# Security Management Information Systems Through Fire Wall Concepts, Logics And Problem Of Deleted Data: An Empirical Analysis

Gulnaz Niazi[1] , Dr. V.K Panchal[2] , Prof. Mansaf Alam[3]

[1]Research Scholar, Department of Computer Science, Al-Falah University, Dhauj, Fridabad, Haryana, India.

[2]PhD Supervisor, Department of Computer Science Al-Falah University, Dhauj, Faridabad, Haryana, India.

[3]PhD Co- Supervisor, Department of Computer Science Faculty of Sciences, Jamia Millia Islamia, New Delhi, India.

## ABSTRACT

The purpose of the study is to learn more about the opinions regarding Security Management Information Systems by examining Fire Wall principles, Logics and findings, and the issue with erased data. In order to learn more about respondents' opinions regarding Security Management Information Systems, a quantitative research methodology was applied. A Likert scale was used in the creation of the questionnaire. The theoretical study's conclusions served as the foundation for the queries. Still, 423 systems practitioners took the time to complete the survey. The data gathered from the surveys has been examined using the statistical application SPSS 20. The coefficient summary shows that the factor's beta values are 0.066, 0.359, and 0.536, which are generally indicative of the impact on Security Management Information System (SMIS). Additionally, the factor's beta values are 0.750 for ISA to FWS, 0.910 for LBS, and 0.873 for ISA to PDDR, which accurately represent the influence of Information Security Awareness (ISA) on Firewall security, Logic Based Security, and Problem of Deleted Data Recovery. The analysis found that there were flaws in the information security practices' conception, execution, and upkeep. It is essential for management to conduct an assessment of their information security procedures since they serve as a safeguard for the organization's and information-related assets.

**Key words**: Information Security Awareness, Security Management Information System, Logic Based Security, Firewall security, Problem of Deleted Data Recovery

## 1. INTRODUCTION

Information security is essential in the globalized world to maintain business continuity. S. E. Chang (2006). ISM is a thorough method that entails putting procedures and safeguards in place to guard against any incursion on an organization's information assets. Organizations continue to face risks, incidents, vulnerabilities, and threats related to information security despite their best efforts. M.A.M (2011) The existing ineffective ISM procedures are one of the major factors. When implementing ISM, organizations frequently place a priority on the technical components without giving the non-technical aspects the proper consideration. Shojaie and H. Federrath (2015). Usually, they proceed with the projects without understanding the crucial elements influencing their success. N. Maarop et al (2015). Given the aforementioned information, it is necessary to determine the critical elements that support ISM's performance. The model for acceptance and deployment of Security Management Information Systems in Information Technology is validated in this study in order to handle this problem.

## 2. OBJECTIVE OF THE STUDY

- To conduct an empirical examination of the suggested framework for determining the correlation between Fire wall concepts, Logics and findings and Problem of deleted data and their impact on Security Management Information Systems
- To propose a validated model for acceptance and implementation of Security Management Information Systems in Information Technology

## 3. LITERATURE REVIEW

### 3.1Information Security (IS)

Protecting data and information systems from unauthorized actions, such as access, use, disclosure, copying, recording, destruction, alteration, and manipulation, is known as information security. (F, Bjorck. 2001; Bokhari, S. and Manzoor, S. 2022).
Information security is actually the science of studying ways to prevent unwanted changes to data in computer and communication systems, as well as safeguarding information and reducing illegal access to it. Information security is the safeguarding of data for accessibility, integrity, and confidentiality. (P. Williams. (2001; Kamariotou, M.; Kitsios, F. 2023).

### 3.2 Security Management Information Systems (SMIS)

Identifying the elements that contribute to success in SMIS is crucial because it offers a helpful indication of the fundamental security management procedures needed in a company. This indicator will give the businesses a broad notion of what to embrace in terms of SMIS for their company. As a result of this finding, the organization might spend money on appropriate SMIS procedures that align with its goals. When considering the purpose of security management, a corporation must take a lot of steps to be eligible to utilize security management wisely. Although there isn't a set rule of thumb, there are numerous factors to take into account, as shown by von Solms and von Solms (2004; Tewamba, et.al. (2019).

### 3.3 Information Security Awareness

Hänsch and Benenson (2014) Describe three interpretations of information security awareness that differ from the majority of researches' interpretations. After attempting to define the term "information security awareness," the researchers arrived at these three interpretations, each of which is open to interpretation.

### 3.4 Firewall

A security defensive tool used in computer network security is the firewall. It functions as a bridge between the extranet and intranet. It is acknowledged that the former is a secure network. The latter is recognized asa comparatively less safe network. Hardware and software make up the firewall. The firewall is the sole device through which connectivity between the intranet and extranet can and should go. The fundamental tool for ensuring network information security is a firewall. It is really protective. In the past, firewalls used as building partitions to stop fires from spreading.

