Print ISSN: 1738-3110 / Online ISSN 2093-7717
JDS website: http://www.jds.or.kr/
http://dx.doi.org/10.15722/jds.20.07.202207.107

A Blocking Distribution Channels to Prevent Illegal Leakage in Supply Chain using Digital Forensic

Jin-Hee HWANG[1]

Received: February 24, 2022. Revised: April 13, 2022. Accepted: July 05, 2022.

Abstract

Purpose: The scope of forensic investigations serves to identify malicious activities, including leakage of crucial corporate information. The investigations also identify security lapses in available networks. The purpose of the present study is to explore how to block distribution channels to protect illegal leakage in supply chain through digital forensic method. **Research design, data and methodology:** The present study conducted the qualitative textual analysis and its data collection process entails five steps: identifying and collecting data, determining coding categories, coding the content, checking validity and reliability, and analyzing and presenting the results. This methodology is a significant research method due to its high quality of previous resources. **Results:** Applying previous literature analysis to the results of this study, the author figured out that there are four solutions as an evidences to block distribution channels, preventing illegal leakage regarding company information. The following subtitles show clear solutions: (1) Communicate with Stakeholders, (2) Preventing and addressing illegal leakage, (3) Victims of Data Breach, (4) Focusing Solely on Technical Teams. **Conclusion: T**here are difficult scenarios that continue to introduce difficult questions surrounding engagement with digital evidence. Consequently, it is important to enhance data handling to provide answers for organizations that suffer due to illegal leakages of sensitive information.

Keywords: Digital Forensic, Supply Chain Management, Distribution Channel, Qualitative Approach

JEL Classification Codes : C81, G14, K13

1. Introduction

In today's computer technology is a major part of daily human life. Computer technology is growing rapidly, similar to computer crimes such as unauthorized intrusion, intellectual theft, identity theft, and illegal leakage. In the corporate world, businesses have adopted computer technology to enhance services provided to consumers. Computer technology helps the corporate world streamline services and achieve a competitive advantage over businesses that do not have the latest computer technologies. On the other hand, digital forensic deals in preserving, extracting, and documentation of computer evidence. It involves retrieving evidence from digital sources such as computers, servers, networks, and mobile phones. In a computer forensic investigation, authorities investigate information leaked from computers and other storage devices, distributing important data to the third party. The authorities follow standard procedures to ascertain the nature of the compromised devices and whether there is unauthorized access or leaked information. The forensic investigators work in teams investigating these incidents and

1 First and corresponding Author, Ph.D. student, Forensics, Sungkyunkwan University E-mail: dndbdndb89@naver.com

assessing the situation through forensic analysis using several methodologies. These methods include Static and Dynamic tools such as ProDiscover and Encase. To ensure the security of computer systems in the supply chain, blocking distribution channels, forensic investigators familiarize themselves with various laws and regulations (Esposito, Castiglione, Martini, & Choo, 2016).

Nelson, Phillips, and Steuart (2014) argued that there are two categories under Computer Forensics Investigation, Public Investigations, and Private or Corporate Investigations. The government is responsible for conducting public investigations which should control distribution routes for illegal leakage in supply chain, while private computer forensic teams are responsible for conducting private investigations. According to the Association of Chief Police Officers (ACPO) laws, a corporate forensic investigation may be conducted. These laws have four principles guiding investigations in computer-based electronic evidence. These principles should be followed to the letter while conducting investigations to prevent illegal leakage and block distribution channels.

The first law suggests that data in computers and other storage devices should not be changed as evidence may be presented in court. The second law suggests that an officer should be competent enough to handle original data in computers and other storage devices to present evidence concerning their actions in court. The third states that audit trials and other electronic computer-focused clue might be produced and preserved. Furthermore, there should be a third party responsible for examining such processes and getting similar results. The fourth suggests that investigators in charge should take overall responsibility for accounting and ensuring that all laws are respected (Skalak, Golden, Clayton, & Pill, 2011).

The scope of forensic investigations serves to identify malicious activities, including leakage of crucial corporate information. The investigations also identify security lapses in available networks. They also assess the impact of the compromised network systems. The investigations assess legal processes where necessary and provide remedial actions to secure the systems. There are also some legal challenges such as determining the relevance of law enforcement assistance, obtaining written documentation to conduct forensic investigations, identifying potential issues raised in improper investigations, and promoting client confidentiality and privacy.

2. Literature Review

Several forensic investigations have given their views surrounding issues in illegal leakage of corporate information in supply chain using digital forensics. These experts include Kruse and Heiser (2001) suggest that the role of computer investigations includes identifying evidence, preserving, extracting, documenting, and validating the evidence. After all, the evidence is analyzed using several theoretical frameworks to identify root causes of malfunctions such as leakages. Consequently, the investigators provide recommendations and solutions to apply and address the existing challenge. The investigators are solely responsible for addressing the challenges in computer-based forensics.

Adams, Hobbs, and Mann (2013) argued that there are a few standard policies in the computer forensics field across different courts and industries. The author further argues that computer forensic models focus on specific areas such as law enforcement and block distribution channels. Furthermore, there is no single universally accepted digital forensic investigation model (Adams et al., 2012). Nonetheless, this research argues that existing digital forensic model frameworks must be flexible enough to support any potential incident and incorporate the latest technologies in supply chain.

