DIGITAL FORENSIC REPORT

By: Koo Wai Kit (TP081761)

Subject: Digital Forensic (062024-VIN)

Lecturer: Ts. Dr. Vinesha A/P Selvarajah

Table of Contents

1. Introduction

In today's digital age, the financial services industry remains one of the primary targets for cybercriminals due to the sensitive nature of the data it handles. Modern financial institutions have been exposed to various cyber threats that have devastating consequences. According to World Economic Forum (2024), around one-fifth of reported cyber incidents have impacted the global financial sector in the past two decades, causing financial firms to suffer $12 billion in direct losses.

TrustD Financial Services, a medium-sized firm that specializes in investment advice and portfolio management suffered a significant security breach and led to financial losses. The company detected unusual activities on 1 April 2024, accompanied by reports of unauthorized transactions and phishing emails by the clients. The initial investigations revealed that the company's email system was breached by cyber criminals, and the email system was used to send phishing emails to clients. The objective of the scam was to collect clients' personal and financial information, which were subsequently used to perform unauthorized transactions.

The case study highlighted the vulnerabilities present in the digital operations of financial institutions today. This report will focus on the cyber threat of phishing, which was central to the online scam that compromised TrustD Financial Services. According to Federal Trade Commission (n.d.), phishing is a kind of online scam that asks consumers to provide their personal identifiable information in an email which seems to originate from a legitimate source. This report aims to review forensic investigation approaches that are relevant to the cyber threat of phishing, propose a robust forensic investigation methodology to address such incidents, evaluate the forensic values of digital evidence, and provide a discussion of the legal and ethical implications related to this case.

2. Review of Relevant Forensic Investigation Approach

In this section, we will delve into three forensic investigation methodologies. These methodologies offer structured approaches for conducting comprehensive and effective digital forensic investigations, each adaptable to specific contexts and investigative needs.

2.1 General systematic approach

The first methodology Is derived from the Guide to Computer Forensics and Investigations, an e-book published by Cengage Learning. It offers a systematic approach to preparing for a digital forensics investigation (Nelson et al., 2019). This approach can guide the process of case preparation in order to tackle the problems systematically. The steps outlined in this approach include:

1. Conducting an initial assessment to determine the nature and scope of the case.
2. Developing an initial plan or strategy to guide the investigation.
3. Creating a detailed checklist outlining specific investigative tasks and timelines.
4. Identifying and preparing the necessary software tools and expertise required.
5. Seizing and creating forensic copies of relevant digital evidence.
6. Performing a risk assessment.
7. Mitigating the risk identified.
8. Testing the investigative approach to ensure its effectiveness and integrity.
9. Utilizing specialized tools and methods to examine and retrieve digital evidence.
10. Examining and interpreting recovered data to uncover relevant information.
11. Compiling a comprehensive report documenting findings and actions taken.
12. Evaluating and reviewing the investigation process for improvements and lessons learned.

Nelson et al. (2019) mentions that the effort and time allocated to each step vary based on the complexity of the investigation. For instance, simple investigations typically require a basic plan to ensure no steps are missed, while complex cases involving multiple computers will need detailed plans with regular updates.

