ISRG Journal of Arts, Humanities and Social Sciences (ISRGJAHSS)

ISRG PUBLISHERS
Abbreviated Key Title: ISRG J Arts Humanit Soc Sci
ISSN: 2583-7672 (Online)
Journal homepage: https://isrgpublishers.com/isrgjahss
Volume – III Issue-I (January- February) 2025
Frequency: Bimonthly

APPLICATION OF DATA SECURITY IN ORGANIZATIONS WITH REFERENCE TO BANGALORE

Ms. Sahana Suresh G[1*], Ms. Sachana, C[2], Ms. Ramya K[3], Dr. T. Vetrivel[4], Dr.R.Satheeshkumar[5]

[1]Office Administrator, Surana College-Autonomous, Kengeri Campus, KST, Bangalore, Karnataka.

[2]Research Scholar, Institute of Management Studies, Davangere University, Davangere, Karnataka.

[3]Student, MBA 2023-2025, Surana College-Autonomous, Kengeri Campus, KST, Bangalore, Karnataka.

[4]Professor and Head, Department of Management Studies, Velalar College of Engineering and Technology, Erode, Tamilnadu, India.

[5]Professor, Department of M.B.A & Research Centre, Surana College-Autonomous, Kengeri Campus, KST, Bangalore

| **Received:** 12.02.2025 | **Accepted:** 15.02.2025 | **Published:** 20.02.2025

***Corresponding author:** Ms. Sahana Suresh G

Office Administrator, Surana College-Autonomous, Kengeri Campus, KST, Bangalore, Karnataka.

Abstract

This paper presents the application of data security in organizations, emphasizing its significance in the digital age. The introduction establishes data as a core organizational asset, in danger to various threats. To address these vulnerabilities, the methodology section outlines a comprehensive framework encompassing Access Controls, Data Encryption, Data Loss Prevention (DLP), Employee Training, Backup and Recovery, Security Software.

Results section is envisioned to present the findings from implementing above outlined methodologies and the discussion section would then analyse these results, exploring the impact of the implemented data security measures. It would delve into the effectiveness of the chosen methodology in achieving its objectives, identify potential areas for improvement, and discuss the broader implications for organizational data security practices.

Findings section includes metrics demonstrating reduced security incidents, improved data access, control effectiveness, or enhanced employee awareness of data security practices. In conclusion, this paper aims to provide a comprehensive overview of data security application in organizations. By presenting a multifaceted methodology, analysing its results, and fostering discussion, this work intends to contribute valuable insights to the ongoing pursuit of robust data protection within organizations.

Keywords: *Data Security, Data Loss Prevention (DLP), Data Recovery, Security Software.*

DOI: 10.5281/zenodo.14898083

1. INTRODUCTION

DATA is Digital Authoring Technology Advancement. Data is a collection of information gathered by observations, measurements, research or analysis. They may consist of facts, numbers, names, figures or even description of things. Data is essential to an organization in today's digital environment. It includes every type of data, including employee and customer information, financial records, and intellectual property.

Data security is the process of safeguarding digital information throughout its entire life cycle to protect it from corruption, theft, or unauthorized access. It covers everything—hardware, software, storage devices, and user devices; access and administrative controls; and organizations' policies and procedures.

The four elements of Data security are: Confidentiality, Integrity, Authenticity, and Availability. The key principles of data security are Lawfulness, fairness and transparency. Purpose limitation. Data minimisation. Accuracy. Data security controls encompass an array of cybersecurity measures taken to protect an organization's data. They include the mechanisms, procedures, policies, and governance strategies to prevent and detect security incidents and data breaches.

Protection from cyberattacks: Sensitive data is always in danger of being stolen or exploited by cybercriminals. Robust data security protocols can significantly impede the success of potential attackers.

Respect for regulations: A lot of sectors have laws dictating how information needs to be safeguarded. Heavy fines and harm to one's reputation may arise from breaking these rules.

Preserving client trust: Customer loyalty and trust can be damaged by data breaches. Establishing trust with clients can be achieved by enterprises through their dedication to data security.

Data security is not a one-time fix. It's an ongoing process that requires a comprehensive strategy that incorporates people, processes, and technology. We'll explore these aspects in more detail in future conversations.