This is expanded to safeguard a protective wall's internal network security. Tang (2018). In practice, firewall behavior is frequently problematic due to its lack of specificity, which is either under- or undefined. Firewalls behave more consistently across implementations and in accordance with established protocol conventions when requirements are specified.

**H1:** Increased knowledge of information security (ISA) can benefit firewalls by making them more consistent across implementations.

**H2:** The specified firewall behavior can positively affect the success of security management information system.

### 3.5 Logic-Based Security

Ensuring safe end-to-end communication is necessary when two entities interact to receive a certain service or services. Systems cannot function effectively without appropriate security measures in place since there are many different kinds of potential attackers. A set of conditions that must be met by the parties involved in communication in order to ensure safe communication and defend services from attackers can be used to define security.

When The authors' reasoning was based on logic, and their main goal was to develop a single static data model that would prevent the introduction of additional rules at runtime. In (Bamgboye O,2019), To ensure the consistency of the data stream generated by physical sensors in smart settings, the authors put forth a reasoning framework. Nevertheless, there is no end-user interaction with this framework.

**H3:** Information Security awareness (ISA) can have a favorable impact on logic based security implementations

**H4:** The logic based security implementations can positively affect the success of security management information system.

### 3.6 Problem of Deleted Data

Recovery is the collection of methods used to retrieve data from any backup server in the event that the original data was lost from the server or was no longer viable for use. Backup is described as a duplicate of any data, file, application, and operating system that may be utilized in the event of a data loss or restoration.

A disaster recovery plan is essential since disasters affect both the client and the cloud side. As stated by (A. Arul Mary, K. Chitra (2019) when “disaster happens in customer side means backup will be stored in the cloud, but disaster happens in the cloud means data will be lost. So, disaster recovery process is urgently needed.

But quality and security are the key issues in the information recovery process" Tyagi et al (2019).

The process of recovering corrupted, missing, or damaged data from storage devices is known as data recovery. This technique is applied to devices such as SD cards, hard disks (internal and external), SSD devices, CDs, DVDs, and any other storage device when the data is not accessible through conventional means, i.e., when the data is corrupted or entirely formatted, or when the storage device is damaged. D Drives (2017)

Alzahrani et al. (2022) presented an architecture that emphasizes recovery and dependability while combining replication and erasure coding benefits to produce the optimal storage solution. In order to allow dynamic structure development in the future and validate the data model, learning and training techniques were developed.

**H5:** Information Security awareness (ISA) about safe data backup and recovery can have a favorable impact on the recovery of deleted data.

**H6:** An effective and practical data recovery plan to recover corrupted, lost, damaged or deleted data can positively affect the success of security management information system.

## 4. CONCEPTUAL FRAMEWORK

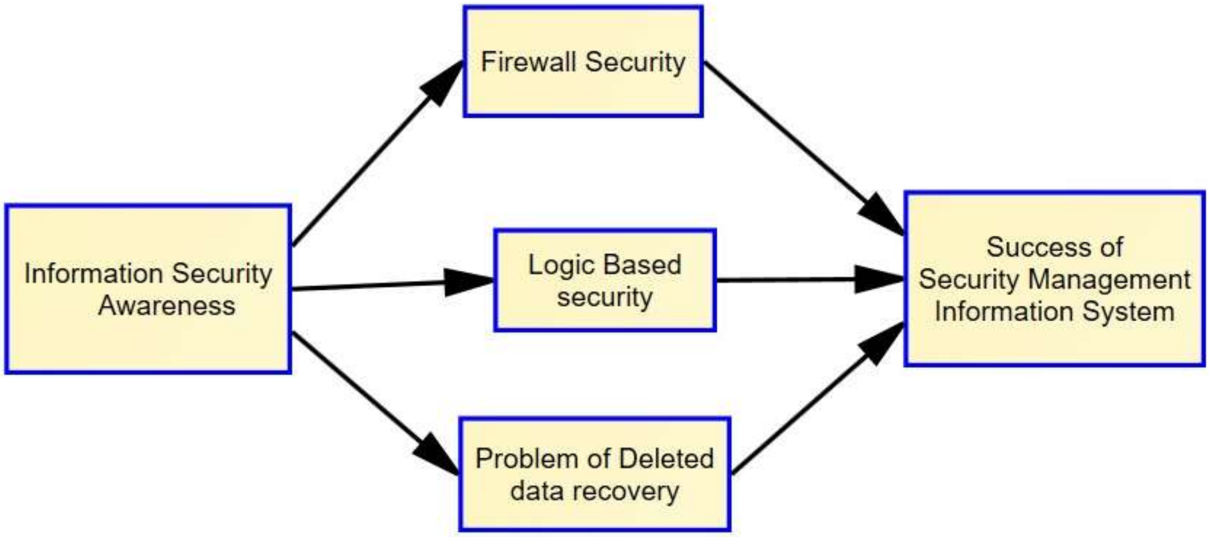
Firewall Security
Information Security Awareness
Logic Based security
Success of Security Management Information System
Problem of Deleted data recovery

**Figure** 1: Conceptual model proposed assessing the relationship among 'Information Security awareness (ISA)', Firewall security, Logic based security, Problem of deleted data recovery and success of security management information system.