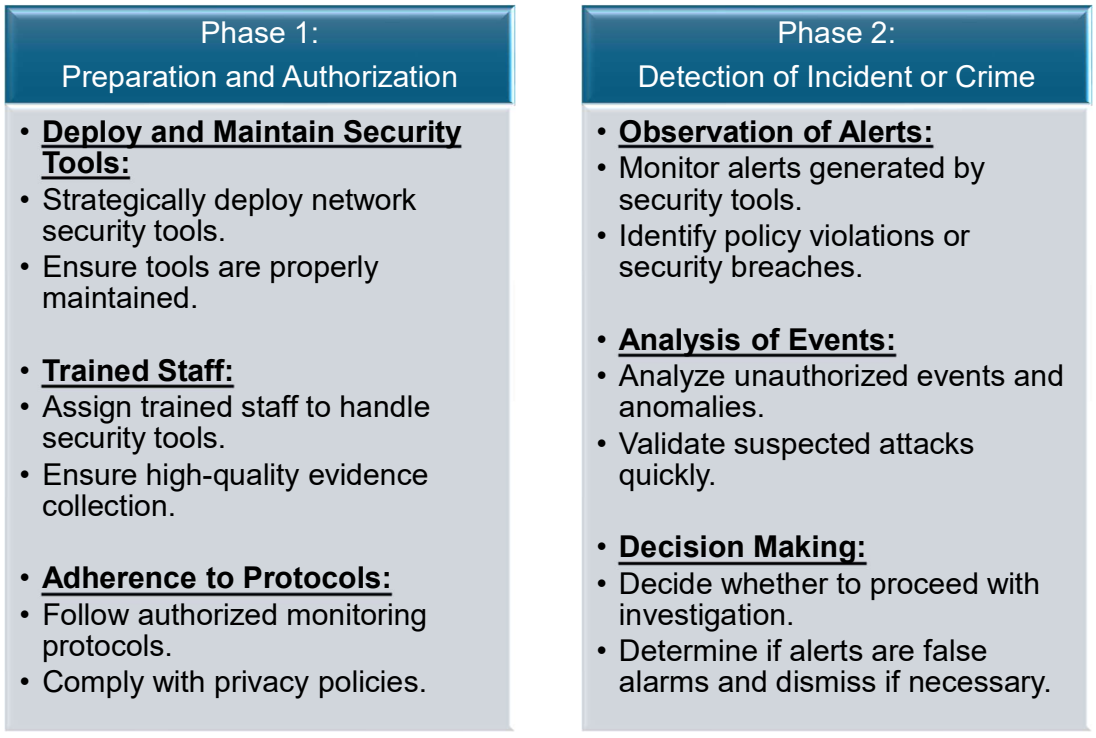
This methodology provides a comprehensive framework that covers various stages of digital forensic investigations. It provides several advantages, including ensuring thoroughness and completeness in the investigation process. Each step is clearly defined, which helps investigators to maintain focus and it can ensure all aspects of the investigation are addressed. The inclusion of risk assessment and mitigation efforts allow potential challenges to be identified early and proactive measures can be taken to minimize their impacts. The emphasis on creating forensic copies and testing the investigative approach can ensure the integrity of the evidence, which is crucial for admissibility in legal cases. A detailed report which is an important part of the

investigation will be compiled at the end, ensuring transparency and providing a clear documentation of findings, actions taken, and conclusions drawn.

However, there are some disadvantages associated with this methodology. Firstly, following all the steps thoroughly can be time-consuming and resource intensive, especially in complex cases involving multiple devices or a huge amount of data. The detailed steps and rigorous testing may be too complex for less experienced investigators or in cases where resources are limited. Although this methodology provides a structured approach, it may not be able to manage unexpected cases that require unique approaches. Moreover, its effectiveness is contingent upon the availability and proficiency of specialized forensic tools and expertise, which may not be readily available.

2.2 General framework for network forensics

Moving on to the next methodology. According to Pilli et al. (2010), this framework is designed specifically for digital investigations that are network based. This suggested methodology is broad, incorporating phases found in various digital forensic models while emphasizing those specifically tailored to network forensics. There are a total of nine phases, which are illustrated and summarized in Diagram 1 below.



Phase 3: Incident Response

- **Validate Information:**
- Validate incident information.
- Follow organizational policies and legal considerations.

- **Create Action Plan:**
- Develop a plan to contain future attacks.
- Create strategies for recovery from damage.

Phase 4: Collection of Network Traces

- **Secure Network Data:**
- Obtain network data from sensors.
- Ensure data integrity during collection.

- **Minimize Network Impact**:
- Collect data with minimal impact on the network.

- **Monitor for Future Attacks**:
- Continue monitoring for potential future attacks.

Phase 5: Protection and Preservation

- **Secure Storage:**
- Store original network traces and logs on backup devices.
- Use hashed verification to ensure data protection and integrity.

- **Chain of Custody:**
- Enforce strict chain of custody protocols.
- Prevent unauthorized access or tampering.

Phase 6: Examination

- **Integration of Data:**
- Integrate traces from security sensors into a single large dataset.
- Map and timeline the data to prevent loss.

- **Data Recovery and Classification:**
- Recover hidden data.
- Classify and cluster collected data to reduce volume.

- **Data Cleaning:**
- Remove redundant and unrelated information.
- Identify minimum representative attributes for analysis.

Phase 7: Analysis

- **Search and Analyze Evidence:**
- Methodically search collected evidence.
- Analyze evidence to extract and correlate crime indicators.

- **Techniques Used:**
- Employ statistical and data mining approaches.

- **Reconstruct and Replay Attacks:**
- Understand attacker methods.
- Validate suspicious activities.

Phase 8: Investigation and Attribution

- **Utilize Evidence Traces:**
- Identify details of the incident.
- Aid in source traceback and attack reconstruction.

- **Establish Attacker's Identity:**
- Overcome challenges like IP spoofing and stepping stone attacks.
-
- **Techniques Used:**
- Implement IP traceback schemes.
- Use similarity-based approaches to packet statistics.