2. THEORETICAL BACKGROUND OF THE STUDY

Data Security: Data security is the process of safeguarding digital information throughout its entire life cycle to protect it from corruption, theft, or unauthorized access. It covers everything—hardware, software, storage devices, and user devices; access and administrative controls; and organizations' policies and procedures.

Data Loss Prevention: Data Loss Prevention is a cybersecurity solution that detects and prevents data breaches.

Data Recovery: Data recovery is the process of retrieving lost, deleted, or corrupted files from a storage device.

Types of Data Security

Organizations can use a wide range of **data security** types to safeguard their data, devices, networks, systems, and users. Some of the most common types of data security, which organizations should look to combine to ensure they have the best possible strategy, include:

Encryption, Data encryption, Data Erasure, Data Masking, Data Resiliency, Biggest Data Security Risks, Accidental Data Exposure, Phishing Attacks, Insider Threats, Malware Ransomware.

MOST POPULAR DATA SECURITY:

- **Bitdefender, Norton 360, McAfee Total Protection, TotalAV and Trend Micro**

3. LITERATURE REVIEW

Karim Abouelmehdi, Abderrahim Beni-Hssane, Hayat Khaloufi, Mostafa Saadi (2017) found that the research is highly diverse enabled data generating technologies in medical, biomedical and healthcare fields and the growing availability of data at the central location that can be used in need of any organization from pharmaceutical manufacturers to health insurance companies to hospitals have primarily make healthcare organizations and all its sub-sectors in face of a flood of big data as never before experienced.

Lakshmi Nivas Nalla, Vijay Mallik Reddy (2023) found that the research is Data privacy and security are paramount concerns in e-commerce, where vast amounts of sensitive customer information are collected, processed, and stored. This paper examines the challenges and opportunities associated with data privacy and security in ecommerce and explore the role of modern database technologies in addressing these concerns.

Oluwatoyin Ajoke Farayola1 & Oluwabukunmi Latifat Olorunfemi, & Philip Olaseni Shoetan (2024) found that the research is interconnected in today's digital world, data privacy and security have emerged as paramount concerns for individuals, organizations, and governments alike. This review provides a comprehensive review of techniques and challenges surrounding data privacy and security in information technology (IT) systems.

Adedoyin Tolulope Oyewole1, Bisola Beatrice Oguejiofor, Nkechi Emmanuella Eneh, Chidiogo Uzoamaka Akpuokwe, & Seun Solomon Bakare (2024) found that the research is based on the digital transformation of financial services is both a boon and a battleground, this paper meticulously navigates the intricate relationship between Financial Technology (FinTech) and the evolving landscape of data privacy laws.

Dolantina Hyka, Alma Hyra , Fatmir Basholli , Besjana Mema, Albina Basholli (2023) found that the research is concerned in today's digital era, especially for public and private administrations that handle sensitive information. This research paper aims to investigate the role of cryptographic techniques in enhancing data security within the context of public and private administration.

Aized Amin Soofi, M. Irfan Khan, Fazal-e-Amin (2014), Cloud computing is an Internet-based computing and next stage in evolution of the internet. It has received significant attention in recent years, but security issue is one of the major inhibitors in decreasing the growth of cloud computing. Data Security concerns arising because both user data and program are in provider premises.

Rajab Muhammad Ssemwogerere, Balyejusa Gusite (2022) found that the research is based on Data privacy which is an intricate job and is becoming a key area of research as far as cloud technologies are concerned. There are numerous ways this data can be protected from unauthorized users.

Vamsikrishna Bandari (2023) This research aims to investigate the types of data security measures commonly used by enterprises to

DOI: 10.5281/zenodo.14898083

safeguard sensitive data and their effectiveness in preventing security incidents. Overall, this research provides insights into the effectiveness of different data security measures, the variations in data security practices across industries and organization types, and the common causes of data breaches in enterprises.

Nathanael David Christian Barus, Natasha Fedora Barus (2024), This literature review explores the evolution of data security algorithms tailored explicitly for the Big Data landscape, aiming to address the increasing demand for robust security solutions capable of handling the unique challenges posed by the massive scale and complexity of data.

Ishu Gupta, et .al (2022), Many researchers, academia, government sectors, and business enterprises are adopting the cloud environment due to the least upfront capital investment, maximum scalability, and several other features of it. This article presents a comparative and systematic study, and in-depth analysis of leading techniques for secure sharing and protecting the data in the cloud environment.