## 5. RESEARCH METHODOLOGY

### 5.1 Research Design

A quantitative methodology was used in the study to explore respondents’ perceptions regarding information security awareness and it impact on the Security Management Information Systems through Fire wall concepts, Logics and Problem of deleted data. The quantitative method is the most useful choice since it enables researchers to collect information in depth and promotes a deeper understanding of the topic, especially because this study employed a empirical approach.

### 5.2 Population and Sample

The sampling was based on the respondents' capacity to address the research questions. strategy. Purposive sampling was therefore used. Participants in the study who were actively involved in Security Management Information Systems and had experience with Security Systems were invited for questionnaire based survey. Every participant had prior knowledge of information systems for security management. Table 1 displays the participants' profiles.

### 5.3 Data Collection

The first step in this study's data collection process was a literature analysis. This theoretical investigation examined both published and unpublished materials from a variety of internet databases with the goal of finding additional pertinent components and validating the factors deduced from the theoretical study. In this study, pre-structured close ended questionnaire was utilized for data collection. The questionnaire was sent through email and online to the targeted respondents seasoned with Security Management Information Systems.

The survey data was collected from January 2023 and April 2023. A Likert scale was used in the creation of the questionnaire. The theoretical study's conclusions served as the foundation for the queries. There were two sections to the questions: A and B. The participants' demographic profile , their organizations and their own experiences with their deployment were covered in Part A.

The respondents’ perceptions and awareness regarding the Security Management Information Systems through Fire wall concepts, Logics, and Problem of deleted data were the focus of part B's questions.

## 6. RESULTS AND ANALYSIS

A total of four hundred and seventy seven Systems practitioners were invited to participate in the survey. Still, 423 replies were found complete, valid, and free from any missing information, they were used for further examination. The statistical analysis has been applied to the survey data using SPSS 22. According to the goals of the study, a number of data analysis techniques, including Karl Pearson regression and correlation analysis were used for data analysis.

### 6.1. Demographic profile

The respondent's demographic characteristics were evaluated using descriptive demographic data that were presented as frequency, proportion, and percentage (Table 1). 84.60% of the responses are judged to be of good quality after careful examination. There were a great deal more male respondents (361, 85.3%) than female respondents (62, 14.7%) Of the 423 participants, 116 (27.4%) were the majority between the ages of 31 and 40, and 182 (43%) had a Professional education, 156 (36.9%) had been working for more than 11 to 15 years, as Network/ firewall administrator (118, 27.9%) and have good Level of Awareness of information security system (104, 24.6%).

**Table 1. Descriptive Statistics of Demographic Profile**

| | 423 | **Frequency** | **Valid %** |
|---|---|---|---|
| **Gender** | Male | 361 | 85.3 |
| | Female | 62 | 14.7 |
| **Age** | 21-30 years | 59 | 13.9 |
| | 31-40 years | 116 | 27.4 |
| | 41-50 years | 81 | 19.1 |
| | 51-60 years | 105 | 24.8 |
| | 61 years and above | 62 | 14.7 |
| **Highest education level** | Bachelor degree | 50 | 11.8 |
| | Master degree | 114 | 27.0 |
| | Prof. Education | 182 | 43.0 |

| | | | |
|---|---|---|---|
| | Other | 77 | 18.2 |
| **Tenure in information security field (in years)** | Less than 5 | 94 | 22.2 |
| | 5 to 10 | 147 | 34.8 |
| | 11 to 15 | 156 | 36.9 |
| | More than 15 | 26 | 6.1 |
| **Primary role within the field of information security** | Technical associate | 57 | 13.5 |
| | Network/ firewall administrator | 118 | 27.9 |
| | ISM Implementer | 84 | 19.9 |
| | Network engineer | 104 | 24.6 |
| | ISM coordinator | 60 | 14.2 |
| **Level of Awareness of information security system** | Very low | 65 | 15.4 |
| | Low | 100 | 23.6 |
| | Moderate | 89 | 21.0 |
| | Good | 104 | 24.6 |
| | Excellent | 65 | 15.4 |

### 6.2. Exploratory Factor and Reliability Analysis

The EFA was used to determine how important the compliant components were. In this experiment, a factor loading of 0.50 serves as the threshold. These findings imply that factor analysis is an appropriate method for gathering this data. Included was any element with factor loadings greater than 0.5. in the final analysis. It is commonly acknowledged that a scale is internally consistent if it meets the Chronbach's Alpha minimum criterion of 0.70. For this study, a Cronbach's alpha cutoff of 0.7 was employed.