- **Varying Investigative Approaches:**
- Adapt investigation methods based on the attack type.

Phase 9: Presentation and Review

- **Presentation to Stakeholders:**
- Present observations to management and legal personnel.
- Use understandable language and clear explanations.

- **Documentation and Visualization:**
- Provide systematic documentation.
- Include visualizations to illustrate findings.

- **Interpretation of Data:**
- Interpret statistical data to support conclusions.

- **Incident Review and Recommendations:**
- Thoroughly review the incident.
- Recommend solutions based on findings.

- **Documentation for Future Use:**
- Document all results.
- Guide future investigations and improve security products.

Diagram 1: Phases in the network forensics framework

There are many benefits that this methodology provides. Firstly, this approach covers all essential aspects of a network forensic investigation, ensuring that no critical step is overlooked. There is also an emphasis on preparation and authorization which ensures that investigators are well-equipped and compliant with legal and organizational policies. The data integrity and chain of custody is emphasized, ensuring that evidence remains untampered and reliable. This is essential for maintaining the credibility of the investigation. In addition, the inclusion of statistical and data mining steps in the analysis phase can enhance the ability to identify and understand complex attack strategies. This methodology is also flexible in dealing with different types of attacks like the IP spoofing attack, which is crucial for addressing the evolving nature of cyber-attacks.

This methodology also comes with some disadvantages. First of all, the comprehensive framework can be resource-intensive and time-consuming. Smaller organizations may not be able to implement all phases effectively. Furthermore, the detailed procedures in each phase can make the framework too complex to be executed, which may lead to challenges in coordination and consistency across different phases. Besides, the dynamic nature of network traffic data is constantly evolving, and it poses a challenge for the collection and analysis phases. Data integrity and management can be difficult, potentially impacting the effectiveness of the investigation. The largest disadvantage would be that this framework may be outdated given the rapid advancements of technology, since it was developed in 2010.

2.3 Cloud forensics process model

Malik et al. (2024) states that cloud digital forensics is a specialized field dedicated to investigating cybercrimes in cloud environments, addressing multi-jurisdictional challenges, and ensuring proper evidence preservation protocols. Therefore, an investigative approach with four key stages is proposed, where each stage is essential for thoroughly understanding a digital incident. The stages are summarized in Diagram 2.