On the other hand, the previous study (Wang, Wang, Sun, Cui, Rahnamayan, & Zeng, 2017) created a basic digital forensic investigation model that is easy to use even for non-technical individuals. The Four-Step Forensic Process (FSFP) framework is among the most flexible processes that corporate organizations can use to prevent illegal leakage and assess damages caused by unexpected situations (Wang et al., 2017). The FSSP model incorporates four steps as follows, collection, examination, analysis, and reporting. Park, Kim, Park, Na, and Chang (2018) suggested that companies are in the procedure to transit for smart workplace circumstances. These organizations apply computing technology to access information assets in the organization through cloud computing technology. They share information without restrictions using mobile terminals and enhance effective work in mobile environments (Park et al., 2018). Therefore, there are increased risks in such environments, such as leakages incorporating information assets through mobile networks with high risks of loss and theft. Consequently, these risks can be addressed preemptively through a digital forensic model in preemptive prevention.

Quick and Choo (2016) discussed a framework for digital forensic investigation of large data. The authors suggest that technology development has seen the birth of an era of big data and data explosion. Therefore, there are increasing amounts of data in cybercrime investigations. The big presents several challenges in finding clues and evidence for investigation. On the other hand, the onset of big data presents new directions and blueprints for digital forensic investigations.

The past research argued the growing preference for automation and digital developments. In supply chain, the authors suggest an exponential rise in the application of computer technology. With the rise in technology comes risks of interaction. Such risks include cyber-attacks which have become more sophisticated (Okereafor & Djehaiche, 2020). Thus it has become difficult to trace cybersecurity breaches. It is important to find accurate mechanisms for analysis in digital forensics.

Kebande and Venter (2018) examined a new design for Digital Forensic Readiness (DFR) in cloud computing. Kebande and Ventor's approach involves a model with functionality operating as a forensic agent-based solution. The model performs forensic logging for digital Forensic Readiness purposes. This model enables organizations to perform forensic assessments in the cloud while protecting operations and functionalities of cloud infrastructure. Consequently, the model enables forensic analysts to maximize the use of digital evidence and minimize design costs. Krishnan and Shashidhar (2021) assessed the interdependence of digital forensics and eDiscovery. The two fields are overly dependent but overlap to enhance a symbiotic relationship. The authors suggest that using the two fields had grown tremendously with the decreasing cloud storage costs, rising internet speeds, and portable storage media (Krishnan & Shashidhar, 2021). The authors discuss the relationship between Digital Forensics and eDiscovery to highlight the skills required and the electronic resources needed in digital evidence management.

Bollam and Malsoru (2011) discussed the disclosure of private information to unauthorized third parties. They argue that disclosure internally or externally is referred to as data leakage, which may occur deliberately or mistakenly. According to the authors, corporates experience huge losses financially and non-financially. Notably, recurrent data leakages create huge concerns for organizations. The authors characterize data leakage in terms of data states, deployment points, and leakage detection approaches. The prior study argued that the number of cyber incidents is on the rise. These attacks have tremendous financial and reputational challenges for the corporate world. Companies are often responsible for these cyber-attacks since they leave themselves vulnerable to poor cybersecurity practices. As such, the author argues that organizations must do all it takes to protect themselves and their business from data leakages (Ribeiro, 2019). They should implement corporate changes to improve overall security behavior. The author applies the example of the Equifax data breach that cost the organization millions of clients across the globe.

Poyraz, Canan, McShane, Pinto, and Cotter (2020) suggested several factors influencing the monetary impact of data leakages in supply chain. The author introduces a model that defines the approximate costs of a mega data breach. According to the study (Poyrza et al., 2020), there is a significant relationship between total data breach cost and revenue. These authors argued that categorizing personal information as sensitive explains the costs of these data leakages and finally suggested that independent variables demonstrate multilevel factorial behavior. The prior research discussed increasing cyber-related issues since the beginning of the covid-19 pandemic. In this pandemic, most workers have found themselves forced to work at home. Through the internet, these individuals connect in work, school, shopping, and entertainment settings. Thus, this paper examines the rise of cybercrimes and technology progress (Monteith, Bauer, Alda, Geddes, Whybrow, & Glenn, 2021). The authors further discuss the evolving cybercrimes and individuals' vulnerabilities to cybercrime. The paper looks at the effects of cybercrime on patients with mental illnesses. It concludes that the most important step in preventing cyber-attacks for this vulnerable group is increasing patient awareness of cybercrime.

According to the study (Vavilis, Petković, & Zannone, 2016), stringent measures exist against data leakages in industrial control systems. These systems engage in high safety assurance to highlight faults and monitor them to enhance proper security protocols. Using anomaly detection, we can detect simple unusual behavior such as system leakages. Additionally, the journal offers an alternative to anomaly detection, which is applying specification-based intrusion detection. On the other hand, Cheng, Liu, and Yao (2017) suggested that data leakages pose serious threats, including reputational damage and revenue loss. The authors suggest that as data volumes continue to rise, data breaches have been occurring more frequently than ever (Cheng et al., 2017). The topic of data breaches remains an active research issue. Inherently, organizations have developed state-of-the-art prevention strategies and detention techniques that address the existing challenges and develop promising solutions.

Guevara, Santos, and Lopez (2017) addressed the issue of data breaches in cloud computing. The authors suggest that there are efforts in supply chain geared towards enhancing the safety of cloud computing. The authors perform several processes when reports of data leakages come to their attention (Guevara, et al., 2017). They adopt the s-max algorithm as it provides a significant improvement to assess the guilty parties in line with the > 0.4 of the reduced data. According to the study (Alneyadi, Sithirasenan, & Muthukkumarasamy, 2016), privacy concerns have arisen from the onset of the social web. Data leakages affect the Privacy of individuals and corporate organizations. The authors acknowledge existing tools that help in preventing data loss. However, they suggest that these tools need a prior step involving identifying sensitive data. They use a prototype known as Named Entity

Recognition (NER) to handle data losses.

