New Method of Forensic Computing in a Small Organization

Suhaila Ismail, Arniyati Ahmad, Mohd Afizi Mohd Shukran

Department of Computer Science, Faculty of Science & Defence Technology, National Defence University of Malaysia, Sungai Besi Camp, 57000 Kuala Lumpur, Malaysia.

Abstract: Forensic computing is an important element in addressing security incidents by conducting digital investigations, retrieving and analyzing digital evidence and prosecuting the offender by taking legal actions. Currently, only larger company and multinational organization are able to implement their forensic computing in house. It is important to motivate and cultivate small organizations to implement forensic computing in their organizations which are smaller in scale in terms of people, technology and resources. Results from interviews conducted shows that most desktop support projects have not implemented forensic computing in their operations due to lack of awareness, knowledge and expertise on this subject, beside the implementation cost that can be the bigger constraint. This paper provides a model that could be adapted in smaller organization in implementing the forensic computing. It also recommends the ‘pre’-planning phase, the ‘during’ phase and the ‘post’ phase which defines the activities that the organization needs to be aware in implementing forensic computing in the organization.

Key words: Forensic Computing, Digital Forensics, Digital Forensic Investigation, Incident Management.

INTRODUCTION

Forensic computing is a “methodological series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media that can be presented in a court of law in a coherent and meaningful format” (Wiles, 2007). Computer forensics is not only a series of activities, but it also requires specialized skills in order to collect and preserve data on systems that have been breached by either internal or external parties. Collecting and processing a digital crime scene can be difficult, time consuming and time sensitive data (British-North American Committee, 2007; Nikkel, 2009).

Forensic computing which is very much essential in this era has not been applied in most of the smaller organizations and desktop support projects, due to lack of awareness and knowledge in this field. There has been tremendous work in terms of mapping out the model and framework of digital forensics investigations as well as the importance of having an incident management in place in an organization and guidelines in implementing digital forensics in an incident management (Sinangin, 2002). As far as addressing security risks are concerned, larger organizations recognize the importance of implementing forensic computing in their organization, but on the other hand, smaller organizations or organizations that outsource their desktop support services to external parties tend to neglect the importance of preserving data and evidence for future digital investigations (Deniz, Sinangin, 2002; Kennedy, 2009).

Organizations that have implemented a forensic capability in their organization have the edge to collect, preserve, examine and analyze the data or evidence to determine the sustainability of their system and whether or not any sensitive and confidential information have been compromised. The digital forensics techniques and methodologies would not only support the digital forensics investigations, but could also assist in analyzing security incidents and operational incidents and recover the effected system (Radack, 2009).

It is essential for the organizations to be more aware that to integrate the security incidents with forensic computing, the first and most important step the organization should take is to plan and prepare for an in-house forensic capability. Another important aspect to be considered in implementing an in-house forensic capability is to work together with the legal advisors from legal department and management team in the organization, also with the law enforcement officials externally (Kent, 2009; Bainbridge, 2000; Tayola, 2007).

In order to implement forensic computing in smaller organization, this paper has proposed a framework model for implementation and recommended some activities need to be considered for the ‘pre’, ‘during’ and ‘post’ phases for the implementation. The scope of this paper is at organizations and the legal aspects associated to forensic computing in United Kingdom and Malaysia.
MATERIALS AND METHODS

Data Gathering for Forensic Computing:
Further study has been made to get more information in the existing market and expert opinions in forensics and incident management fields, two sets of interview questionnaires were sent to two different groups of experts. The first wave interview was targeted for the forensic experts in Malaysia. The second interview questionnaires were sent to desktop support specialist and project managers that have experience in dealing with desktop and servers based projects. The reason why the interview questionnaires were distributed to the specialists in Malaysia is to gain more insight to the situation of organizations in Malaysia. This is a different case for the organizations in the UK, where the level of awareness of the need to implement forensic computing in organizations is better and recognized. There were 8 sets of interview questions sent to forensic organizations and government bodies which only 2 have responded. Table I, listed the interview sets in detail.