Ricardo Raimundo and Alberico Rosário (2021), This paper aims at identifying research trends in the field through a systematic bibliometric literature review (LRSB) of research on AI and system security.

3.1. Objectives of the Study

1. To assess the data security awareness level and practices among organizations in Bangalore.
2. To examine the relationship between organizational size, industry sector, and the level of data security maturity in Bangalore-based organizations.
3. To evaluate the effectiveness of data security training and awareness programs in Bangalore.
4. To identify the most common data security challenges faced by organizations in Bangalore and their corresponding mitigation strategies.
5. To explore the role of technology in enhancing data security practices in Bangalore-based organizations.

3.2. Limitations of the study

1. Study is subject to respondents' bias.
2. Developing accurate and reliable measures for data security awareness, practices, and maturity can be challenging.
3. Findings of the study might not be directly applicable to all organizations due to differences in size, industry, and risk profile.

4. DATA ANALYSIS

Table no. 4.1 - Demographic Profile of the Respondents

Sl.No	Gender	No. of Respondent	Percentage
1	FEMALE	54	54
2	MALE	46	46
	Total	100	100
Sl.No	**Employment Status**	**No. of Respondent**	**Percentage**
1	Full-Time	76	76
2	Part-Time	5	5
3	Seeking opportunities currently	19	19
	Total	100	100
Sl.No	**Age**	**No. of Respondent**	**Percentage**
1	Up to 25 years	51	51
2	26-30 years	15	15
3	31-35 years	16	16
4	36-40 years	3	3
5	Over 40 years	15	15
	Total	100	100
Sl.No	**Academic Qualification**	**No. of Respondent**	**Percentage**
1	School Level	0	0
2	Undergraduate	24	24
3	Postgraduate	76	76
4	Professional	0	0
5	Others	0	0
	Total	100	100
Sl.No	**Monthly Income (Amount in Rupee)**	**No. of Respondent**	**Percentage**
1	Below Rs.25000	37	37
2	Rs.25001-45000	31	31
3	Rs.45001-65000	13	13
4	Rs.65001-85001	8	8
5	Above 85000	11	11
Total		100	100
Sl.No	**Present Employment Role**	**No. of Respondent**	**Percentage**
1	Team Lead	13	13
2	Digital Lead	0	0
3	Operation Lead	2	2
4	Front Line Executive	3	3
5	Software Engineer	5	5
6	Business Development	6	6

DOI: 10.5281/zenodo.14898083

	Executive		
7	Trainee	4	4
8	Software Design Testing Executive	0	0
9	Human Resource Executive	4	4
10	Other Role	63	63
	Total	100	100

Source of Data: Primary Data

Interpretation:
The above demographic analysis from the study implies that there were 76% full time employees, 5% were part-time employees and 19% were seeking job opportunities. It is found that 51% of respondents belong to the age group below 25 years, 15% belongs to the age groups between 26 to 30 Years, 16% belongs to the age groups between 31 to 35 Years, 3% belongs to the age groups between 36 to 40 years and 15% belongs to the age group above 40 years.

The study indicated that 24% respondents were undergraduates, 76% respondents were postgraduates. It is found that 37% of respondents have a monthly income below Rs.25,000/-, 31% of them have a monthly income between Rs.25,001 to Rs. 45,000/-, 13% of them have a monthly income between Rs. 45,001 to 65,000/-, 8% of them have a monthly income between Rs.65,001 to 85,000/- and 11% of them have a monthly income lies above Rs. 85,000/-.

The study depicts that 13% of them were Team Leads, 2% of them were Operation Head, 3% of them were Front Line Executive, 5% of them were Software Engineers, 6% of them were Business Development Executive, 4% of them were Trainee and 4% of them were Human Resource Executive.

Table No. 4.2 - Awareness Level on Data Security

Sl. No	Employees' awareness on importance of Data Security.	No. of Respondent	Percentage
1	Regular training sessions	46	46
2	Email reminders	28	28
3	Posters and banners	1	1
4	Intranet resources	11	11
5	None of the above	14	14
	Total	100	100

Source of Data: Primary Data

Interpretation:
The above chart implies the awareness level on Data Security among the employees in which 46% of the respondents have regular training sessions, 28% of them would be getting E-mail reminders, 1% of them were having the awareness through posters and banners, 11% of them through Intranet resources and 14% of them have no clue about the data security.