The prior research suggested a new context-based model (Coban) that handles accidental and intentional data leakages for organizations. In data leakage prevention, the authors identify specific key terms and phrases by applying statistical methods (Katz, Elovici, & Shapira, 2014). Their model comprises two ashes, the training phase and the detection phase. Through extensive research (Katz et al., 2014), model proves superior to other data leakage models. The previous study insisted a security evaluation framework that has an objective evaluation measurement. This research also argues that organizations face risks both from the inside and outside. Furthermore, there are limits to external security risks and improper measures for dealing with these security risks (Kim, Lee, & Chang, 2020).

The research proposes a method for assessing the levels and securing the objectivity of preferred models. The method suggested allows effectiveness and objectivity of assessing security preparedness. The alternative workplace strategy, the "Bring Your Own Device," is a popular workplace strategy that allows employees to use personal devices to conduct business. On the contrary, the strategy is prone to risks in cybersecurity (Ali & Kaur, 2020).

Thus, there are measures to mitigate these cyber risks, including detection and protection from advanced attack levels. Another measure for mitigating risk is conducting forensic investigations to find digital evidence and find sources of attack. Yuan and Yu (2015) argued that data sharing enhances and augments the digital economy. In the same way, the paper designs an effective data supervision technique to enhance data sharing. The authors conclude that data leaking in corporate entities is influenced by relative technical and data supervision processes (Yuan & Yu, 2015). These authors suggest a model that makes up for the shortcomings of low technology in companies. This model helps control corporate choices of data leakage behavior. It also enhances the stability of data sharing and severe data supervision.

Anomaly based-solutions can assess unknown data breaches but have a high false-positive rate. The authors suggest that signature-based solutions are accurate and most suitable for preventing data breaches and leakages. According to the study (Liu & Kuhn, 2010), the data loss prevention framework is ideal in the contemporary supply chain. The framework combines several approaches to develop the best solutions for preventing illegal leakages of corporate data.

The relationship between illegal leakage of corporate information and the process of obtaining digital evidence does not clarify, thus, that would not be clear which one is most important in preventing leakage of corporate information using digital forensics. This research, therefore, analyses the two processes to elaborate the root causes of illegal leakages of corporate information in supply chain. The research finds that the increasing amount of data in new technologies poses threats to safety. At the same time, there are existing measures in place to obtain digital evidence in addressing digital breaches.

Table 1: Main Literature Review for Forensic Investigation: Creating by the Present Author

Key point	Summary
1. Computer Investigation and Forensics	* Identifying evidence, preserving, extracting, documenting in law enforcement and block distribution channels.
2. Basic Digital Forensic Investigation Model	* It is not difficult to apply for non-technical individuals. The FSSP model incorporates four steps as follows, collection, examination, analysis, and reporting.
3. Framework for Digital Forensic Investigation of Large Data.	* Technology development has seen the birth of an era of big data and data explosion. Therefore, there are increasing data needed to have been operated in cybercrime investigations.
4. Growing preference for automation and digital developments.	* An exponential rise in the application of computer technology. With the rise in technology comes risks of interaction. Such risks include cyber-attacks which have become more sophisticated.

Table 2: Main Literature Review for Forensic Factors: Creating by the Present Author

Key point	Summary
1. New Design for Digital Forensic Readiness (DFR)	* It involves a model with functionality operating as a forensic agent-based solution. The model performs forensic logging for digital Forensic Readiness purposes.
2. Interdependence of digital forensics and eDiscovery.	*The relationship between Digital Forensics and eDiscovery to highlight the skills required and the electronic resources needed in digital evidence management.
3. Disclosure of private information to unauthorized third parties.	* Disclosure internally or externally is referred to as data leakage, which may occur deliberately or mistakenly. According to the authors, corporates experience huge losses financially and non-financially.
4. Several factors influencing the monetary impact of data leakages in the corporate world.	* Categorizing personal information as sensitive explains the costs of these data leakages and finally suggested that independent variables demonstrate multilevel factorial behavior.

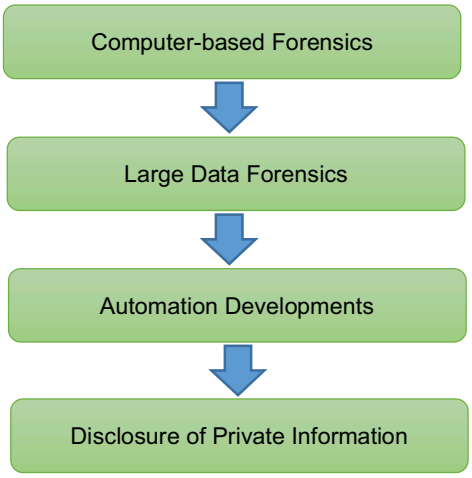

Figure 1: The Summaried Views of prior Literature: Creating by the Present Author

3. Method

The Collecting and analyzing data to achieve a valid conclusion follows several stages before presenting it to the rightful stakeholders. Verbal and non-verbal interactions between the researcher and the participant shape the collected data, eventually influencing the research findings. It is important to note that the written or verbal questions are correctly formulated to align with the research method, thus helping the researcher develop an understanding of the problem being researched (Lee, 2021; Gaur & Kumar, 2018).

