Cognitive Approaches for Digital Forensic Readiness Planning

Antonio Pooe, Les Labuschagne

Chapter 4

COGNITIVE APPROACHES FOR DIGITAL FORENSIC READINESS PLANNING

Antonio Pooe and Les Labuschagne

Abstract This paper focuses on the use of cognitive approaches for digital forensic readiness planning. Research has revealed that a well-thought-out and legally contextualized digital forensic readiness strategy can provide organizations with an increased ability to respond to security incidents while maintaining the integrity of the evidence gathered and keeping investigative costs low. This paper contributes to the body of knowledge in digital forensics related to the design and implementation of digital forensic readiness plans aimed at maximizing the use of digital evidence in organizations. The study uses interviews as part of a mixed-methods approach. In particular, it employs a mix of informal conversational and standardized open-ended interview styles conducted with industry experts over a variety of communication media.

Keywords: Digital forensic readiness, digital evidence, cognitive approaches

1. Introduction

From the perspective of law enforcement agencies, the forensic process begins when a crime has been committed or when a crime has been discovered and reported [6]. Forensic readiness enables organizations to preempt the occurrence of crimes by gathering evidence in advance and, in doing so, derive benefits in instances where prosecution becomes an issue and limit their risks [5].

The organizational requirement to gather and use digital evidence has been recognized in a number of studies (see, e.g., [2, 5]). These studies stress the importance of a structure to maintain the integrity of forensic evidence. In particular, Yasinsac and Manzano [7] note that organizational policies play a critical role in providing the needed structure. Yasinsac and Manzano also propose six categories of policies to facili-

tate digital forensic investigations. The categories are designed to help organizations deter digital crime and position themselves to respond to attacks by improving their ability to conduct investigations. The six categories of policies that facilitate digital forensic investigations are:

1. **Retaining Information:** Policies that relate to the storage of information by an organization.
2. **Planning the Response:** Policies that guide an organization's plans for responding to incidents and situations.
3. **Training:** Policies that address the training of staff members and others affiliated with an organization.
4. **Accelerating the Investigation:** Policies that address the operational aspects of investigations.
5. **Preventing Anonymous Activities:** Policies that address an organization's proactive efforts against fraud.
6. **Protecting the Evidence:** Policies that address the handling and protection of evidence and other vital data.

From the above discussion, the concept of digital forensic readiness has two main objectives: (i) maximizing the ability to collect credible digital evidence (Categories 1, 2, 5 and 6 above); and (ii) minimizing the cost of digital forensics during incident response (Categories 3 and 4). While this reinforces the importance of cohesive policies in organizations, the problem with the categorization is that it suggests that organizations must have all six policies in place, which may result in possible duplication and/or conflicting policy statements. Furthermore, it may lead to confusion in identifying the authority/governing policy for facilitating digital investigations. While the policies are important, they alone do not guarantee a holistic digital forensic readiness plan.

Because of the potential policy conflicts, our study used mixed methods interviews [4] as a means to develop a holistic digital forensic readiness plan. The interviews were employed as an exploratory research tool to gather information from subject matter experts and to capture real-world experiences with the goal of identifying key components for consideration.

2. Research Design

Mixed method research is a design with philosophical assumptions and various methods of inquiry [4]. The philosophical assumptions guide the

direction of the collection and analysis of data while the combination of qualitative and quantitative methods of inquiry in a single or series of studies offers a better understanding of research problems than each approach on its own [12].

The intent of the two-phase exploratory design is that the results of the first method (qualitative) can help develop or inform the second method (quantitative) [4]. This is based on the premise that an exploration may be needed for one or more reasons, which takes into account the possibility that measures or instruments are not available, variables are unknown and no guiding framework or theory exists.

This design is used because it enables the exploration of a phenomenon in detail and the development and testing of the resulting conceptual model [4, 12]. The use of the design in this study helps validate qualitative data with quantitative results.

Interviews were used as the data collection method. In mixed methods research, open-ended qualitative interviews (INT-QUAL) are featured more frequently than closed-ended quantitative interviews (INT-QUAN). Qualitative interviews are usually non-directive and general ("tell me about your school"). On the other hand, quantitative interviews are structured and closed-ended ("which of the following describes the food in your school cafeteria – very good, good, bad, very bad") [12].

2.1 Types of Interviews

Patton [8] defined four types of open-ended interviews, ranging from the least structured (informal conversational interviews) to the more structured (general interview-guided approaches) to the most structured (standardized open-ended interviews). He also described closed fixed-response interviews but does not advocate their use. The four types of open-ended interviews are:

- **Type 1: Informal Conversational Interviews:** Questions emerge from the immediate context and are asked in the natural course of the interview. The question topics and wording are not predetermined.