**Table 2. Results of Exploratory Factor Analysis**

| **Variable** | **Cronbach alpha** | **Statement** | **Factor loadings** | **KMO Measure of Sample Adequacy (>0.5)** | **Bartlett's Test of Sphericity** | | **Items confirmed** | **Items dropped** | **Cum % of loading** |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | **Chi Square** | **Sig. (<.10)** | | | |
| ISA | 0.816 | ISA-1 | 0.900 | 0.743 | 774.739 | 0.000 | 4 | 1 | |
| | | ISA-2 | 0.760 | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | ISA-3 | 0.682 | | | | | | 55.451 |
| | | ISA-4 | 0.466 | | | | | | |
| | | ISA-5 | 0.838 | | | | | | |
| FWS | 0.746 | FWS-1 | 0.761 | 0.740 | 376.215 | 0.000 | 4 | 1 | 45.495 |
| | | FWS-2 | 0.805 | | | | | | |
| | | FWS-3 | 0.068 | | | | | | |
| | | FWS-4 | 0.756 | | | | | | |
| | | FWS-5 | 0.686 | | | | | | |
| LBS | 0.954 | LBS-1 | 0.163 | 0.856 | 1833.181 | 0.000 | 4 | 1 | 70.725 |
| | | LBS-2 | 0.926 | | | | | | |
| | | LBS-3 | 0.944 | | | | | | |
| | | LBS-4 | 0.951 | | | | | | |
| | | LBS-5 | 0.926 | | | | | | |
| PDDR | 0.972 | PDDR-1 | 0.948 | 0.716 | 5038.643 | 0.000 | 5 | 0 | 89.985 |
| | | PDDR-2 | 0.945 | | | | | | |
| | | PDDR-3 | 0.949 | | | | | | |
| | | PDDR-4 | 0.956 | | | | | | |
| | | PDDR-5 | 0.945 | | | | | | |
| SMIS | 0.897 | SMIS-1 | 0.884 | 0.832 | 1379.193 | 0.000 | 5 | 0 | 70.868 |
| | | SMIS-2 | 0.906 | | | | | | |
| | | SMIS-3 | 0.883 | | | | | | |
| | | SMIS-4 | 0.798 | | | | | | |
| | | SMIS-5 | 0.725 | | | | | | |

### 6.3. Correlatıon Analysis

Every variable that was taken into consideration has a substantial association with every other variable (Table 4). It was found that the strongest association (0.946) between Problem of Deleted Data Recovery (PDDR) and Security Management Information System (SMIS), whereas the weakest (0.750) was discovered between Information Security Awareness (ISA) and Firewall security (FWS).

**Table 3: Correlations**

| | ISA | FWS | LBS | PDDR | SMIS |
|---|---|---|---|---|---|
| **ISA** | 1 | | | | |
| **FWS** | .750** | 1 | | | |
| **LBS** | .910** | .833** | 1 | | |
| **PDDR** | .873** | .810** | .917** | 1 | |
| **SMIS** | .865** | .821** | .930** | .946** | 1 |

**. At the 2-tailed 0.01 significance level, there is a correlation.

## 6.4. Regression Analysis

The researcher determines the impact of independent factors on dependent variables, examines hypotheses, and supports the prototype assumption statistically using a significant multivariate regression analysis at the five percent enter method level. Each variable's mean and standard deviation values were analyzed in order to determine the questionnaire items and findings.

Stepwise The predictor-criterion link between the independent and dependent variables was ascertained by regression analysis. This study employs linear regression as opposed to nonlinear regression, in contrast to previous studies. To evaluate if a model is appropriate, scalable, and capable of dismissing the theory that the total regression coefficient is equal to zero, researchers employ the F-test, adjusted coefficient R2, and t-test.

### 6.4.1 Firewall security, Logic Based Security and Problem of Deleted Data Recovery as dependent variable

Table 4a's regression analysis aims to investigate your perceptions about the Security Management Information Systems through Fire wall concepts, Logics and findings and Problem of deleted data.

The R square value of 0.562 in dicate that Information Security Awareness (ISA) can account for 56.2% of Firewall security (FWS).

Information Security Awareness (ISA) has R square values between 0.762 and 0.828 indicate that it can explain 82.8% and 76.2% of Logic Based Security (LBS) and Problem of Deleted Data Recovery (PDDR). Table 4b's The regression model's ANOVA results show that, with a 95% confidence level, the validation is valid. The summary of coefficients shown in Table 4c indicates that information security awareness (ISA) has an impact on logic-based security and firewall security and Problem of Deleted Data Recovery, The beta values of 0.873 for LBS, 0.910 for ISA to FWS, and 0.750 for LBS appropriately represent ISA to PDDR.