All types of questions defining the objective of the qualitative content analysis should be used. The choice of the qualitative method hardly reflects the true context of participants. Essentially, the words used by the participants may not be interpreted depending on the researcher's perception of their meaning, thus resulting in bias. Additionally, the data collected may have misrepresentations due to participants being unable to express themselves, failing to tell the ultimate truth, or being affected by the information the researcher expects to hear from them. The process of data collection in qualitative content analysis entails five steps: identifying and collecting data, determining coding categories, coding the content, checking validity and reliability, and analyzing and presenting the results (Patrucco, Luzzini, & Ronchi, 2017; Sung, 2021).

The numerous prior studies have indicated the main procedure of qualitative textual analysis (Hong, 2021; Assarroudi, Heshmati Nabavi, Armat, Ebadi, & Vaismoradi, 2018; Woo & Kang, 2021; Lee, 2021).

Step 1: Identifying and collecting data: There are a couple of procedures used by researchers to collect data for QCA. Collecting data from the participants of the research can be conducted using verbal and non-verbal techniques. More methods used to collect QCA data include interviews, podcasts, online feedback, surveys, social media comments, and web conversations. A researcher considers seven main elements while conducting QCA. The elements include themes, words, characters, concepts, paragraphs, items, and semantics. The researcher needs to note the needed data relevant to the content analysis to develop substantive data for the QCA. Similar to all other types of studies, QCA encompasses sampling, not for the products or people, but for the content itself. The researcher should make the sample big enough to accommodate the entire population (Chen, Huang, & Li, 2022; Kang, 2021).

Step 2: Determining coding categories: Measuring of content in QCA is dependent on structured observation and adheres to particular written rules. Researchers use such rules to categorize the content. Researchers use mutually exclusive categories for easy replication and improve reliability. For proper QCA, the researcher classifies the content into different categories for better management. Dividing the collected data into categories helps the researcher focus on the particular categories for specific patterns and words.

Step 3: Coding the content: Coding is the process used by researchers to label the text to be analyzed. A text can be a phrase or a word. Researchers assign a number to every category to make the code mutually exclusive. Coding is a defined set of rules describing the techniques of observing content in a particular text, with the process helping researchers identify four essential characteristics, namely intensity, frequency, direction, and space.

Step 4: Checking validity and reliability: The role of the fourth stage is to test the designed codes. To achieve reliability, the codes need to be validated, with researchers testing the code to determine if it measures what is supposed to be measured. Additionally, testing the codes help the researchers understand whether the results are consistent. Researchers use a reliability check to understand the reliability of the collecting data.

Step 5: Analyzing and presenting data: Completing the qualitative content analysis means the collected raw data has been organized into sets of information, with the role of the researcher being able to present the report in a format that the stakeholders easily understand. This stage allows the researcher to review the final findings, plan all the information in a sequence, identify patterns and present it in the form of a report.

Additionally, the current author also conducted the 'Qualitative Data Analysis' (QDA) via web-based software which provides helpful platform to adjust and select a similar topics and categories in prior resources, checking

numerous themes to include emerging subjects. And then, the current author took care of the limitation of the qualitative textual approach to maintain the same quality of test information, interpreting deeply collected resources' through internal analysis of the results. As a result, this research could obtain a high level of the quality of textual instrument. The below Table 2 indicates the main process of the literature review analysis.

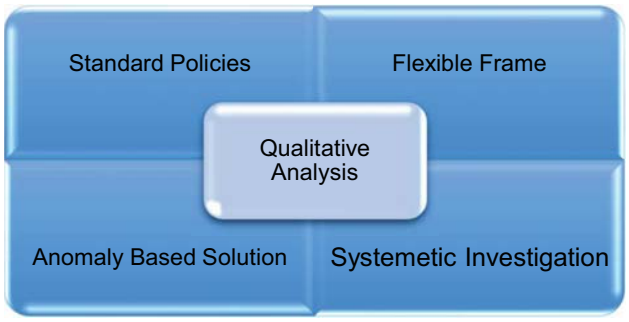

Figure 2: The Key Procedure of Qualitative Literature Analysis: Creating by the Present Author

4. Research Findings

4.1. Communicate with Stakeholders

There are several solutions regarding data leakage using digital forensics for corporate organizations. If the data leakage has already taken place, the first crucial step is to communicate with internal and external stakeholders. Internal communication involves informing employees and anyone who can help. Some employees that may be able to help include technical specialists and client service managers. Regarding external communication, corporate entities can reach out to clients through direct mailing (Zawoad & Hasan, 2016). The corporate entity may also release official media reports that indicate the nature of the data leakage. In communication, there are basic rules that must be followed. The organization with the data leakage must be open and sincere. In openness and sincerity, the company admits its wrongdoings and accepts responsibility. The corporate entity must also provide details of the data leakage to relevant stakeholders (Shabtai, Elovici, & Rokach, 2012). Providing details entails explaining the reasons for the data leakage. The company ought to have an internal audit to identify why the breach has occurred and the impact on company and client information. The organization with the data leakage must also attempt to mitigate the risk caused by the problem. In mitigation, the organization makes conclusions from the disaster and identifies the affected users.