- **Type 2: General Interview Guide Approaches:** Topics and issues are specified in advance in outline form. The interviewer decides the sequence and working of questions in the course of the interview.

- **Type 3: Standardized Open-Ended Interviews:** The exact wording and sequence of questions are determined in advance. All

the interviewees are asked the same basic questions in the same order. Questions are worded in a completely open-ended format.

- **Type 4: Closed Fixed-Response Interviews:** Questions and response categories are determined in advance. The responses are fixed. The respondent chooses from among the fixed responses.

For purposes of this study, a mixture of Type 1 and Type 3 open-ended interviews was used. Teddie and Tashakkori [12] state that researchers who select the INT-QUAL strategy may use any of the open-ended interview approaches and potentially combine the interview types. They suggest the following sequence of interview techniques:

- Start with the unstructured informal conversational interview approach to build rapport and elicit spontaneous responses.
- Move to the interview guide approach, which provides a more comprehensive outline of topics, but still maintains a conversational tone.
- Finish with the highly structured, standardized open-ended interview approach, which greatly increases response comparability.

Our study began with an unstructured informal conversational interview approach, followed by a highly structured, standardized open-ended interview approach. The questions were formulated based on a literature survey conducted in 2011 [9].

2.2 Interviews

This section discusses the criteria used to select the interviewees, the communication channels used to conduct the interviews and the ethical considerations related to the interview process.

The interviewees were selected based on three criteria:

- Individuals from the private sector and law enforcement were selected in order to emphasize the multi-disciplinary aspects of the domain and to capture a broad range of views from subject matter experts involved in different aspects of the digital forensic process.
- Individuals with experience in digital law and/or digital forensics were selected to ensure that the input gathered was not biased and addressed the technical and legal dimensions of digital forensics.
- Individuals who had been practicing digital forensics in South Africa for a period of no less than three years were selected. Since

Table 1. Interviewee profiles.

Interviewee	Experience > 3 Years	Law Enforcement	Private Sector	Management Position
INT1	Yes	Yes	No	Yes
INT2	Yes	Yes	Yes	Yes
INT3	Yes	No	Yes	Yes
INT4	Yes	Yes	Yes	Yes
INT5	Yes	No	Yes	Yes
INT6	Yes	Yes	No	Yes
INT7	Yes	Yes	Yes	Yes

the context of the study was South Africa, it was important to identify subject matter experts with experience in the geographical context.

These criteria ensured that the interviewees would provide a mixture of opinions based on their experiences in their different working environments.

Studies have shown that, while open-ended interviews are typically conducted in a face-to-face manner, they may also be conducted by telephone or over the Internet [11, 12].

A total of seven interviews were conducted using three channels: four interviews were conducted face-to-face, one was conducted over the phone and two over the Internet. Due to the volume of data collected during the interviews, the ATLAS.ti tool [1] was used to process and analyze the data.

3. Interview Results

This section describes the results of the seven interviews. All the interviewees met the selection criteria. Table 1 summarizes the interviewee profiles.

We now provide a summary of some of the questions, the responses received and the interviewees that were in agreement. Based on the responses, cognitive approaches to digital forensic readiness planning were used to develop a conceptual model.

- *Question 1: Should South African organizations be concerned about digital crimes?*

  The responses to this question revealed the following opinions:

  - Digital crimes are on the increase (All).

  - The intangible nature of data in an electronic format causes people to lower their defenses (INT1, INT4, INT7).
  - Modern criminals are technologically literate and have access to good legal representation (INT1, INT2, INT3).
  - Immaturity of the digital forensics profession allows criminals to go free (INT5).
  - Following correct investigative processes to preserve evidence is important (INT6).

- *Question 2: Which three types of digital crimes do you find to be the most prevalent?*

  The following crimes were found to be prevalent:

  - Financial crimes (All).
  - Child pornography (INT4, INT5, INT6, INT7).
  - 419 scams (INT4, INT6).
  - Malware-related crimes (INT1, INT2).
  - Intellectual property theft (INT1, INT5).
  - Hacking and illegal access (INT2, INT3).
  - Internet misuse (INT5).

- *Question 3: Which sector do you find to be the most targeted?*

  The responses indicated the following sectors:

  - Banking/financial sector (All).
  - Large corporations (INT2, INT4, INT7).
  - Individuals (INT2, INT3).
  - Mining (INT4).
  - Businesses (INT5).