**Table 4a : Regression analysis**

| **Model** | **Predictors** | **Dependent variable** | **R** | **R Square** | **Adjusted R Square** | **Std. Error of the Estimate** |
|---|---|---|---|---|---|---|
| 1 | ISA | FWS | 0.750 | 0.562 | 0.561 | 0.48552 |
| 2 | ISA | LBS | 0.910 | 0.828 | 0.827 | 0.39621 |
| 3 | ISA | PDDR | 0.873 | 0.762 | 0.761 | 0.47198 |

**Table 4b : ANOVA analysis**

| **Model** | **Predictors** | **Dependent variable** | | **Sum of Squares** | **df** | **Mean Square** | **F** | **Sig.** |
|---|---|---|---|---|---|---|---|---|
| 1 | ISA | FWS | Regression<br>Residual<br>Total | 127.246<br>99.243<br>226.489 | 1<br>421<br>422 | 127.246<br>0.236 | 539.794 | 0.000 |
| 2 | ISA | LBS | Regression<br>Residual<br>Total | 317.396<br>66.088<br>383.484 | 1<br>421<br>422 | 317.396<br>0.157 | 2021.892 | 0.000 |
| 3 | ISA | PDDR | Regression<br>Residual<br>Total | 300.299<br>93.784<br>394.082 | 1<br>421<br>422 | 300.299<br>0.223 | 1348.055 | 0.000 |

**Table 4c: Regression coefficients table for dependent variables**

| Model | | Dependent variable | Unstandardized Coefficients | | Standardized Coefficients | | |
|---|---|---|---|---|---|---|---|
| | | | B | Std. Error | Beta | t | Sig. |
| 1 | ISA | FWS | 0.665 | 0.029 | 0.750 | 23.233 | 0.000 |
| 2 | ISA | LBS | 1.051 | 0.023 | 0.910 | 44.965 | 0.000 |
| 3 | ISA | PDDR | 1.022 | 0.028 | 0.873 | 36.716 | 0.000 |

### 6.4.2 Security Management Information System (SMIS) as dependent variable

Step-wise regression analysis shows that the three independent factors— Firewall security (FWS), Logic Based Security (LBS), Problem of Deleted Data Recovery (PDDR)—are all significant predictors of the Security Management Information System (SMIS). Based on Table 5a's highest R square values of 0.921, it is possible that 92.1% of the influence on the One might attribute the Security Management Information System (SMIS) to the variables. ANOVA findings for the regression model at a 95% confidence level are displayed in Table 5b. The coefficient summary in Table 5c indicates that the factor's beta values are 0.066, 0.359 and 0.536 which are generally indicative of the impact on Security Management Information System (SMIS).

**Table 5a : Regression analysis**

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | 0.960[a] | 0.921 | 0.920 | 0.24130 |

a. Predictors: (Constant), PDDR, FWS, LBS

**Table 5b : ANOVA analysis**

| Model | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | Regression | 283.766 | 3 | 94.589 | 1624.551 | 0.000$^b$ |
| | Residual | 24.396 | 419 | 0.058 | | |
| | Total | 308.162 | 422 | | | |

a. Dependent Variable: SMIS

b. Predictors: (Constant), PDDR, FWS, LBS

**Table 5c: Regression coefficients table for dependent variables**

| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | 0.204 | 0.048 | | 4.256 | 0.000 |
| | FWS | 0.077 | 0.030 | 0.066 | 2.605 | 0.010 |
| | LBS | 0.322 | 0.033 | 0.359 | 9.628 | 0.000 |
| | PDDR | 0.498 | 0.031 | 0.563 | 15.999 | 0.000 |

a. Dependent Variable: SMIS

### 6.5. Results of Hypotheses Testing

Six All of the hypotheses presented in the conceptual research framework (table 6) have received acknowledgement.

**Table 6: Summary of Hypotheses Testing**

| Hy. No. | Independe ntVariables | Dependent Variables | R-Square | Beta Coefficient | t-value | Sig Value | Status of Hypotheses |
|---|---|---|---|---|---|---|---|
| H1 | Information Security Awareness (ISA) | Firewall security (FWS) | 0.562 | 0.750 | 23.233 | 0.000 | Accepted |
| H2 | Firewall security (FWS) | Security Management Information System (SMIS) | 0.921 | 0.066 | 2.605 | 0.000 | Accepted |
| H3 | Information Security Awareness (ISA) | Logic Based Security (LBS) | 0.828 | 0.910 | 44.965 | 0.000 | Accepted |
| H4 | Logic Based Security (LBS) | Security Management Information System (SMIS) | 0.921 | 0.359 | 9.628 | 0.000 | Accepted |
| H5 | Information Security Awareness (ISA) | Problem of Deleted Data Recovery (PDDR) | 0.762 | 0.873 | 36.716 | 0.000 | Accepted |
| H6 | Problem of Deleted Data Recovery (PDDR) | Security Management Information System (SMIS) | 0.921 | 0.563 | 15.999 | 0.000 | Accepted |

