customer/departmental complaints. According to Krauss *et al.* (1979), activities on the report logs without supporting records of authorisation could point toward potential fraudulent activities.

(2) Planning the investigation

Planning is an essential part of the investigation process that will be scrutinized if ineffectively performed. The work plan of the investigation team will decide which direction the investigation will take and, ultimately, if the goals of the investigation were met. The work plan will typically include aspects such as scope, goal, statement, questions that need to be answered, resources required, presentation considerations and modus operandi.

(3) The modus operandi

The proven methods followed during the investigation determine the success of the outcome of any investigation. Proper planning is the answer to the effective use of resources and minimal wastage of time. Covert operations and undercover investigations can work well when dealing with potential employee suspicions. Surveillance methods and the investigation team work on strategies that will best suit the situation of the identified work plan.

(4) Interviews and interrogations

Interviews are usually conducted with the witnesses of crime. Computer investigations need a different approach as most will witnesses an intangible, often indefinable event. The investigator will conduct interviews to gain an understanding of the environment and the incident. Planning and conducting interview considerations are very important. According to Krauss *et al.* (1979), the purpose of an interview will be to achieve the following:

- Information the establishes essential information about the crime;
- Leads for developing the case further;
- Cooperation of victims for further testimony in court; and
- Information about those involved to discern possible economic motives.

Interrogations are used to gain evidence or useful admissions for the court case. Interrogations reveal that an investigation is taking place. Interviews and interrogations may alert the culprit of a computer incident that an investigation is taking place. Therefore, the investigation plan will outline the discreetness of the investigation.

(5) Gathering the case

Properly organisation investigations lead to strong cases. The investigation is always conducted as though it were to appear in court. According to Kuchta (2002), the value of all work done during the investigation is dramatically reduces is proper reporting is not considered. The internal and external investigation team will be responsible for the immaculate quality of work.

4. Conclusion

Businesses manages and balances time, scope and costing constraints. In terms of disaster recovery and business continuity, every activity that occurs within the borders of a company should have formal processes to be followed in the event of an emergency. According to Vecchio-Flaim (2001), regardless of whether the incident is a criminal matter, civil matter or corporate internal personnel issue, investigators must be cognisant of the fact that computers touch every facet of our lives. A formal framework includes the processes and practices to follow in the event of an incident and includes the segregation of duties and responsibilities. The company ensures that all relevant and feasible incidences are investigated as though the case were a criminal proceeding. Incidences can only be taken to court if the correct procedure and forensically sound methods were followed.

The CIRF is the first step to effectively deal with internal and external computer incidences. This will ensure that the company is:

- Adequately prepared;
- Proving due diligence to the company's share holders;
- Legally pursuing internal and external incidences;
- Avoiding panic and rumours;
- Managing incidences well.

Bibliography

I. JORDAN, E., SILCOCK, L. (2005) Beating IT Risks. John Wiley & Sons Ltd. West Sussex, England.

II. KIPPER, G (2007). Wireless Crime and Forensic Investigation. Auerbach Publications.

III. KRAUSS, L., MACGAHAN, A. (1979) Computer Fraud and Countermeasures. Prentice-Hall Inc.

IV. KRUSE, W., HEISER, J. (2002) Computer Forensics: Incident Response Essentials. Addison Wesley.

V. KUCHTA, K. (2002). Forensic Methodologies: A Computer Forensic Professional's Compass! Law, Investigation and Ethics.

VI. MARCELLA, A., GREENFIELD, R. (2002) Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes. Auerbach Publications.

VII. RYDER, K. (2002). Computer Forensics – We've had an incident, who do we get to investigate. SANS Institute.

VIII. STEPHENSON, P. (2000). Investigating Computer-Related Crime. CRC Press LLC.

IX. TSOUTSOURIS, D. (2001). Computer Forensic Legal Standards and Equipment. SANS Institute.

X. VON SOLMS, S., VON SOLMS, R (2008) Information Security Governance. Springer, United States of America.

XI. VECCHIO-FLAIM, C. (2001). Developing a Computer Forensics Team. SANS Institute.
XII. WILDING, E. (2006). Information Risk and Security. Gower Publishing Limited.