Table No. 4.3 – Training methods used by the Organization to the employees on Data Security.

Sl. No	Training methods used by the Organization to the employees on Data Security.	No. of Respondent	Percentage
1	Online courses	29	29
2	In-person workshops	33	33
3	Webinars	17	17
4	Self-study materials	11	11
5	None of the above	10	10
	Total	100	100

Source of Data: Primary Data

Interpretation:

The study found that 29% of the respondents have been trained by Online courses, 33% of them were having the training through In-person workshops, 17% of them through webinars, 11% of them through self-study materials and 10% of them were excluded.

Table No. 4.4 – Update towards Data Security Policies by the Organisation to their Employees.

Sl. No	Update towards Data Security Policies by the Organisation to their Employees.	No. of Respondent	Percentage
1	Monthly	30	30
2	Quarterly	27	27
3	Annually	8	8
4	As needed	29	29
5	Never	6	6
	Total	100	100

Source of Data: Primary Data

Interpretation:
The study depicts that 30% of the Data Security Policies were updated on monthly basis, 27% were updated on quarterly basis, 8% have been informed annually, 29% were given information whenever required and 6% were non updated.

Table No. 4.5 – Roles played by the Organization in defining Data Security Plan.

Sl. No	Roles played by the Organization in defining Data Security Plan.	No. of Respondent	Percentage
1	Data Security Officer	29	29
2	IT Security Manager	28	28
3	Incident Response Team	11	11
4	Data Privacy Officer	10	10
5	None of the above	22	22
	Total	100	100

Source of Data: Primary Data

DOI: 10.5281/zenodo.14898083

Interpretation:

From the study, it is evident that 29% of the respondents were the Data Security Officer, 28% of the respondents were IT Security Manager, 11% of them were Incident Response Team, 10% of them were Data Privacy Officer who plays a role in the organization in defining Data Security Plan and 22% were not involved.

Table No. 4.6 – Employees' awareness towards the risk of Data breaches.

Sl. No	Employees' awareness towards the risk of Data breaches.	No. of Respondent	Percentage
1	Financial loss	14	14
2	Legal consequences	33	33
3	Reputation damage	22	22
4	Operational disruption	17	17
5	None of the above	14	14
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is observed that 14% of the respondents were aware about the risk of data breaches – financial loss, 33% of them were known that would lead to legal consequences, 22% of them aware that it would damage reputation, 17% of them would know that lead to operational disruption and 14% of them were unaware.

Table No. 4.7 – Implementation of Data Security Measures

Sl. No	Implementation of Data Security Measures in the Organisation.	No. of Respondent	Percentage
1	Firewalls	27	27
2	Antivirus software	18	18
3	Data encryption	35	35
4	Intrusion detection systems	14	14
5	None of the above	6	6
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is found that 27% of the respondents would opt for firewalls as a Data Security measures, 18% would rely on the antivirus software, 35% of them would choose data encryption, 14% would opt for Intrusion Detection Systems and 6% of them would not be opting for any of the Data Security measures.

Table No. 4.8 - Data Encryption managed by the Organisation

Sl. No	Data Encryption managed by the Organisation.	No. of Respondent	Percentage
1	Encrypted emails	24	24
2	Encrypted databases	27	27
3	Encrypted file storage	23	23
4	Encrypted backups	8	8
5	None of the above	18	18
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is evident that in an organization, 24% were encrypted emails, 27% were encrypted databases, 23% were encrypted file storage, 8% were encrypted backups and 18% were not encrypted.

Table 4.9 - Conduct of Data Security Audits.

Sl. No	Conducts of Data Security Audits.	No. of Respondent	Percentage
1	Monthly	19	19
2	Quarterly	33	33
3	Annually	12	12
4	As needed	28	28
5	Never	8	8
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is found that the organizations emphasis on the Data Security Audit in which 19% respondents feel it will be conducted monthly, 33% feels it will be conducted quarterly, 12% feels it will be conducted annually, 28% feels it will be conducted when it is required and 8% feels it will not be conducted at all.

Table 4.10 - Authentication methods used for accessing sensitive data.