### 6.6 Discussion

Security awareness, Training and instruction in security are among the most essential components needed for an information security culture. within the company, according to Soomro et al. (2016). Top management should place a high priority on these aspects. Employees need to understand that following policies and procedures is essential to preventing unintentional or deliberate security breaches. Nonetheless, security awareness has not kept up with the rapid advancements in technology, where dangers are emerging from nearly every direction (D'Arcy et al., 2009; Safa et al., 2016). As stated by Da Veiga and Eloff (2010), a deficiency of security awareness leads to security noncompliance in cloud environments, hence increasing the complexity of IT service outsourcing arrangements. Without appropriate People lack understanding of potential security risks despite security awareness, education, and training initiatives. breaches. According to Bachlechner et al. (2014), these awareness campaigns have a beneficial impact on controlling and discouraging security-related behaviour.

Furthermore, companies with appropriate Policies and procedures for information security (SPP) are more effective at teaching staff members how to behave securely. According to research, adhering to an organization's security policy helps influence and reduce the likelihood of misbehavior by employees (Van Niekerk et al., 2010). To have an effective deterrence element, however, staff members need to Recognize the established information security policies. (Parsons et al., 2014). Establishing an ethical behavior policy is also essential for establishing a security culture inside the company (Connolly et al., 2015; Herath & Rao, 2009).

The study's results on the connection between firewall security (FWS) and information security awareness (ISA), as well as how it affects security Management Information System (SMIS) further supported a significant positive relationship (H1 and H2; R-square = 0.562 and 0.921; beta coefficient = 0.750 and 0.066; t-value = 23.233 and 2.605). Firewalls, which can be host-based or network-based, are a crucial component of any network's security, according to Sheth and Thakker (2011). Host-based firewalls assist in filtering traffic to the hosts or end devices, whereas network firewalls, which are based on network hardware, aid in securing networks. Firewalls historically operated using statically configured rules, like access policy lists, according to Patil et al. (2018). They have evolved to recognize and react to network threats in real time. as a result of growing threats over time. Firewalls, according to Mothersole and Reed (2011), can dynamically control the Over their ports, information is exchanged. The concept is that you must establish a connection. Regulate unreliable services. As Wang Qiang qiang (2019) points out, firewalls are an efficient way to regulate insecure services. Establish in advance the policies for Data input and departure between the distrust and trust domains. Unsafe services that are not on the intranet can be blocked. Plans for rules can also be defined. When a policy for starting and shutdown is needed, automatically launch and close. It provides versatility in addition to significantly boosting intranet security. Peng Zhen Yu (2020) claims that firewalls have the ability to concentrate all of the software required for intranet security. encompassing all upgrades and additions to the software. similar to a password on a computer. Verification and passwords. Firewalls can be used to centrally control these security concerns. It is simple to use and has a high efficiency. The firewall must be at the center of the security strategy in order to provide centralized security protection configuration.

The empirical investigation of hypothesis 3 and 4 revealed a significant positive correlation (R-square = 0.828 and 0.921; Beta coefficient = 0.910 and 0.359; t-value = 44.965 and 9.628) between Information Security Awareness (ISA) and Logic Based Security (LBS) with respect to Security Management Information System (SMIS). K. Sanzgiri et al. (2005) state that in order to define and evaluate any security requirement in any system that uses logic to provide multi-hop communication, there must be a logic-based security. Any protocol or system that claims to be secure can be mapped; to put it another way, it needs to be defined using a variety of global and local settings and actions before being subjected to various criteria for analysis. Rather than relying solely on simulation tools, the correctness of which is debatable among many researchers, LBS offers a formal method for analyzing security enforcement and security protocols. Furthermore, according to Y. Xu and X. Xie (2008), employing simulation tools often covers a limited number of scenarios, but employing LBS allows for the coverage of additional cases that simulation methods are typically unable to cover completely. Z. Shao (2008) claims that applying LBS to the two widely used enforcers, the digital certificate and the MAC —it is possible to validate security enforcers. Furthermore, the security of Ariadne, a safe routing system utilized within sensor and ad hoc networks, was assessed via LBS.

The suggested security architecture addresses the most significant enforcers, as far as we are aware. Future developments of new enforcers might only require the addition of new sets, behaviors, and regulations. Additionally, new guidelines and procedures for the interaction between the Systems for preventing intrusions and detecting intrusions (IDS and IPS) may taken into consideration to expand LBS. Additionally, LBS can analyze security using computational intelligence technologies (Madria and Yin, 2009; Stavrou and Pitsillides, 2010; Almomani and Saadeh, 2012).