Additionally, the organization with the data leakage must describe solutions for their affected clients and users. Where possible, affected users are given special offers aimed at helping them address their losses. Helping these affected users also helps promote trust in the company. In the business world, clients understand the possible threats to the safety of information. Thus, it is up to the organization to maximize trust from its consumers (Tabrizchi & Rafsanjani, 2020). The next step is the education of employees, especially those responsible for safeguarding company data. Education helps identify measures to avoid similar issues in the future (Alneyadi et al., 2016). Also, companies should invite dialogue from clients, experts, analysts, media, and the public. Dialogue fosters a broader discussion regarding the source of the data leakages and ways to mitigate the risk in the future. Dialogue also allows an organization with the challenge of data leakages to assess the views of other stakeholders regarding the issue at hand.

4.2. Preventing and Addressing Illegal Leakage

The second solution in preventing and addressing illegal leakage of corporate information is adopting a proactive security model. Several basic steps are recommended by SANS' First Five. These steps highlight the tactics that develop a more defense-in-depth approach to cybersecurity. However, many companies worldwide cannot meet these basic security steps (Baig, Szewczyk, Valli, Rabadia, Hannay, Chernyshev, & Peacock, 2017). For example, perimeter technologies such as firewalls cannot prevent certain types of external attacks. Yet, several organizations have these perimeter technologies applied even with the knowledge that they cannot meet the required levels of security preparedness. Thus, when under attack, these companies cannot block malware found in the organization's endpoints. Inherently, when malware finds itself within an organization's endpoints, it puts information at risk of intentional or accidental leakages. Therefore, corporates should develop multi-layered strategies with solutions such as patching and privilege management (Karie & Venter, 2015). These approaches help limit the pathways for malware to find crucial corporate information. Proactive technologies are essential in addressing information leakages in organizations. However, these technologies must not affect worker motivation and productivity (Dezfoli, Dehghantanha, Mahmoud, Sani, & Daryabar, 2013). They must ensure connectivity and seamless job progression. Inherently, it is difficult to balance the strike between productivity and security. The internet develops a pathway for malware to affect organizations.

On the other hand, employees require seamless connectivity to perform their jobs at high levels. Thus, several solutions, such as sandboxing, allow isolation of

web browsers to address malware challenges. In this approach, employees can work effectively and freely without wasting an organization's time and resources. Ensuring workers remain active during addressing cyber issues ensures that an organization remains profitable. Otherwise, the organization stands to lose its businesses to other function g organizations. While the threat of data leakages is real and affects several organizations, the organization has to safeguard the workplace to continue to see maximum output for the organization. Inherently, clients still need services rendered without interfering with data leakage solutions in digital forensics. Consequently, preventing illegal leakage of corporate information involves developing strategies to address the present challenge in the present and future.

4.3. Victims of Data Breach

The third solution involves victims of a data breach. The victim should first contact the "breach" company. Contact entails finding out the extent of the damage and the proposed steps. The "breach" company should have instructions on what steps to adopt. If the company suggests that the leaked information was encrypted, the victim should not trust them.

Furthermore, the thieves target the information first, and the likelihood that the information is in safe hands is nil. Next, the victim should ensure to change all passwords. In changing passwords, one should use complex terms and symbols to maintain the high security of sensitive information. Additionally, the victim should apply different passwords for different accounts. The victim should also call their banks and credit card companies to lock accounts (Bollam & Malsoru, 2011). Locking accounts ensures no further transactions can take place. Fast notification will also ensure that these companies release liability from the victims. Notably, after a data leakage, it is advisable to get a police report.

The damages should all be included in these reports to enhance recovery and investigation. The victim should also file an FTC report. They should also document everyone they have to talk to and everything they need to do. Documentation ensures that all processes are followed to enhance recovery and investigation of these data leakages. Documentation may also serve as evidence in courts (Jain & Lenka, 2016). The victim should also get a copy of their credit report to assess damages. The report allows you to inquire about unusual practices such as transactions on your credit. This credit report is to be included in the police report and the FTC report. Inherently, as a victim of a data breach in a corporate organization, one should subscribe to an I.D. theft Recovery program. Such programs enhance data recovery and ensure that the victim can get their lost data if their organization manages to successfully apprehend the data thrives or those who intentionally leaked the information. Inherently, it is impossible to prevent identity theft. Consumers can only protect themselves. Big companies may involve huge languages that make it hard for consumers to guarantee self-protection. Thus, the consumer should get ideal identity theft coverage that enhances recovery protection at affordable costs.

4.4. Focusing Solely on Technical Teams

The fourth solution suggests focusing solely on technical teams to address data leakages. A corporate organization affected by an illegal leakage of data should send in engineering teams to assess the breach and explain how it happened and ways to manage it. Organizations have to defend against illegal hackers who leak sensitive information (Simou, Kalloniatis, Kavakli, & Gritzalis, 2014). The system and network experts are well-versed with technical challenges. These experts are good at root cause analysis, collecting evidence, breach notification, and disclosure laws. There are several entities at stake when illegal leakages happen. There are liabilities, brand damages, among other issues. Handling the illegal leakage can provide minimal damages and devastation for an organization. Inherently, handling an illegal leakage issue is more than a technical issue. Therefore, it requires more than just technical resources.

The authority and involvement of senior management are vital to enforce decisions affecting the state of an organization. Notably, a corporate organization can benefit from experts in several fields, including forensic investigation, public relations, legal issues, media (Pichan, Lazarescu, & Soh, 2015). These entities enhance appropriate and timely responses to illegal data leakages for corporate organizations. Inherently, unprepared organizations hurt their reputation further through unorganized responses and chaos. Thus, these organizations need to exercise knowledge and experience in handling these security breaches (Collie, 2018). For instant success in illegal data leakages, these organizations should establish crisis management points of contact, implement incident response plans, conduct internal investigations, and contact law enforcement agencies.