- *Question 4: Have you noted any challenges regarding the prosecution of digital crimes?*

  The following challenges were noted:

  - Knowledge of digital forensic principles is lacking among the stakeholders (All).
  - Lack of understanding of legal requirements (INT1, INT3, INT4, INT5, INT6).
  - Lack of resources (INT2, INT7).

- *Question 5: Do you or your organization have a digital forensic model that has been adopted?*

  All the respondents indicated that they use their own entity-specific model, which may differ from those used by other organizations.

- *Question 6: Does electronic evidence provide sufficient assurance of non-manipulation?*

  Provided that the correct processes were followed, all the respondents were of the opinion that electronic evidence can be relied upon.

- *Question 7: Is there a standard process for electronic evidence gathering?*

  All the respondents indicated that, while processes adopted in their individual organizations were similar, no process standards specific to South Africa exist.

- *Question 8: Does the law adequately position the acceptable use of and/or extent to which electronic evidence can be used in civil or criminal proceedings?*

  All the respondents referred to the Electronic Communications and Transactions (ECT) Act of 2002 as legislation that makes it possible to present electronic evidence in a South African court of law. However, the following contradictions were noted:

  - Existing laws support the ECT Act (INT4, INT5, INT7).
  - Discrepancies exist between the ECT Act and existing laws (INT2).

- *Question 9: Does the law cater to the complexities of modern IT devices?*

  All the respondents indicated that the law lagged behind technology. While the ECT Act was found to be strong legislation, the respondents indicated that it needed periodic review.

- *Question 10: What are the factors that contribute to electronic evidence being rendered inadmissible?*

  All the respondents pointed to digital forensic processes and procedures as a good foundation for ensuring the admissibility of evidence.

- *Question 11: Have you noted any challenges that prevent digital crime investigators from correctly applying a digital forensic model or framework?*

All the respondents indicated that a single point of reference was needed. Other points noted were:

- South Africa needs a specific model (INT5, INT7).
- The model must enable and support legal processes (INT7).
- The model must be flexible (INT5).

- *Question 12: Do you think digital forensic investigators are sufficiently trained to do their work?*

  All the respondents identified a need for more training of local digital forensic investigators.

- *Question 13: Have you noted any challenges that prevent prosecutors from successfully prosecuting digital crimes?*

  The responses identified the following challenges:

  - Lack of interest in digital crimes (INT1, INT3, INT4, INT5, INT6, INT7).
  - High case loads (INT1, INT2, INT4, INT5, INT7).
  - Lack of digital forensic training and awareness (INT2, INT5, INT7).
  - Lack of cooperation (INT5).

- *Question 14: Do you think state prosecutors are sufficiently trained to do their work?*

  All the respondents opined that a training need exists for state prosecutors.

- *Question 15: What do you think should be done to increase the prosecution rate of digital crimes in South Africa?*

  The responses included:

  - Special digital forensic courts (INT1, INT3, INT4, INT5, INT7).
  - More digital forensic education, training and awareness (INT1, INT2, INT6, INT7).
  - More research focused on digital forensics (INT1, INT6).
  - Compulsory reporting requirements (INT1, INT5).
  - A new law of evidence for electronic crimes (INT2).
  - Define processes and a model (INT4).

4. Data Analysis and Interpretation

This section discusses the application of the data analysis method and presents the results of the analysis.

The data analysis was conducted by transcribing each interview and reading each transcript repeatedly to identify the codes for each question answered by the interviewees. Techniques from immersion/crystallization and constant comparison (grounded theory) were applied to assist in developing the initial and final codes [3]. The iterative reading process made it possible for focus/immersion to be applied to each question and for the emergence/crystallization of themes to take place. Differences in findings (codes and themes) were also resolved using the iterative process. The process resulted in three environments: corporate, industry and legislative.

4.1 Corporate Environment

The correlation of the interview results yielded the following key findings and analyses:

- **Organizational Culture:** A large proportion of organizations were found to have a habit/culture of ignoring/overlooking small crimes. Additionally, organizations were found to invest the least amount of resources to address the risk of digital crimes. Also, a lack of awareness about digital crime prevention and detection was found to exist.

  These findings suggest that, by creating a culture of no tolerance to crime and taking action on reported crimes, an organization can significantly reduce its risk exposure to digital crimes.

- **Policies:** Interviewees noted that a general lack of governance, policies and procedures relating to fraud risk management existed in many of the organizations with which they had been in contact.

  These findings support existing literature (as discussed earlier in this study) on the importance of policies as they relate to achieving digital forensic readiness.