Information Security Awareness (ISA) and Problem of Deleted Data Recovery (PDDR) independently shown a strong positive relationship between the two constructs. and further show impact on Security Management Information System (SMIS). The results of this study (R-square = 0.762 and 0.921; beta coefficient = 0.873 and 0.563; t-value = 36.716 and 15.999) are consistent with Hypothesis 5 and 6. According to Bardis et al. (2017), data recovery services need to provide high data reliability and flexibility by implementing a workable and efficient data recovery plan that can support any organization's growth. The authors state that cost, security, latency-free operation, redundancy, and cloud data storage are the most important factors pertaining to data recovery in cloud computing. Faria et al. (2019) discovered a variety of methods, each with its own specialization for creating backup and recovery. According to Zhong & Xiang's (2012) experimental results, a large number of businesses and organizations have used disaster recovery solutions in an effort to reduce downtime and data loss that occurs during natural disasters.

## 7. CONCLUSION

In order to comprehend and investigate the Security Management Information System of Indian IT development and services firms, the current study employs a quantitative research methodology. The study's cases have been analyzed using pre-structured questionnaire and descriptive analysis techniques. The study's conclusions may prove beneficial to companies operating in related fields with comparable tasks or roles. Similar research can be done in the future for companies in many sectors and industries. An interesting observation would be how various information security methods are affected by organization size and industry. Linkages between different Security Management Information System components can be found as an extension of this study to investigate their causal links with one another. Additionally, this might aid in the creation of an organizational framework for security management, which would be helpful to practitioners in setting priorities for different security management procedures.

## 8. FUTURE PROSPECTS

The analysis found that there were flaws in the information security practices' conception, execution, and upkeep. It is imperative that management evaluate their information security. procedures since they serve as a safeguard for the organization's and information-related assets. To provide protection, any missing interventions or gaps in the system should be fixed. Studies of a similar nature can be conducted for other Indian IT sector institutes. The application of regulations governing mobile devices, funding, training, user awareness, information security policy review, and updates and enhancements were found to have deficiencies and require improvement.

## 9. LIMITATIONS

The study has a rather small sample size, which considerably reduces the study's trustworthiness given the scope of the information security industry. The use of an open-ended questionnaire and anonymity have a detrimental effect on the results' trustworthiness because it is not possible to ensure that all of the respondents were among the potential respondents we had selected. Nevertheless, there is no basis for us to believe that the questionnaire was ever distributed in an unauthorized manner.

## REFERENCES

A. Alzahrani, T. Alyas, K. Alissa, Q. Abbas, Y. Alsaawy, and N. Tabassum. Hybrid (2022). Approach for Improving the Performance of Data Reliability in Cloud Storage Management. Sensors, 22(16), 5966. 2022.

A Arul Mary, K. Chitra, (2019).”OGSO-DR: oppositional group search optimizer based efficient disaster recovery in a cloud environment” J Ambient In tell Human Comput 10, 1885–1895 (2019).

Bachlechner, D., Thalmann, S., & Maier, R. (2014). Security and compliance challenges in complex IT outsourcing arrangements: A multi-stakeholder perspective. Computers & Security, 40, 38-59.

Bamgboye O, Liu X, Cruickshank P.(2019). Semantic stream management framework for data consistency in smart spaces. In: 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC);2019. p. 85–90.

Bardis N.G., Doukas N. and Markovskyi O.P. (2017). “A Method for Cloud Storage Data Recovery with Limited Loss of Access”, Proceedings - 2017 4th International Conference on Mathematics and Computers in Sciences and in Industry, MCSI 2017, vol nr.2018-January,2018, pp.128- 133

Bokhari, S. and Manzoor, S. (2022) Impact of Information Security Management System on Firm Financial Performance: Perspective of Corporate Reputation and Branding. American Journal of Industrial and Business Management, 12, 934-954. doi: 10.4236/ajibm.2022.125048.

B. Shojaie and H. Federrath, (2015).“The effects of cultural dimensions on the development of an ISMS based on the ISO 27001,” in 10thInternational Conference on Availability, Reliability and Security,2015, pp. 159–167.

Connolly, L., Lang, M., & Tygar, J. D. (2015). Investigation of employee security behaviour: A grounded theory approach. In IFIP International Information Security and Privacy Conference (pp. 283-296). Springer, Cham.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79-98.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196-207.

D Drives.(2017).”Hard Drive Circuit Board Replacement.“july (2017). [Online].Available: http://www.donordrives.com/pcbreplacement-guide.

E. Stavrou and A. Pitsillides. (2010). “A survey on secure multipath routing protocols in WSNs,” Computer Networks, vol. 54, no. 13, pp. 2215–2238, 2010.

Faria H., Solís P., Bordim J. and Hagstrom R. (2019).” A backup-as-a-service (BaaS) software solution”, CLOSER 2019 - Proceedings of the 9th International Conference on Cloud Computing and Services Science, Brasilia,2019, pp.225-232.