Regarding third-party expertise, it is important to create strategies and communicate to the media. The organization should also conduct forensic investigations using outside investigators. Notably, the organizations should await confirmation from forensic teams to communicate with customers and notify them whether sensitive information has been lost. Consequently, there should be a containment and remediation plan to address the underlying issue in preparation for legal assessment.

Table 3: The summary of the present research findings: Creating by the Present Author

Research Findings	Summary
1. Communicate with Stakeholders	* Educates employees on the various strategies handling cultural diversity.
2. Standardization Business Strategy	* A particular single product is able to meet the needs of all consumers irrespective of their cultural values and norms. * It reduces costs of production as well as cultural distance.
3. Preventing and Addressing Illegal Leakage	* Enhances the ability of a multinational company to establish effective interaction with the target customers, a situation that may result in convenient communication with the target customers.
4. Focusing Solely on Technical Teams	* Helps in the acquisition of knowledge about the values, lifestyles, customs, and attitudes of the various cultures

5. Conclusion and Implication

Implication of this research provides an overview of the state and processes involved in gathering digital evidence. Future studies will benefit from this research as it provides ideal solutions that can be applied in cases of cyber-attacks and illegal leakages of sensitive information through digital forensics (Talesh, 2018). This study offers a well-structured analysis of how companies should use their action plans in case of illegal leakages of information, blocking distribution channels. As discussed, all companies face the challenge of securing sensitive corporate information. As the world continues to see massive technological advancements, the security of increasing amounts of data is at risk of cyber-attacks (Bulbul, Yavuzcan, & Ozel, 2013).

In the same way, the corporate world in the distribution channels is at risk of data leakage through accidental or intentional leakages. This research will help future researchers find ways to deal with all types of data leakages. Inherently, the research provides future studies with information surrounding organizations' preparedness in dealing with these cyber-attacks. The research recommends finding the services of forensic investigators among other experts who are in the best positions to conduct assessments and retrieve stolen information. Additionally, the research provides recommendations that assist victims of data breaches finding their stolen information and securing their accounts. The research provides guidelines for victims to follow in retrieving their lost or stolen data and prevent additional damages. Researchers will benefit from this research in several ways, including following the law in obtaining digital evidence.

The practical implications of preventing illegal leakage of corporate information to prevent distribution channels using digital forensics involve the integrity of collecting evidence (Daryabar, Dehghantanha, Udzir, bin Shamsuddin, & Norouzizadeh, 2013). The digital forensics community establishes standards for obtaining such evidence. Following the Fourth Amendment, the government should not perform illegal searches and seizures in digital forensics. Individuals and corporations enjoy the protection of their privacy rights in cases of acquiring digital evidence. Also, the fourth amendment asks typical questions surrounding the rights of individuals to enjoy security at the home, office and whether they are hence a reasonable expectation of privacy in storing electronic information on electronic devices. Inherently, there are challenges for both prosecutors and defendants regarding computer evidence.

Regarding digital evidence from computers, it is important to have proper documentation that allows performing forensic investigations. There are instances where the court allows forceful searches in cases where evidence can be altered or destroyed. There is an exception for handheld devices which is restricted by time. Following the law, such evidence may be searched without a warrant. The court allowed evidence acquired without proper documentation to enhance the reservation of the digital evidence (Park et al., 2018). In developing the Fourth Amendment, the power of contemporary technology was not envisioned. Thus, there are difficult scenarios that continue to introduce difficult questions surrounding engagement with digital evidence. Consequently, it is important to enhance data handling to provide answers for organizations that suffer due to illegal leakages of sensitive information, blocking distribution channels (Losavio, Chow, Koltay, & James, 2018). Forensic investigators should acquire evidence based on utilizing universally accepted methods in digital forensics.

6. Limitation and Future Suggestion

Vast amounts of data varied ICTs and borderless cyberinfrastructure present new challenges for security and cybercrime enforcement authorities. These problems and the development essential for securing modern societies and efficiently pursuing internet criminals are addressed to digital forensics. While digital forensics may seem like a new discipline, its origins stretch back to 1970, when technicians retrieved their first unintentionally destroyed copy of a database (Khan, Gani, Wahab, Shiraz, & Ahmad, 2016). Digital forensics quickly advanced from that point of departure. It is now conceivable, for example, to undelete the data or dump a trademark network for re-establishing a backup of the digital examination. The standard digital forensics toolkit includes all components of the cyber

investigative process. However, developments in the ICT sector are less likely and entail dangers, as mentioned previously.

The integrity of confiscated evidence, including hard drives, is anticipated by digital forensic specialists. Thus, the safe use is to read-only access the device and makes functioning copies of forensic pictures using forensic tools. For example, forensic images can analyze files and installed software or investigate deleted data in new regions. Nevertheless, the growth in gadgets and the available data make creating and evaluating such working replicates highly time intensive. The current advance attempts an exist system that allows forensic investigators to gather evidence, such as clipboard or RAM information, the details of open files, operative programs, effective network connections and graphed disks hidden in volatile digital devices.

Network forensics often needs the traffic generated by the host, intermediary node, or whole network to be collected and analyzed. Forensic analysts rely on traffic recording, network logs, and security devices such as intrusion detection systems for their availability. Different grains are feasible for this purpose (Khan et al., 2016). Unfortunately, it is cost-effective to gather and store each big network infrastructure package and overwhelm router or dedicated security tools like firewall resources. In addition, the volume of data cannot be assessed using commodity technology, making forensic analysis prohibitively costly, particularly if the criteria for real-time compliance are met.

