A framework for handling digital forensic evidence and evaluation on cyber resilience

Vinesha Selvarajah  
PhD in Computing Forensic  
Asia Pacific University of Technology & Innovation (APU)  
Kuala Lumpur, Malaysia  
vinesha@apu.edu.my

Jothy Mailvagnam  
MsC Cyber Security  
Asia Pacific University of Technology & Innovation (APU)  
Kuala Lumpur, Malaysia  
TP041322@mail.apu.edu.my

Abstract—Handling cybercrime investigations by identifying digital forensic evidence that intent to analyze and preserve it in well terms and conditions. Most research materials did implement frameworks on handling digital forensic evidence based on their source, format, and type of classification without understanding the process of digital evidence accordingly. As a forensic investigator is a MUST to understand the concept of handling digital evidence by studying each stage of the process with law facts. To this end, we have designed a use case framework on how to handle digital forensic evidence along the process with an explanation in detail. Therefore, evaluating the cyber resilience at this pandemic crisis to highlight the influence of advanced technologies on people. Cyber resilience has been planted in all aspects such as medical fields, business, or industrial areas, or even through cyber threat intelligence with advanced technologies like Artificial Intelligence (AI). Based on cyber resilience studies, the developer has designed a framework for handling digital forensic evidence start with the Identification, Collection, Acquisition, and Preservation phase to be followed for analyzing the correct path of that evidence in a criminal investigation. [1]. Below figure 1 describe a sample flow of cybercrime scene that handle digital evidence adequately whereas the evidence gathered to submit in court for committing that this crime has been occurred by the suspect.

An attack that occurs risk to a person or an organization, is a common routine to erase sensitive data through smart devices or even in a cloud environment where the main motives of a hacker. As incident becomes persistent and sophisticated to an organization floor, they need to be twice secure on cyber resilience that may lead them to damage their internal and external services eventually. [2]

To keep an effective cyber resilience, we bear in mind 3P’s concepts which are, Predict, Prioritize, and Practice. This concept will be helpful to prevent or alert employees if any event occurs to identify the cyber risks and vulnerabilities that have been attacked before. Furthermore, the organization itself being lack of intelligence threat to discover any potential cyber-attack. [2]

Fig. 1. Flow of digital forensic process

The best way to prevent these potential threats in organizations then, employees should attend regular training based on CISRT (computer incident response team) or understanding the incident response policies and to be tested frequently before or after any attack occur which stabilizes the cyber resilience rate. [2]. Where in figure 2 shows the extensions of cyber resilience from ISO 27001 to ISO 27014.

Fig. 2. Cyber resilience framework in general
Usually, the targeted will be forensic investigator, forensic examiner, forensic analyst, and expert witness who able to capture the intent and motive of the preserve evidence. Besides, CSIRT or Incident Respond team can be a part of researching or even analyzing the gathered evidence such as, in an organization that occurred malicious attack or security breaches in SOC lab. The targeted user will undergo investigation stages with a proper procedure under law enforcement in legal action taken. The scope of this study:

- Analyzing and designing a framework for handling digital forensic evidence based on past studies.
- Justification of the proposed framework on digital forensic evidence that could be related to cyber resilience.
- Determining the past facts from the author’s reviews with a conclusion statement.
- Identifying the effectiveness of cyber resilience towards everyone in the technology era.

II. RESEARCH METHODOLOGY

This section explains the past studies of the existing framework for handling digital forensic evidence in various aspects of the technology field along with cyber resilience research done by authors. Hence, those research materials had evaluated and clarified the proposed framework with a hypothesis from the developer reviews. Therefore, knowing about cyber resilience and the impact on the technology era.

Handling the digital forensic evidence process has been designed and implemented in past studies to overcome cybercrime investigation by preserving its digital evidence accurately and securely to proceed in court. Most forensic analysts fail in progressing the evidence stages. In an overall investigation, the investigator will only rely on evidence analyzed and examined by forensic examiners in the lab to make sure the jury reliable the evidence under law enforcement to make a legal judgment for that particular suspect of the crime.

The author [3], has implemented VODE (verification of digital evidence) framework in figure 3 below that encounters undocumented digital artifacts and data of an investigation. Therefore, an interpretative methodology was helpful for a practitioner to complete the process accurately to identify the digital data.

As a result, the author’s VODE has been supportive to the practitioner for analyzing the digital evidence along with an interpretative methodology that founded a digital trace term on the suspect system which captured the testing and verification data. [3]

For a live forensic analysis, three authors [4] has designed a visual decision-support system as a methodology to analyze the inflected system even devices turn off. Which able to erase evidence that is known as “Fileless Malware”. The authors made defined and identified the domain issue by analyzing the visualization system to abstract available evidence during a live investigation. Figure 4 has a layout of four timeline version of visualization-support system in detail.