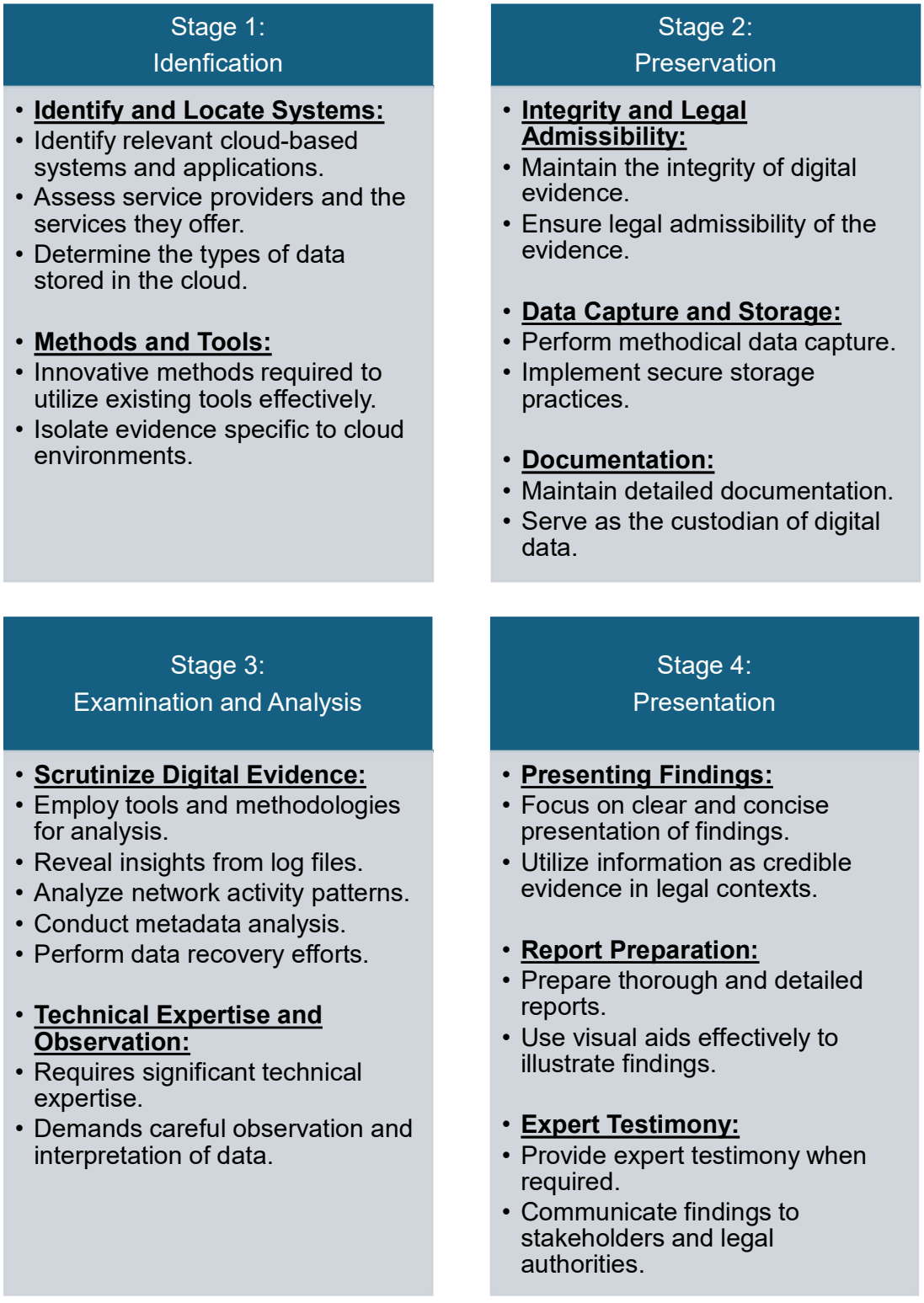


Diagram 2: Stages of cloud forensics process model

The methodology offers some distinct advantages. Firstly, it provides a comprehensive approach that covers all crucial stages from initial identification of cloud-based

systems to the presentation of findings in legal contexts. This ensures that investigations are conducted systematically, enhancing the reliability and credibility of forensic findings. Moreover, the emphasis on evidence integrity during the Preservation stage is pivotal. It safeguards digital evidence against tampering, thereby bolstering its admissibility in legal proceedings. Besides, the methodology recognizes the complexities of cloud environments, and it proposes innovative methods to effectively use existing forensic tools and isolate cloud-specific evidence.

Despite the strengths, the methodology also has some shortcomings. The first disadvantage is the methodology is reliant on digital forensic tools and technologies. This will introduces a dependency on their availability and effectiveness. In addition, continuous adaptation and investment in forensic capabilities are required to ensure the methodology remains effective over time. This is due to the rapidly changing nature of cloud environments. Lastly, adhering to diverse legal frameworks and compliance requirements adds a layer of complexity. Ensuring that the procedures are legal and align with regulatory requirements will require meticulous attention to detail throughout the investigation.

2.4 Comparison of the approaches

The Table 1 below provides a comparison of the strengths and weaknesses of the methodologies discussed above. Each methodology has its unique strengths and weaknesses, tailored to different aspects of digital forensics, including general investigations, network-based investigations, and cloud-based environments.

Table 1: Strengths and weaknesses of each methodology

Approach	Strengths	Weaknesses
General Systematic Approach (Nelson et al., 2019)	a) Comprehensive and thorough framework. b) Clearly defined steps ensuring focus and completeness. c) Includes risk assessment and mitigation.	a) Time-consuming and resource-intensive, especially for complex cases. b) May be too complex for less experienced investigators.

	d) Emphasizes evidence integrity and detailed reporting.	c) Rigid structure, may struggle with unexpected cases. d) Requires specialized tools and expertise.
General Framework for Network Forensics (Pilli et al., 2010)	a) Covers all essential aspects of network forensic investigation. b) Emphasizes preparation, authorization, and data integrity. c) Includes statistical and data mining steps. d) Flexible in dealing with different types of attacks.	a) Resource-intensive and time-consuming. b) Detailed procedures can complicate execution and coordination. c) Dynamic nature of network traffic data poses challenges. d) May be outdated due to rapid technological advancements.
Cloud Forensics Process Model (Malik et al., 2024)	a) Comprehensive approach covering all crucial stages. b) Emphasis on evidence integrity. c) Recognizes complexities of cloud environments and proposes innovative methods. d) Enhances reliability and credibility of forensic findings.	a) Dependent on availability and effectiveness of forensic tools and technologies. b) Requires continuous adaptation and investment. c) Complexity due to diverse legal frameworks and compliance requirements.