<table>
<thead>
<tr>
<th>No</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Is there currently any Digital Evidence Handling and Acquisition Procedures implemented in Malaysia? If yes, how long has it been implemented? And is the document accessible to public? If no, what is the procedure that is currently being used in Malaysia? (Using basis from ACPO guidelines in the UK or Electronic Crime Scene Investigation: a Guide for First Responder by the US Department of Justice)</td>
</tr>
<tr>
<td>2</td>
<td>From your point of view, is Forensic Computing/Digital Forensics implemented in most of the organizations in Malaysia? Is there a need to implement Forensic Computing in smaller organizations?</td>
</tr>
<tr>
<td>3</td>
<td>As your organization is a member of the Information Security Technical Committee (TC 5) that plays a significant role in developing and establishing security and standards, what is your opinion on the standards that are currently used in forensic computing implementations and how effective is it?</td>
</tr>
<tr>
<td>4</td>
<td>What are the current challenges in implementing Forensic Computing in organizations and what are the suggested guidelines from your expert view for the organizations to address the challenges?</td>
</tr>
<tr>
<td>5</td>
<td>Based on your expert opinion, how would you indicate the level of awareness for implementing forensic computing in organizations in Malaysia? And what has been done to promote this?</td>
</tr>
</tbody>
</table>

The second interview questions are targeted towards gaining more information from the desktop support specialists on their take on digital forensics and implementing it in desktop support projects. The interview questionnaires distributed to Malaysia’s desktop support experts to align with the first set of questionnaires. List of interview questions are explained in Table II.

There were 10 sets of interview questions sent to desktop support specialists that resulted in 7 feedbacks, 2 answering the questionnaires briefly and 5 responded that they are not qualified to answer the interviews because of lack of awareness, knowledge and experience in forensic computing.

<table>
<thead>
<tr>
<th>No</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Please describe briefly forensic computer forensics from your point of view</td>
</tr>
<tr>
<td>2</td>
<td>In your opinion, what is the importance of implementing forensic computing?</td>
</tr>
<tr>
<td>3</td>
<td>Is Forensic Computing/Digital Forensics implemented in most organizations? Is there a need to implement Forensic computing in smaller organizations or outsourced projects (e.g.: desktop support projects)? Have you been involved in small organizations or desktop projects that have implemented computer forensics in their operation?</td>
</tr>
<tr>
<td>4</td>
<td>How would you indicate the level of awareness for implementing forensic computing in organizations? And what has been done to promote this?</td>
</tr>
<tr>
<td>5</td>
<td>How important and to what extent would you implement forensic computing in a small organization/a desktop support project? What are the main determinants or factors to establish this? (in terms of resources, cost and etc)</td>
</tr>
<tr>
<td>6</td>
<td>From your expert opinion, what are the potential challenges that the organization will face in implementing forensic computing in their organization?</td>
</tr>
<tr>
<td>7</td>
<td>Referring to the above question, what are the actions that need to be taken to address the challenges stated above?</td>
</tr>
<tr>
<td>8</td>
<td>If a forensic computing framework is aligned with the current incident management, what are the implications to the organizations?</td>
</tr>
<tr>
<td>9</td>
<td>Finally, do you have any recommendations in implementing forensic computing in small organizations or desktop support projects based on the substantial need for a forensic computing capability in organizations?</td>
</tr>
</tbody>
</table>

Interviewees’ Findings:
Findings from the first wave interview can be summarized as follow:

- Summary Answer of Question 1:
There is currently no official or standardized Digital Evidence Handling and Acquisition Procedures implemented in Malaysia. Many companies performing digital forensics, both private and semi-government agencies follow different procedures. Some will follow UK guidelines as Malaysia’s laws are more aligned with the UK but others will follow the US standards as they are more influenced by US standards as a lot of the professional certifications (such as CISSP and CISA) are initiated in the US.
• **Summary Answer of Question 2:**
  Not many organizations have a Forensic Readiness program and don’t know where to escalate the problem in the event of need a digital forensics investigation. The lack of confidence in the law enforcement’s capability to address the issues is also a concern and this is due to lack of funding, training and resources of the law enforcers. Most organizations do not know much about forensics and are not concerned about preserving any evidence when a security breach or incident occurs. Forensic computing is a matter of having the right processes and technology in place. For smaller organizations in Malaysia, the cost is the biggest factor, which they have to justify the cost benefit of implementing such forensic computing. The least an organization could do is provide basic training (i.e. basic first responder) and use existing IT staff and train them with the best practices of digital forensics and procedures.

• **Summary Answer of Question 3:**
  There are currently no published forensic computing standards from the International Standards Committee or any other international body (ITU-T, etc) for the moment. The only standards available are developed by individual organizations within a country, so they only apply for their native countries, like in the UK, US and Australia. Work is being done to come out with a standard that will apply across all countries so that digital forensic evidence captured in one country can be applied in the court of law in another country. This is important and crucial as internet crimes are now being perpetrated by people in one continent on people across the globe. Evidence will eventually need to be collected all over the globe and a standard will greatly enhance the admissibility of digital evidence in whichever court it will appear in the future.

• **Summary Answer of Question 4:**
  One of the challenges is to identify the need for implementing Forensic Computing, whether the benefits outweigh the costs. This can be done with proper Risk Management techniques but not many organizations apply a proper Risk Management framework. To address this, there is only education and regulatory compliance. Education will help expose IT managers to evaluate Risk and determine the effectiveness of the IT Programs they wish to implement, be they Forensic Computing or even a server upgrade exercise. Courses on risk management need to run, IT Managers should consider taking IT certification courses that cover such topics and more importantly, top Management has to push the idea from the top down. Next challenge is educating the personnel, especially the 1st responders. They always fail to adhere to the best evidence rule and eventually render the evidence unusable in the court of law. Organizations need to create awareness programs and keep educating the staff on the procedures and practices of forensic computing. The third challenge is the high cost of setting a forensic team. However, this can be tackled by using open-source forensic tools and freeware.

• **Summary Answer of Question 5:**
  The level of awareness for implementing forensic computing is still very low. Most organizations won't think of it until an incident occurs. It's like buying insurance. Most people will not think of buying insurance until after they got into an accident or are struck by a serious illness. This could be overcome by making it a mandatory requirement for certain businesses, have road shows by corporations who have successfully implemented such programs and had them pay off, increase awareness during security and IT conferences and exhibitions (WCIT, SecurAsia, Cebit, etc.) by having speakers talk on such topics. Best would be in general IT settings and not in security focused events as the awareness has to be instilled in the general IT group, especially among the key decision makers and stake-holders in a company (CIO, CEO, etc).

  The second wave interview can be summarized as follow:

• **Summary Answer of Question 1:**
  Forensic computer forensics is about investigating computer crimes and implementing the precautions against computer crimes from re-occurring in an organization.

• **Summary Answer of Question 2:**
  Forensic computing is important to help eliminate security threats like email harassment, falsification of data, embezzlement, sabotage, and industrial espionage, which involves selling sensitive information to a competitor.

• **Summary Answer of Question 3:**
  Not all organizations, but most big organization has put in place processes, procedures and security policies. There is a need to do the same for smaller organizations likewise outsourced projects as smaller organization too faces the same security threats.
**Summary Answer of Question 4:**
As there are more security threats today, it is essential to implement forensic computing. There is awareness for implementing forensic computing in organizations; hence, they have deployed different security tools for intrusion detection / prevention but no digital forensics considerations.

**Summary Answer of Question 5:**
Cost is surely a main factor to establish the implementation forensic computing in a small organization/a desktop support project. The need for purchasing tools, also to re-design network architecture to allow the deployment of tools.