F, Bjorck. (2001). Security scandin avian style, interpreting the practice of managing information security in organizations, Stockholm University & Royal Institute of Technology.

Hänsch, N., Benenson, Z., (2014). Specifying IT Security Awareness, in: 2014 25th International Work-shop on Database and Expert Systems Applications. pp. 326–330.DOI: https://doi.org/10.1109/DEXA.2014.71

Herath, T. & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165.

I. Almomani and M. Saadeh. (2012). "Security model for tree-based routing in wireless sensor networks: structure and evaluation," KSII Transactions on Internet and Information Systems, vol. 6, no. 4, pp. 1223–1247, 2012.

I. Mothersole and M. J. Reed. (2011). Optimising Rule Order for a Packet Filtering Firewall, 2011 Conference on Network and Information Systems Security, La Rochelle., pp. 1-6.

Conceptual Framework. Electronics 2023, 12, 382.https://doi.org/10.3390/electronics12020382

Kamariotou, M.; Kitsios, F.(2023), Information Systems Strategy and Security Policy: A Conceptual Framework. Electronics 2023, 12, 382.https://doi.org/10.3390/electronics12020382

K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer. (2005). "Authenticated routing for ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598–610, 2005.

M.A.M. Stambul & R. Razali, (2011)."An assessment model of information security implementation levels," in Proc. 2011 Int. Conf. Electr. Eng. Informatics, 2011, July, p. 1–6.

N. Maarop, N. Mustapha, R. Yusoff, R. Ibrahim, and N. M. M. Zainuddin, (2015). "Understanding success factors of an information security management system plan phase self-implementation," International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering, vol. 9, no. 3, pp. 884–889, 2015.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & security, 42, 165-176.

Peng Zhen yu. (2020). Based on computer network security and preventive countermeasures research, cyber security technology and application, 2020 (08): 3-4.

P. Williams. (2001). Information security governance, Information Security Technical Report 6 (3), pp. 60–70.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. computers & security, 56, 70-82.

S. E. Chang and C. B. Ho, (2006) "Organizational factors to the effectiveness of implementing information security management," Ind. Manag. Data Syst., vol. 106, no. 3, pp. 345–361, 2006.

Sheth, C and Thakker, R. (2011). Performance Evaluation and Comparative Analysis of Network Firewalls, 2011 International Conference on Devices and Communications (ICDeCom), Mesra., pp. 1-5.

S. Madria and J. Yin. (2009). "SeRWA: a secure routing protocol against wormhole attacks in sensor networks," Ad Hoc Networks, vol. 7, no. 6, pp. 1051–1063, 2009.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.

Tang (2018).Xiao bin. Computer Network Security Research [J] Based on Firewall Technology Digital World, 2018(07): 38.

Tewamba, H. N., Kamdjoug, J. R. K., Bitjoka, G. B., Wamba, S. F., & Bahanag, N. N. M. (2019). Effects of Information Security Management Systems on Firm Performance. American Journal of Operations Management and Information Systems, 4, 99-108. https://doi.org/10.11648/j.ajomis.20190403.15

Tyagi H, Apergis-Schoute AM, Akram H, Foltynie T, Limousin P, Drummond LM, Fineberg NA, Matthews K, Jahanshahi M, Robbins TW, Sahakian BJ, Zrinzo L, Hariz M, Joyce EM, (2019). A randomized trial directly comparing ventral capsule and anteromedial subthalamic nucleus stimulation in obsessive-compulsive disorder: clinical and imaging evidence for dissociable effects. Biol. Psychiatry 85 (9), 726–734. [PMC free article] [PubMed] [Google Scholar]

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. Computers & security, 29(4), 476-486.

Vinay T. Patil et al. (2018). Performance and information security evolution with firewalls, International Science and Technology Journal, Volume 7, Issue 2, pp. 33- 38.

Von Solms B, von Solms R (2004). The 10 deadly sins of information security management. Computers & Security, 23(5): 371-376.

Wang Qiang qiang. (2019). Analysis on Application of Firewall-based Technology in Computer Security Construction [J] of China Digital World, 2019 (08): 244.

Y. Xu and X. Xie. (2008). "Extending rubin logic for electronic commerce protocols," in Proceedings of the 2nd International Conference on Anti-counterfeiting, Security and Identification (ASID ’08), pp. 448–451, Guiyang, China, August 2008.

Zhong R. and Xiang F. (2012).” A cost aware backup strategy in hybrid clouds”, Proceedings - 2012 3rd IEEE International Conference on Network Infrastructure and Digital Content, IC-NIDC 2012, Beijing, 2012, pp.256-260.

Z. Shao. (2008). “Certificate-based fair exchange protocol of signatures from pairings,” Computer Networks, vol. 52, no. 16, pp. 3075–3084, 2008.