3. Proposed Forensic Investigation Methodology

This section outlines a tailored forensic investigation methodology aimed at comprehensively examining the cyber incident reported at TrustD Financial Services. This methodology will consist of five phases: Identification, Collection and Preservation, Examination and Analysis, Reconstruction, and Reporting. Each phase

is designed to build upon the previous one, creating a comprehensive and detailed investigation process. This methodology aims to uncover the full extent of the breach and also provides actionable insights to prevent future incidents. The chronological order of the phases in the methodology is shown in Diagram 3.

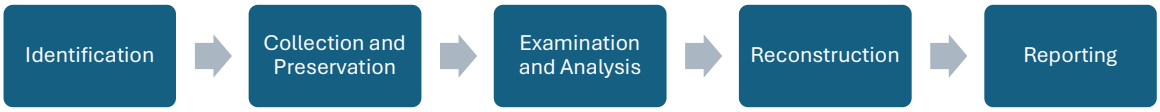


Diagram 3: Proposed Forensic Investigation Methodology

3.1 Identification

First phase is identification, in which the forensic team must determine where relevant evidence might be found (Exterro, n.d.). In many ways, the identification phase serves as a preliminary step to the core tasks of a digital forensic investigation. According to Exterro (n.d.), the forensic team have to determine the primary evidence-holders, the devices that could contain evidence related to the investigation, and the evidence types found on the devices under examination. In a data breach investigation, the primary evidence-holders may be the individuals who clicked on a phishing email. Moreover, there are several types of devices that could contain evidence, which include computers and servers. The device type will also determine the type of evidence that it could contain. Once devices are identified, the forensic team will seize and isolate the devices to prevent them from being tampered with.

For TrustD Financial Services, the identification phase involves identifying where the relevant evidence of the cyber incident is located. The forensic team will start by identifying primary evidence-holders, such as employees and clients who reported unauthorized transactions and received phishing emails. Next, they will focus on key devices that might contain critical evidence, including the company's email servers which were breached, employee workstations that may have been targeted, and client devices that interacted with the phishing emails. Additionally, network devices like routers and firewalls will be examined for signs of intrusion and data exfiltration. By isolating these devices to prevent tampering, the forensic team can ensure the integrity of the evidence for subsequent phases of the investigation.

3.2 Collection and Preservation

Once evidence has been identified and the devices have been seized, the next phase will be collection and preservation. The forensic team will use specialized methods to extract any potentially relevant data for the investigation and securely stores it (ERMProtect, n.d.). There are many methods of collection, such as dead-box collection, live forensics, on-network collection, and off-network collection (Exterro, n.d.). In addition, the digital evidence will need to be collected and maintained in a manner that preserves its integrity, since the evidence may need to be presented in court (Exterro, n.d.). The forensic team must isolate and safeguard digital evidence in its original state, ensuring it remains unaltered for future analysis. Exterro (n.d.) also mentions that the evidence can be preserved by performing imaging to create forensic copies. This can prevent alteration or contamination to the original data. The investigators will also need to maintain the chain of custody, which refers to the process of managing physical or digital evidence during an investigation. Chain of custody is important to ensure the integrity and reliability of evidence.

In the TrustD Financial Services case, the collection and preservation phase will involve using various methods to ensure all relevant digital evidence is gathered without any alteration. Dead-box collection will be used to create forensic images of compromised employee workstations and client devices, maintaining their state at the time of the breach. Live forensics will capture volatile data from the company's email servers and network devices before the information is lost, such as active connections and running processes. On-network and off-network collection techniques will gather logs and data from connected systems while minimizing disruption to operations. All evidence will be documented comprehensively and the chain of custody will be maintained to preserve the integrity and reliability of the evidence, which may be needed in court.

3.3 Examination and Analysis

Subsequently, the investigation will proceed to the examination phase and analysis phase. There are three major steps in this stage, which are filtering, class characteristics and evaluation of source, and data recovery (Selvarajah, 2024). Filtering allows irrelevant or confidential data to be excluded, and the focus will be on the most probable user-created data. Redundant files would also be managed properly.

Class characteristics and evaluation of source allows the forensic team to classify evidence based on its characteristics and evaluate where the evidence originates from. Data recovery can be performed to recover deleted files to uncover more evidence. Data recovery techniques will be employed to retrieve these deleted files, potentially uncovering critical evidence.

In the context of the TrustD Financial Services case, this phase will be crucial for uncovering insights into the online scam. The initial data collection would likely include vast amounts of information from various sources. Filtering will help the forensic team eliminate irrelevant system data and focus on potential indicators of the breach, such as phishing emails and unauthorized transactions. Class characteristics and evaluation of source would involve examining the phishing emails to understand their structure, content, and the methods used by attackers to deceive clients. It would also include evaluating transaction logs to identify unauthorized activities and tracing these activities back to their origin. Data recovery can be performed since the attackers might have deleted logs, emails, or other traces of their activities. The data recovered can potentially reveal further evidence of how the breach occurred and who was involved.