**Summary Answer of Question 6:**
Cost is definitely one of the challenges. Other than that, it is the skills required to implement forensic computing.

**Summary Answer of Question 7:**
The most important action is to train up resources with the right skills, which is needed in addressing these problems.

**Summary Answer of Question 8:**
Incident management process is different from organization to organization. Hence, how to align the two is subjective.

**Summary Answer of Question 9:**
To start-off, it is good to put in place procedures and policies. It is also a good practice to keep updated all computer / OS patches when it comes to desktop support.

This clearly indicates the level of awareness in regards of forensic computing is very low in Malaysia, and necessary steps should be taken to promote this.

**The Proposed Method:**
In order to provide a clearer standard for organizations to integrate forensic computing into a readily available desktop support process or incident management or desktop support, this section outlines the methods by developing a framework for addressing this concern.

![A Framework for integrating forensic computing in an organization.](image)

Fig. 1: A Framework for integrating forensic computing in an organization.

In addressing all the requirements, the framework was formed on these specifications.

1. The framework would be efficient and effective in meeting the elements in any existing incident management (as illustrated in Figure 1). The components in the framework are realistic and common and easily implemented in the organization.
2. The framework would accommodate in creating and establishing forensic policies, procedures and guidelines by providing a clear process flow and connecting all the relevant parties involved and in which process they belong to.
3. The framework allows constant monitoring and if in any cases after evaluation of the attributes of the framework, and the components are not functioning as planned and not addressing the overall digital forensics implementation, the framework could be improved, redesigned and reestablished.

Figure 1 illustrates the framework in integrating forensic computing to an incident management or system support. The following key roles have been established using both the existing parties in an incident
management process and introducing new parties, such as the forensic team and external party into the whole picture to ensure adequate services and support for addressing digital forensics issue in the organization. The layers represent the grouping of processes and parties which is significant at a point of time. This will be further explained in detail as follow:

1. **Request Layer:**
   This layer defines the channels or parties that assist in the incident management process as the first level responder. The first level responder are usually either the IT Helpdesk, where the users call or log in their incidents, or the onsite IT technicians that are available to the users, depending on the nature of the organization. This group will then record the incident logged by the user and solve the incident. If they are unable to solve the incident, which shows that the incident does not normally occur, this incident will then be assigned to the second level responder.

2. **Channel Layer:**
   This layer defines the channels or parties that assist in the incident management process as the first level responder. The first level responder is usually either the IT Helpdesk, where the users call or log in their incidents, or the onsite IT technicians that are available to the users, depending on the nature of the organization. This group will then record the incident logged by the user, and solve the incident. If they are unable to solve the incident, which shows that the incident does not normally occur, this incident will then be assigned to the second level responder.

3. **Fulfillment Layer:**
   This layer defines the parties that will assist in the fulfillment of the incident request and will address the incidents assigned by the first level responder. The second level responders are the people that are assigned with the unsolved incidents, by analyzing and determining the nature, and the criticality of the incident. It will be the responsibility of the second level responder to report the problem to the management team if the incident is deemed to be a threat to the organization and out of the ordinary. If the incidents could not be solved, then it would be assigned to the specialist’s team. The second level responder will also assign the case to the forensic team if the need arises. The forensic team would then follow up on the case, and instigate the incident without interrupting the incident resolution. If the organization does not have the capability to further analyze the evidence retrieved, then a predetermined external party would be engaged.

4. **Monitoring Layer:**
   This layer defines the monitoring part of the framework. The management team has the responsibility to measure and monitor the overall major security incidents and the digital forensic investigation. The management team could vary according to the organization, it might be the project manager in charge, or the team leader or even the top management, the party which have the power to make decisions and resolve non-technical matters, such as law suits or financial issues.