Reverse engineering analyses a malware sample binary, network traffic track records and other tracks, such as guest OS log files. However, the efficacy is restricted by deploying a fraction of contemporary anti-forensic threats, for example, the obstruction of code or multi-stage loading designs that are covered up and encrypted at every step of the attack. The same applies to malware that is hidden-fit for information that connects secretly with a remote-control system.

The following should be considered as a future suggestion. Most digital forensic tools for finding information are meant to live on the suspect but give limited functions, including big-data resources, for new and challenging environments (Caviglione, Wendzel, & Mazurczyk, 2017). Consequently, the bulk of forensic software does not automatically identify anomalies or not. Therefore, the principal challenges to address soon are creating instruments and methods for assessing the volume of data and providing credible digital information to the investigator. Unfortunately, such tools and technical technologies, including proper visualization functions, represent complex challenges for the forensic investigator because of the absence of consistent standards and computer demands.

Fortunately, Digital research may use cloud computing features to download; for example, the highest digital forensic needs log analysis, including multimedia processing and data indexing. From that view, one of the intriguing components in A new paradigm in which the cloud exploits forensics as a service. For instance, Giuseppe Totara and his colleagues have built a program that researchers can index forensic disk images through a web interface.

Finally, even in new and unanticipated circumstances, digital forensics might soon become vital. IoT generates a connection between the cyber and the physical environment, making digital IOT forensics an efficient means of collecting nondigital environment information. For example, indoor presence sensor data may be examined by IoT nodes as to when a person is present in the room. Of course, such studies are connected to other data protection issues14, 15 since sensors could be impacted not just by one user but by an undefined group of influencers.

Table 4: The summary of conclusion and implications: Creating by the Present Author

Conclusion	Implication
Studies in feature will benefits from this study research since it provides solution applied in cyber- attack cases and illegal leakage of information.	* The research provides an overview of the state and process involved in digital gathering.
The research provides recommendation that assist victims of data breaches finding their stolen information and securing their account	* This study offers a well-structured analysis of how companies should use their action plan in case of information leakage.
The research will enable future researchers find ways of dealing with data leakages attack.	* Corporate world is at risk of data leakage through accident or intentional due to massive advancement of technology the security increase of data is at risk of cyber attacks
The research provides future studies with information surrounding organizations preparedness in cyber-attacks.	The practical implication of preventing illegal corporate information leakage using digital forensic involves the integrity evidence collecting

References

Adams, R. B., Hobbs, V., & Mann, G. (2013). The advanced data acquisition model (ADAM): A process model for digital forensic practice. JDFSL: *The Journal of Digital Forensics, Security and Law, 8*(4), 25-48.

Ali, M. D., & Kaur, D. (2020). Byod cyber forensic eco-system. *International Journal of Advanced Research in Engineering and Technology, 11*(9), 417-437.

Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. (2016). A survey on data leakage prevention systems. *Journal of*

Network and Computer Applications, 62(February), 137-152.

Assarroudi, A., Heshmati Nabavi, F., Armat, M. R., Ebadi, A., & Vaismoradi, M. (2018). Directed qualitative content analysis: the description and elaboration of its underpinning methods and data analysis process. *Journal of Research in Nursing, 23*(1), 42-55.

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., & Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation, 22*(September), 3-13.

Bollam, N., & Malsoru, M. V. (2011). Review on Data Leakage Detection. *International Journal of Engineering Research and Applications, 1*(3), 1088-1091.

Bulbul, H. I., Yavuzcan, H. G., & Ozel, M. (2013). Digital forensics: an analytical crime scene procedure model (ACSPM). *Forensic science international, 233*(1-3), 244-256.

Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The future of digital forensics: Challenges and the road ahead. *IEEE Security & Privacy, 15*(6), 12-17.

Chen, H., Huang, X., & Li, Z. (2022). A content analysis of Chinese news coverage on COVID-19 and tourism. *Current Issues in Tourism, 25*(2), 198-205.

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7*(5), 1-14.

Collie, J. (2018). A strategic model for forensic readiness. *Athens Journal of Sciences, 5*(2), 167-182.

Daryabar, F., Dehghantanha, A., Udzir, N. I., bin Shamsuddin, S., & Norouzizadeh, F. (2013). A survey about impacts of cloud computing on digital forensics. *International Journal of Cyber-Security and Digital Forensics, 2*(2), 77-95.

Dezfoli, F. N., Dehghantanha, A., Mahmoud, R., Sani, N. F. B. M., & Daryabar, F. (2013). Digital forensic trends and future. International *Journal of Cyber-Security and Digital Forensics, 2*(2), 48-77.

Esposito, C., Castiglione, A., Martini, B., & Choo, K. K. R. (2016). Cloud manufacturing: security, privacy, and forensic concerns. *IEEE Cloud Computing, 3*(4), 16-22.

Gaur, A., & Kumar, M. (2018). A systematic approach to conducting review studies: An assessment of content analysis in 25 years of IB research. *Journal of World Business, 53*(2), 280-289.

Guevara, C., Santos, M., & Lopez, V. (2017). Data leakage detection algorithm based on task sequences and probabilities. *Knowledge-Based Systems, 120*(March), 236-246.

Hong, J. H. (2021). A Global Strategy of a Company that Uses Culture Content as its Core Business. *The Journal of Industrial Distribution & Business, 12*(6), 37-46.