3.4 Reconstruction

Subsequently, the reconstruction phase is needed to recreate the sequence of events leading up to and during the cyber incident (Selvarajah, 2024). There are three fundamental types of reconstruction, which are functional analysis, relational analysis, and temporal analysis. Functional analysis involves understanding how different components of the system interacted and functioned during the cyber incident. Additionally, the relational analysis allows the forensic team to understand how different components and actors are interlinked. Furthermore, temporal analysis involves creating a detailed timeline of the events related to the cyber incident.

For TrustD Financial Services, functional analysis would involve the examination of how the compromised email system interacted with phishing emails and facilitated unauthorized access to client information. This will help in understanding the technical aspects of the breach, such as how malware may have been deployed and data exfiltrated. Relational analysis would involve mapping the connections between the compromised email accounts, the clients who received phishing emails, and the

subsequent unauthorized transactions. Moreover, temporal analysis would involve constructing a timeline that chronologically orders the activities of the cyber criminals, from the initial phishing emails detected on April 1, 2024, to the unauthorized transactions reported by clients. Thus, this phase helps in understanding the attack's progression, the methods used, and the timeline of events. This stage provides a deeper understanding of how the incident occurred, which will help in identifying vulnerabilities and improving defences.

3.5 Reporting

After concluding the investigation and documenting the critical evidence, the next step involves presenting the findings to the authorities responsible for making decisions based on the investigation's outcome (Exterro, n.d.). In addition, the reporting phase allows all findings and conclusions to be integrated into a final report (Selvarajah, 2024). This report can also provide actionable recommendations. Several key information that can be obtained from the report include the evidence summary, examination summary, analysis, and conclusion. The forensic team would also need to interpret the digital evidence by providing opinions that has a statistical basis. For each conclusion that the investigator made, a level of certainty can be given. This phase is crucial to communicate the investigation’s outcomes to stakeholders, ensuring that they understand the impacts of the incident.

For TrustD Financial Services, in the reporting phase, the forensic team will consolidate all findings and conclusions derived from the forensic investigation into a comprehensive report. The final report would cover all aspects of the investigation, which includes details like how the breach occurred, the methods used by the attackers, and the impact on client accounts. It will also include an analysis of how the cyber incident unfolded. Recommendations on how to enhance the email system security and the measures to avoid future incidents will be included in the report, which helps the firm to make informed decisions on improving their security posture. Each conclusion drawn by the forensic team will be supported by statistical analysis where applicable, providing a level of certainty to stakeholders regarding the findings. This phase ensures that all stakeholders, including management and information security teams, are well-informed about the incident's impact and equipped with insights to prevent similar incidents in the future.

4. Related Legal and Ethical Issues

4.1 Ethical Considerations

According to Infosec (n.d.), code of ethics is divided into two sections: actions that practitioners will perform at all times and actions they will never engage in. This code articulates the values and principles that direct the organization's mission and the conduct of its practitioners.

Phishing attacks, such as the one at TrustD Financial Services, raise several important ethical considerations. Ethical issues may arise when forensic investigators handle a phishing incident, particularly concerning their adherence to the code of ethics for computer forensics.

4.1.1 Integrity and Objectivity

The first issue lies within the integrity and objectivity of forensic investigators throughout the investigation process. According to Jaju (2023), there is a possibility of bias and discrimination when digital evidence is collected and analysed. When investigating the phishing attack, the forensic investigators need to avoid biases and ensure that their findings are based on factual evidence rather than assumptions.

For instance, the investigators should not immediately assume that certain employees are involved in the phishing attack without solid evidence. Instead, they should objectively analyse all available data, such as email logs and server access records, to identify the true perpetrators based on factual evidence rather than assumptions.

4.1.2 Confidentiality

The investigators have a duty to handle all information related to the phishing incident with strict confidentiality. It is mentioned in Infosec that a certified computer examiner will never reveal any confidential information (n.d.). The investigations need to be done in a manner that respects the individuals' rights to privacy (Jaju, 2023). It is necessary for the forensic team to adhere to privacy laws and handle the clients' sensitive data with care to prevent further exposure.

For instance, when the investigators are handling sensitive client information obtained from compromised emails, they should store the extracted data in encrypted files and limit access to authorized personnel only. Additionally, they should avoid discussing

specific client details with unauthorized individuals to protect client privacy and comply with legal obligations under privacy laws.