- **Communication Channels:** The reporting of digital crimes was found to be low. The causes mentioned included a culture of "sweeping things under the carpet" along with ignorance, and the lack of education and law enforcement effectiveness.

  These findings suggest that encouraging and supporting open dialog, coupled with crime reporting mechanisms can positively impact organizational culture.

- **Emerging Risks:** The following areas of risk were identified:
  - The intangible aspect of technology causes people to lower their defenses. This is evident in the various types of white-collar crimes committed using technology.
  - Modern criminals are technologically literate and have access to financial and other resources, including good legal representation.
  - Criminals are quick to exploit innovations in mobile technology.
  - The digital forensic industry is not sufficiently mature, enabling criminals to take advantage of ambiguities in global legislative structures.
  - Digital forensic investigators often do not follow due process, which contributes to the low prosecution rate of digital crimes.

  The findings suggest the importance of being cognizant about emerging risks because they affect the nature of controls and mitigation strategies that organizations employ.

- **Crime Trends:** Respondents were of the opinion that digital crimes are on the increase and will affect all current and future users of technology. The high prevalence of crime is attributed to legislative gaps.

These findings suggest that increased awareness of crime trends can aid organizations in focusing their attention and resources on high risk areas.

4.2 Industry Environment

The correlation of the interview results yielded the following key findings and analyses:

- **Standards:** The absence of standards for digital forensics was identified as an inhibiting factor to the prosecution of digital crimes. An open culture of information sharing was noted as necessary to promote the maturity of the digital forensic profession. Specific to a digital forensic model, this should not be legislation but, instead, recommended guidelines that enable and support the legal process while being sufficiently flexible to accommodate advances and changes in legislation and technology.

These findings suggest that establishing governance structures is an important step to building quality digital forensic case law and professionalizing the digital forensic industry.

- **Methodology:** While digital forensic investigation methodologies exist, there is a need for a single point of reference. This extends to the need for consistency in country-specific standards, processes and methodology. Awareness of research-based methodologies and their alignment to legislation was also found to be necessary.

  These findings suggest that standardization can encourage consistency, conformity, compliance and increase competitiveness in the digital forensic profession.

- **Education:** A lack of cohesion between academics and practitioners was found to exist. While interviewees noted that no single qualification is a prerequisite to qualify as a digital forensic practitioner, specialized training and a balance of education and experience were found to be necessary. A digital forensic model was also found to be essential to guide training efforts.

  These findings suggest that the ideal qualification requirements for digital forensic practitioners are formal education coupled with advanced training in a field of specialization.

- **Training:** Training of all stakeholders was noted as essential. In particular, emphasis was placed on legal requirements as superseding technical processes. Some practitioners lack an understanding of the legal requirements and/or incorrectly apply technical knowledge.

  These findings suggest the need to expose digital forensic investigators to a balanced training curriculum that covers all related disciplines.

- **Development:** There was a lack of continued professional development for individuals in the investigation value chain, including prosecutors, judges and digital forensics practitioners across all sectors.

  These findings suggest the need for organizations to employ qualified digital forensic investigators and provide continuous education and career development in order to ensure that investigators are equipped with the skills necessary to handle modern digital crimes.

4.3 Legislative Environment

The correlation of the interview results yielded the following key findings and analyses:

- **Legislative Culture:** A lack of consideration of digital crimes exists among some judges and prosecutors; this was attributed to high caseloads and limited resources. The creation of special interest groups and special courts could introduce positive changes.

  These findings suggest the need for a culture of cooperation between organizations, law enforcement and prosecuting authorities.

- **eLaw Development:** Specific to South African legislation on electronic evidence [10], the findings indicate that the key strengths of the law are robust legislation and good baselines. On the other hand, the findings also suggest that the law imposes low penalties, there is limited awareness and understanding of the law, and considerable complexity in its use of technical terminology. Lastly, the South African legislation on electronic evidence was perceived as being adequate to cover technological advances over the next ten to twenty years.

  These findings suggest the need for continuous review and development of legislation relating to digital crimes in order to close the gap (of relevance) between technology and the law.

- **Awareness:** The findings suggest that the judiciary is presented with challenges that result in a reluctance to prioritize digital evidence. High caseloads and a lack of awareness of digital forensic processes and methodologies exist. Interviewees pointed to a need for a change in culture. Training and awareness were suggested as effective drivers to implement this change.

  These findings point to the importance of digital forensic awareness initiatives as a means to reduce the reluctance to prioritize digital crimes and increase confidence levels when prosecuting crimes.