In conclusion, the authors contributed a tailor-made visualization approach that enables to gather data during the forensic investigation to archive the domain issue faced on how visual security analytics generated. [4]
framework accomplished data storage integrity to manage the digital evidence which is shown in figure 6 below. [6]

![Architecture B-DEC](image1)

Fig. 6. Architecture B-DEC

The author made a statement of forensic investigation process was not processing accordingly. Due to that, the author analyzed and evaluate the observation on how to preserve and gather evidence securely by following each step of handling digital forensic evidence. Also, the author highlighted law enforcement of digital evidence of an investigation to the jury for leading to inadmissibility at court. [7]

The author summarised of cybercrimes involves cloud computing threats to the industrial world. Based on the law enforcement agencies they discovered many digital crime cases that attacked through cloud computing platform. [8]. At the final stage, the author evaluates the difference between modern and traditional digital forensic and examiner process to identify the fastest way of gathering evidence. [8]

Nowadays, technology changes due to advanced AI and electronic devices that make it easier to discover any tiny data from a bulk storage space. Based on that, the author [9] differentiates the traditional digital forensic process in a cloud computing environment to conduct an acquisition phase as a methodology that able to teaches the limitation of cloud environment due to complexity.

From the result, a classroom of Delphi study applied this methodology by analyzing a 20 forensic acquisition process that categorized by SMEs (subject matter experts). Where these experts have skills and knowledge about conducting a forensic process in a cloud computing environment. [9]

Thusly, the author [10] has proposed a proactive mechanized quantity of procedures to discovered the condition and challenges of an electronic logical method. By developing it, in the end, the author registered the circulated condition usage of current logical systems during that period.

On that approach, the system has been utilized as an IaaS model to apply on other sensible logic mechanical assemblies’ structure before an organization process initialized. [10]

![Data Life cycle](image2)

Fig. 7. Data Life cycle

OSINT (open-source intelligence forensic) used in criminal intelligence to discover link analysis and data mining for tracking espionage or cyber terrorism activities. Based on this situation, the author [11] has investigated the incident from the employee who has been suspected. The aim of this investigation to identify the potential evidence by collecting with the selected tools.

Based on intelligence development their benefits of data link in digital forensic by analyzing it can be gathered irrelevant databases. In conclusion, the author’s proposed tool was evaluated in a virtual lab to be designed and verified made under control environment shown in figure 7 below. [11]

![Model of Forensic Performance](image3)

Fig. 8. Model of Forensic Performance

From Fig. 8, the forensic analysis phases were divided into four stages of architecture: [12]

1. Collection of data and generator of information.
2. Analytics and extraction module of future.
3. ML (machine learning) models.
4. Types of metrics in models of analysis.

III. CYBER RESILIENCE REVIEWS

The article has concluded the difficulty of handling the cyber resilience policies of an organization structure. The cyber resilience policies prevent risk from cyber threats or espionage terms which may lead to human error or company reputation. The author succeeds by designing a model and defined an effective cyber resilience strategy to maintain the
methodology of system dynamics for the perfect investment in cyber resilience. [13]

Based on the system dynamics of developing the cyber resilience strategy, the author has analyzed several experts by interviewing them into behavior culture to this issue faced. Whereby, the model highlights importance of personnel training and technology for building the cyber resilience process rather than overlooking investment strategy. It might decrease the cyberattack threats as a strategy of the corporate whole. [13]

Overall, the author’s model used for the decision-making stage for IT organization to be aware of cyber resilience with a proper policy, systematic investment strategy, and IoT devices been structured in a good manner. [13]

Therefore, the author [14] has analyzed and identified existing CRF (Cyber Resilience Framework) as an instance of 25 research areas with 36 types of industries. Based on the survey it determined the strategic or operational consist of CRF as a decision influence by the methods used to does CRF research as a result.

It concluded the CRF research had identified certain gaps and similarities to proposes an opportunity for interdisciplinary research to label as a guideline for future research path in the field to analyze the intention of cyber resilience. [14]

Conversely, airports being advanced technology in their infrastructure that tracks the number of travelers every year has increased continuously. The author [15], identified challenges for aviation to integrate with IoT (Internet of Things) such as communication between smart devices with smart airports facilities developed by programmers. This smart layout enables a key to cyber resilience security and safety for users. The article emphasizes tracing malicious threats due to IoT and smart devices that are installed with mitigation actions to countermeasure the rate of cybersecurity in airports. [15]

By monitoring and securing smart airports may have high risks that involve cyber threats for aviation stakeholders, employees, airline operators, and regulators. The authors also collaborated on a cyber resilience model that defined the airport’s cybersecurity prevention structure that highly prioritizes the safety and security of passengers and airline operators. [15]

SG (smart grids) brought threats to computer-based software that enhanced the use of communication and information technologies. Which intend to lead cyber-attack in an organization. [16]. In figure 9, a model was designed by the author to address the vulnerabilities of the SG control system to monitor any cyber-attacks.

As result, the author analyzed the SG control system with identified various vulnerabilities that might occur event without security protection. Understanding the IT security strategies helps to maintain and monitor the system without hacker’s threat to be destroy and reduces its impact to control systems. [16]

Besides, the author has simulated and identified advanced communication technologies network known as VANET (Ad Hoc Network) that receive possible outcome to coordinate action for ITS (Information Transportation System). [17]. Based on the top 10 cyber threats surveyed, the author approached cyber resistance access on VANET/ITS model have identified the threats pattern of vulnerability and centralization management. [17]

Moreover, the proposed steps had delayed issues of vulnerabilities exploits from neutralization to prevent the model of forecasting and designed cyber system of VANET/ITS within the level of cyber resistance. [17]

References


Fig. 9. SG Control System Vulnerabilities [16]