4.1.3 Transparency

The investigators need to be transparent about the investigation. It is important to advocate for transparency and accountability in digital forensics procedures (Jaju, 2023). They should clearly communicate the investigative process to the stakeholders, including the affected clients and regulatory bodies. A detailed incident report that contains any relevant information about the incident should be created.

In the TrustD Financial Services case, investigators should provide regular updates to the firm's management and affected clients about the progress of the investigation. Moreover, they should hold regular meetings to discuss findings and share investigative methodologies used to uncover the phishing attack's origins and methods. The investigators would need to come up with a comprehensive incident report detailing how the phishing emails were crafted to deceive clients and how the unauthorized transactions were executed, ensuring stakeholders understand the full scope and impact of the incident.

4.1.4 Accountability

The investigators need to have a strong sense of accountability since they will be held accountable for their findings and recommendations. Also, they must be prepared to justify their conclusions based on solid evidence. According to Infosec (n.d.), the forensic investigators must always conduct a comprehensive examinations of all evidence within the investigation's scope, as well as never withhold any pertinent evidence.

During the investigation of the phishing attack, the investigators should document their investigative process meticulously to ensure accountability. They should maintain detailed logs of all actions taken. If there are any discrepancies, they must be prepared to explain and justify their actions or conclusions based on the evidence gathered.

4.1.5 Competence and Training

Lastly, the investigators must possess the necessary skills and training to conduct thorough and accurate forensic examinations related to phishing incidents. They must participate in ongoing training and education on ethical practices to stay informed

about current privacy laws and regulations, recognize and mitigate bias, and maintain accuracy and reliability in data analysis (Jaju, 2023).

In response to the phishing incident, the investigators should demonstrate their competence by applying advanced techniques in digital forensic analysis. For instance, they should use data recovery techniques to retrieve deleted phishing emails from compromised email server. In addition, attending specialized training sessions on phishing detection and prevention would be beneficial for the investigators to enhance their skills in identifying similar cyber threats in the future.

4.2 Legal Issues

Phishing attacks pose significant legal challenges for organizations like TrustD Financial Services. This section delves into the legal implications of phishing incidents within the context of Malaysia and Singapore. It is crucial to understand these legal considerations as they are essential for ensuring compliance and mitigating risks in the aftermath of cyber threats.

4.2.1 Malaysia

According to Pillai and Yong (2019), there are no specific laws addressing phishing as an offense in Malaysia. However, statutory provisions like section 416 of the Malaysian Penal Code can be applied to tackle such offenses. This section defines "cheating by personation" as deceiving others by pretending to be someone else or misrepresenting identities. This is punishable by up to seven years in prison and/or a fine. Despite this legal framework, there have been no reported cases specifically related to phishing to date.

In addition, Chia (2019) states that according to Section 417, this offence can result in imprisonment for up to five years, a fine, or both upon conviction, regardless of whether the person being impersonated is real or fictional.

However, due to the nature of phishing attacks, other laws that do not explicitly mention phishing may also be relevant and applicable. This includes the Computer Crimes Act 1997, Communications and Multimedia Act 1998, Electronic Commerce Act 2006, and Personal Data Protection Act 2010 (NACSA, n.d.). These laws could all have implications depending on the specific circumstances of the attack and the data involved.

A. Computer Crimes Act 1997
    - For offences related to computer abuse, including unauthorized access, intent to commit offenses, and modification of computer data.
    - Relevant to phishing as it addresses unauthorized access to computer systems and data, which can occur when cybercriminals breach systems to deploy phishing campaigns.

B. Electronic Commerce Act 2006
    - Establishes legal recognition for electronic messages in commercial transactions and facilitates the use of electronic means to fulfil legal requirements.
    - Relevant to phishing as it sets guidelines for electronic communications and transactions, which can be exploited by cybercriminals to deceive individuals into providing sensitive information through fraudulent emails.

C. Personal Data Protection Act 2010
    - Regulates the processing of personal data in commercial transactions, imposing obligations on organizations that collect, process, and store such data to safeguard individuals' personal information.
    - Relevant to phishing because phishing often involves the unauthorized collection and misuse of personal data.

4.2.2 Singapore

Similarly, phishing incidents are not explicitly defined as offenses under any dedicated legislation in Singapore (Lim et al., 2023).

However, several provisions can be invoked to address such cybercrimes. Particularly, Section 3 of the Computer Misuse and Cybersecurity Act (CMA) criminalizes causing a computer to perform any function for the purpose of securing unauthorized access to data held in any computer.

Depending on the circumstances, phishing activities where unauthorized access to sensitive information is sought could fall under this provision. Offenders convicted under this section face penalties including fines up to $5,000, imprisonment for up to two years, or both for a first offense.