Jain, M., & Lenka, S. K. (2016). A review on data leakage prevention using image steganography. *International Journal of Computer Science Engineering, 5*(2), 56-59.

Kang, E. (2021). Qualitative Content Approach: Impact of Organizational Climate on Employee Capability. *East Asian Journal of Business Economics, 9*(4), 57-67.

Karie, N. M., & Venter, H. S. (2015). Taxonomy of challenges for digital forensics. *Journal of forensic sciences, 60*(4), 885-893.

Katz, G., Elovici, Y., & Shapira, B. (2014). CoBAn: A context-based model for data leakage prevention. *Information sciences, 262*(March), 137-158.

Kebande, V. R., & Venter, H. S. (2018). Novel digital forensic readiness technique in the cloud environment. *Australian Journal of Forensic Sciences, 50*(5), 552-591.

Khan, S., Gani, A., Wahab, A. W. A., Shiraz, M., & Ahmad. I. (2016). Network forensics: Review, taxonomy, and open challenges. *Journal of Network and Computer Applications, 66*(May), 214-235.

Kim, J., Lee, C., & Chang, H. (2020). The Development of a Security Evaluation Model Focused on Information Leakage Protection for Sustainable Growth. *Sustainability, 12*(24), 10639.

Krishnan, S., & Shashidhar, N. (2021). Interplay of Digital Forensics in eDiscovery. *International Journal of Computer Science and Security, 15*(2), 19-44.

Kruse II, W. G., & Heiser, J. G. (2001). *Computer forensics: incident response essentials.* London, United Kingdom: Pearson Education.

Lee, J. H. (2021). Effect of Sports Psychology on Enhancing Consumer Purchase Intention for Retailers of Sports Shops: Literature Content Analysis. *Journal of Distribution Science, 19*(4), 5-13.

Liu, S., & Kuhn, R. (2010). Data loss prevention. *IT professional, 12*(2), 10-13.

Losavio, M. M., Chow, K. P., Koltay, A., & James, J. (2018). The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. *Security and Privacy, 1*(3), 1-11.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports, 23*(4), 1-9.

Nelson, B., Phillips, A., & Steuart, C. (2014). *Guide to computer forensics and investigations.* Boston, MA: Cengage Learning.

Okereafor, K., & Djehaiche, R. (2020). A Review of Application Challenges of Digital Forensics. International *Journal of Simulation Systems Science and Technology, 21*(2), 351-357.

Park, S., Kim, Y., Park, G., Na, O., & Chang, H. (2018). Research on digital forensic readiness design in a cloud computing-based smart work environment. *Sustainability, 10*(4), 1203.

Patrucco, A. S., Luzzini, D., & Ronchi, S. (2017). Research perspectives on public procurement: Content analysis of 14 years of publications in the journal of public procurement. *Journal of Public Procurement, 17*(2), 229-269.

Pichan, A., Lazarescu, M., & Soh, S. T. (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital investigation, 13*(June), 38-57.

Poyraz, O. I., Canan, M., McShane, M., Pinto, C. A., & Cotter, T. S. (2020). Cyber assets at risk: monetary impact of US personally identifiable information mega data breaches. *The Geneva Papers on Risk and Insurance-Issues and Practice, 45*(4), 616-638.

Quick, D., & Choo, K. K. R. (2016). Big forensic data reduction: digital forensic images and electronic evidence. *Cluster Computing, 19*(2), 723-740.

Ribeiro, L. E. (2019). High-profile data breaches: Designing the right data protection architecture based on the law, ethics and trust. *Applied Marketing Analytics, 5*(2), 146-158.

Shabtai, A., Elovici, Y., & Rokach, L. (2012). *Data leakage*

detection/prevention solutions. In A Survey of Data Leakage Detection and Prevention Solutions (pp. 17-37). Boston, MA: Springer.

Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). *Cloud forensics: identifying the major issues and challenges. In International conference on advanced information systems engineering* (pp. 271-284). Cham, Switzerland: Springer.

Skalak, S. L., Golden, T. W., Clayton, M. M., & Pill, J. S. (2011). *A guide to forensic accounting investigation.* Hoboken, NJ : John Wiley & Sons.

Sung, I. (2021). Interdisciplinary Literaure Analysis between Cosmetic Container Design and Customer Purchasing Intention. *The Journal of Industrial Distribution & Business, 12*(3), 21-29.

Tabrizchi, H., & Rafsanjani, M. K. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing, 76*(12), 9493-9532.

Vavilis, S., Petković, M., & Zannone, N. (2016). A severity-based quantification of data leakages in database systems. *Journal of Computer Security, 24*(3), 321-345.

Wang, H., Wang, W., Sun, H., Cui, Z., Rahnamayan, S., & Zeng, S. (2017). A new cuckoo search algorithm with hybrid strategies for flow shop scheduling problems. *Soft Computing, 21*(15), 4297-4307.

Woo, E. J., & Kang, E. (2021). The effect of environmental factors on customer's environmental protection pattern: An empirical text analysis in the literature. *International Journal of Environmental Sciences, 7*(1), 1-15.

Yuan, J., & Yu, S. (2015). Public integrity auditing for dynamic data sharing with multiuser modification. *IEEE Transactions on Information Forensics and Security, 10*(8), 1717-1726.

Zawoad, S., & Hasan, R. (2016). Trustworthy digital forensics in the cloud. *Computer, 49*(3), 78-81.