**RESULTS AND DISCUSSION**

**Recommendations (The Pre, During and Post):**

After mapping out the possible solution for the organization to implement a forensic computing capability or readiness, there are several key recommendations that could be very useful for the organization. These recommendations are categorized in terms of the periods in implementation, the ‘pre’-planning phase of the overall forensic capability, the ‘during’ phase which are the activities that needs to be done during implementation of forensic computing and the ‘post’ phase which defines the activities that the organization needs to be aware of after implementing forensic computing in the organization.

- The ‘Pre’ Recommendations
  1. Conduct a thorough risk assessment to determine how much the damage of a computer incident would affect the organization, and evaluate the necessity of housing an in-house lab, and outweigh the benefits through the results.
  2. Establish a Regulatory Compliance in the organization by following the legal expectations.
  3. Identify the personnel or a team, in charge of forensics dealings in the organization. This will then depend on the nature and risk evaluation, whether it would be a dedicated staff or IT personnel, who would then be trained with the suitable investigations and computer skills, and educated in terms of the digital forensics investigations procedure and guidelines.
  4. Familiarize the legal aspects of digital forensics, the processes in handling digital evidence, analyzing and reporting the results to be presented in court.
5. Identify the external parties that would be able to assist in analyzing the evidence during the investigations.
6. Develop and implement a clear and sound Forensic Policy and disseminate the policy to the users.
7. Develop and implement a standard digital forensic guideline which is customized to suit the organization, in terms of processes and personnel.
8. Identify the Forensic team according to the nature and capability of the organization.
9. Prepare the IT Team; including the incident responds team and the specialists on the forensics knowledge and techniques.
10. Identify the third party that would assist in analyzing the data if the organization decides to outsource.

- The ‘During’ Recommendations
  1. Ensure that the forensic investigation will progress without interrupting the incident response to the current security breaches in the organization. The day to day operations would still be intact.
  2. Ensure that the evidence is preserved, without contamination and provide a trail of evidence.
  3. Ensure the forensic team follow and abide the guidelines, and conduct the investigation on the standards that are predetermined by the organization.
  4. Ensure that the forensic tools, forensic toolkit, forensics software and application, forensics workstation are up and running, and updated accordingly.

- The ‘Post’ Recommendations
  1. Take appropriate actions, if the case would be presented in court, the proper preparations needs to be executed. The preparations are in terms of documentations, and witnesses of the investigation.
  2. For criminal cases, the organization must have a procedure to report the problem to the local law enforcement for further actions. If the case is then decided to not be taken to court, then appropriate measures needs to be taken to enforce the policies and legal implications that has been described. If it is an internal case, then the employee deserves disciplinary action and etc.
  3. The organization, or the security and forensics team, must always be updated with the latest news and latest security breaches.
  4. Monitor and review the forensic policy, guidelines, and procedures accordingly, which includes the appropriate maintenance and use of forensic equipments and tools.
  5. Constantly educate and train the parties identified in the framework on their responsibilities and tasks in the whole forensics process, with the latest techniques and appropriate training.
  6. When in doubt on legal matters concerning digital evidence or investigations, always refer to the legal advisors in the organization to eliminate any future.

Conclusion:
As a conclusion, that most all small organizations and desktop support projects have not implemented forensic computing in their operations, and are not fully aware of the implications of neglecting the importance of having a forensic capability within the organization. It was based on the feedback from the interview questionnaires that have been sent out. Most of the desktop support specialists interviewed were reluctant to provide information due to lack of knowledge and experience on this subject. Meanwhile the feedback from questionnaires that have been sent out to the forensic specialists were more concerned about the level of awareness of the organizations in implementing forensic capability and how the organizations fail outweigh the benefits to the cost of this newly recognized field. Given this situation, this research maps out the process flow and provides a suggested framework to integrate forensic computing into an existing incident management process in a desktop environment, which is intended to be a basic recommended guideline for desktop support projects or smaller organizations to kick-off a forensic capability.

REFERENCES