In addition, offenders involved in phishing scams may also face charges under laws targeting the possession or attempted use of proceeds derived from criminal activities.

Lim et al. (2023) provides a case example, where the accused facilitated a phishing scam by operating a phishing website that deceived victims into divulging sensitive information. The accused was then charged of an offence under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 as the accused tried to deposit two checks that were the criminal gains from the phishing scheme.

Additionally, Singapore has recently passed a new Act called the Online Criminal Harms Act (OCHA) on July 5, 2023, that allows the government to get rid of online illegal content (Sun, 2024). It aims to address the evolving nature of online criminal harms, with a focus on scams and malicious cyber activities. Under OCHA, the government has the authority to issue directives and orders to restrict and limit the exposure of Singaporean users to criminal activities on online platforms. Sun (2024) mentions that the threshold for intervention is even lower for scams and malicious cyber activities, as mere suspicion that certain online actions are in the middle of preparation for such offenses will be sufficient to allow directives to be issued.

5. Conclusion

In summary, this report has provided a comprehensive review of three relevant forensic investigation approaches. Subsequently, a tailored methodology has been developed and proposed to effectively address the specific requirements of investigating the TrustD Financial Services incident. Several legal and ethical issues have been discussed, as it is crucial to adhere to the legal and ethical standards throughout the investigation.

By employing appropriate forensic techniques and ensuring that the legal and ethical guidelines are adhered to, the forensic investigators can effectively address phishing incidents, minimize the impact, and help organizations recover.

6. References

Chia, S.Y. (2018). Basics of cyber security law in Malaysia. Chia, Lee & Associates. https://chialee.com.my/basics-of-cyber-security-law-in-malaysia/

ERMProtect (n.d.). What Are the 5 Stages of a Digital Forensics Investigation?. https://ermprotect.com/blog/what-are-the-5-stages-of-a-digital-forensics-investigation/

Exterro (n.d.) The Forensic Investigation Process. https://www.exterro.com/basics-of-digital-forensics/chapter-2-the-forensic-investigation-process

Federal Trade Commission (n.d.). Phishing Scams and How to Spot Them. https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams

Infosec (n.d.). Computer Forensics Code of Ethics. https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-code-ethics/#:~:text=The%20code%20states%2C%20in%20part,the%20scope%20of%20an%20investigation.

Jaju, A. (2023). Ethical digital forensics – Balancing investigation procedures with privacy concerns. Enterprise IT World. https://www.enterpriseitworld.com/ethical-digital-forensics-balancing-investigation-procedures-with-privacy-concerns/

Lim, C. K., Alfred, D. N., & Pichlmaier, A. (2023). Cybersecurity Laws and Regulations Singapore 2024. International Comparative Legal Guides. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/singapore

Malik, A. W., Bhatti, D. S., Park, T.-J., Ishtiaq, H. U., Ryou, J.-C., & Kim, K.-I. (2024). Cloud digital forensics: Beyond tools, techniques, and challenges. National Center for Biotechnology Information. https://doi.org/10.3390%2Fs24020433

National Cyber Security Agency (NACSA) (n.d.). Malaysian cyber laws. https://www.nacsa.gov.my/legal.php

Nelson, B., Phillips, A., Steuart, C. (2019). Guide to computer forensics and

investigations (6th ed.). Cengage Learning. https://cenexp.com/biblioteca/librerias/FOR/Bforense/LF20.pdf

Pillai, D., & Yong, S. H. (2019). *The International Comparative Legal Guide to: Cybersecurity 2019, 2nd Edition, Chapter 21 Malaysia*. https://www.rajahtannasia.com/media/3126/cyb19_chapter-21-malaysia.pdf

Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). A generic framework for network forensics. https://www.ijcaonline.org/volume1/number11/pxc387408.pdf

Selvarajah, V. A. (2024). Forensic Investigation Methodology, Tools & Techniques. [PowerPoint slides]. Data Forensics. Asia Pacific University of Technology & Innovation (APU).

Sun, D. (2024). Online Criminal Harms Act to kick in from Feb 1, with special provisions for scams. The Straits Times. https://www.straitstimes.com/singapore/online-criminal-harms-act-to-kick-in-from-feb-1-with-special-provisions-for-scams#:~:text=SINGAPORE%20%2D%20The%20Online%20Criminal%20Harms,scams%20and%20malicious%20cyber%20activities.

World Economic Forum (2024). Global financial stability is at risk due to cyber threats, the IMF warns. Here's what needs to happen. https://www.weforum.org/agenda/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/#:~:text=In%20the%20past%20two%20decades,to%20an%20estimated%20%242.5%20billion.