4.4 Cognitive Approaches

From the breadth of responses and the associated analysis, it is clear that the development of a digital forensic readiness plan extends beyond the realm of an organization. The corporate, industry and legislative environments each have properties that must be considered when developing a digital forensic readiness plan. These properties are presented in Figure 1.

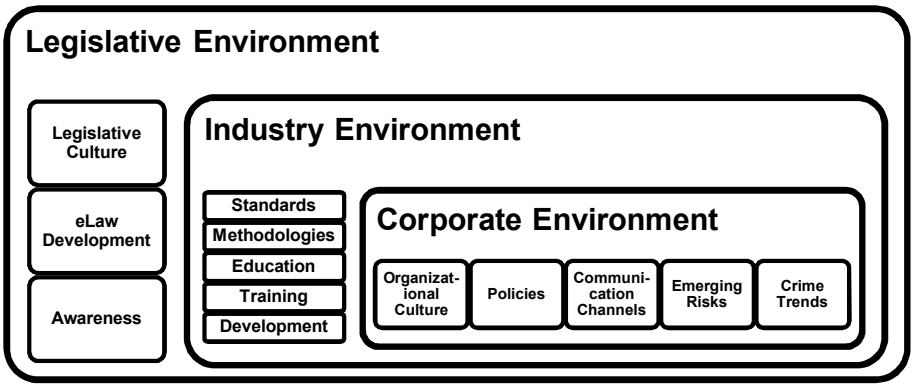

Figure 1. Cognitive approaches for digital forensic readiness planning.

The corporate environment has properties within an organization's control that must be aligned with and support the organization's digital forensic readiness plan. The corporate environment operates within the limitations of the industry environment, which, in turn, is influenced by the limitations of the legislative environment. A critical component of a digital forensic readiness plan is to establish a cooperation strategy that ensures that digital forensic cases can progress seamlessly from their inception in a corporate environment to their conclusion in a court of law (legislative environment), following relevant guidelines in the industry environment to ensure that the integrity of evidence is maintained.

5. Conclusions

This study has sought to investigate cognitive approaches that aid in developing digital forensic readiness plans. The study reveals that developing a digital forensic readiness plan is a task that involves many factors beyond the realm of a single organization. The factors are presented in the form of a conceptual model for organizations to use in process planning to achieve digital forensic readiness. By focusing on the lessons learned from experience, the study provides cognitive approaches to digital forensic readiness that can be used by individuals who wish to explore this topic further as well as by organizations that desire to enhance their ability to respond to security incidents while maintaining the integrity of evidence and keeping investigative costs low.

Our future research will examine digital forensic readiness as it relates to specific contexts such as mobile devices, wireless networks, public key infrastructures and cloud computing.

References

[1] ATLAS.ti Scientific Software Development, A world of data in your hand, Berlin, Germany (www.atlasti.com).

[2] M. Cohen, D. Bilby and G. Caronni, Distributed forensics and incident response in the enterprise, *Digital Investigation*, vol. 8(S), pp. S101–S110, 2011.

[3] J. Corbin and A. Strauss, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, Sage Publications, Thousand Oaks, California, 2008.

[4] J. Cresswell and V. Clark, *Designing and Conducting Mixed Methods Research*, Sage Publications, Thousand Oaks, California, 2011.

[5] S. Hoolachan and W. Glisson, Organizational handling of digital evidence, *Proceedings of the Conference on Digital Forensics, Security and Law*, pp. 33–44, 2010.

[6] P. Kanellis, E. Kiountouzis, N. Kolokotronics and D. Martakos (Eds.), *Digital Crime and Forensic Science in Cyberspace*, Idea Group Publishing, Hershey, Pennsylvania, 2006.

[7] Y. Manzano and A. Yasinsac, Policies to enhance computer and network forensics, *Proceedings of the Second Annual IEEE SMC Information Assurance Workshop*, pp. 289–295, 2001.

[8] M. Patton, *Qualitative Research and Evaluation Methods*, Sage Publications, Thousand Oaks, California, 2002.

[9] A. Pooe and L. Labuschagne, A conceptual model for digital forensic readiness, *Proceedings of the South African Information Security Conference*, 2012.

[10] Republic of South Africa, Electronic Communications and Transactions Act 2002, *Government Gazette*, vol. 446(2), no. 23708, August 2, 2002.

[11] J. Salmons, *Online Interviews in Real Time*, Sage Publications, Thousand Oaks, California, 2010.

[12] C. Teddlie and A. Tashakkori, *Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences*, Sage Publications, Thousand Oaks, California, 2009.