Sl. No	Authentication methods used for accessing sensitive data.	No. of Respondent	Percentage
1	Passwords	24	24
2	Multi-factor authentication (MFA)	49	49
3	Biometric authentication	14	14
4	Smart cards	4	4
5	None of the above	9	9
	Total	100	100

Source of Data: Primary Data

DOI: 10.5281/zenodo.14898083

Interpretation:

It is depicted in the chart above pertaining to the authentication methods used for accessing sensitive data in which 24% respondents use passwords, 49% of them use multi-factor authentication, 14% of them relies on biometric authentication, 4% would go with smart cards and 9% were not using any authentication mode to safeguard the sensitive data.

Table 4.11 – Access Controls used for Confidential Data

Sl. No	Access Controls used for Confidential Data.	No. of Respondent	Percentage
1	Role-based access	33	33
2	Mandatory access reviews	25	25
3	User activity monitoring	25	25
4	Data masking	4	4
5	None of the above	13	13
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is inferred that 33% of the respondents would take for Role-based access, 25% of them would feel mandatory access reviews, 25% of them would go with user activity monitoring, 4% would take it for data masking and 13% would not opt for any access controls to safeguard the confidential data.

Table 4.12 – Data Breach Response Management

Sl. No	Components included in Organisation's data breach response plan.	No. of Respondent	Percentage
1	Incident response team	19	19
2	Communication plan	19	19
3	Data recovery procedures	28	28
4	Legal and regulatory compliance steps	21	21
5	None of the above	13	13
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is observed that Data Breach Response Management included with 19% respondents go with the Incident Response Team, 19% feels communication plan is also one components of the Data breach response plan, 28% respondents would go with Data Recovery procedure, 21% would opt for legal and regulatory compliance steps and 13% respondents felt the organizations have other components except the above-mentioned components.

Table 4.13 - Employees training towards the response of data breach.

Sl. No	Employees training towards the response of data breach.	No. of Respondent	Percentage
1	Simulation exercises	6	6
2	Step-by-step guides	44	44
3	Online courses	18	18
4	In-person workshops	17	17
5	None of the above	15	15
	Total	100	100

Source of Data: Primary Data

Interpretation:

The above chart depicts that 6% of the respondents feels that the simulation exercises is one of the employee's training towards the response of data breach, 44% of them would opt for step-by-step guides that would work, 18% of them go with online courses, 17% of respondents for In-person workshops and 15% would feel that there are other training that would help them for the response of data breach.

Table 4.14 – The incident response team for data breaches.

Sl. No	The incident response team for data breaches.	No. of Respondent	Percentage
1	IT staff	34	34
2	Legal team	30	30
3	Communication team	18	18
4	Executive leadership	7	7
5	None of the above	11	11
	Total	100	100

Source of Data: Primary Data

Interpretation:

In an organization, the respondents felt that if the data get breached, 34% will be of IT staff who will be handling the data, 30% would be legal team, 18% would be the communication team, 7% would be the executive team and 11% will go unaddressed.

Table 4.15 – Updating of data breach plan

Sl. No	Updating of data breach plan.	No. of Respondent	Percentage
1	Monthly	18	18
2	Quarterly	36	36
3	Annually	11	11
4	As needed	29	29
5	Never	6	6
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is evident that 18% respondents felt that the updating of data breach plan have been conducted monthly, 36% respondents felt it was done quarterly, 11% of them felt it was done annually, 29% respondents felt it will be done when it is required and 6% respondents felt the data breach plan is not updated.

DOI: 10.5281/zenodo.14898083

Table 4.16 - Reporting of data breaches.

Sl. No	Reporting of data breaches.	No. of Respondent	Percentage
1	Internal security team	43	43
2	Local authorities	14	14
3	Regulatory bodies	22	22
4	Affected customers/clients	13	13
5	None of the above	8	8
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is crucial to report the data breaches, 43% respondents felt that it will be reported to Internal Security team, 14% respondents felt that the data breach will be reported to local authorities, 22% respondents felt that it will be reported to regulatory bodies, 13% respondents felt that it will raised by affected customers/clients and 8% felt that breaches will be reported other than the above mentioned security bodies.

Table 4.17 - Data Security Polices

Sl. No	Regulations used by the Organisation to comply Data Protection.	No. of Respondent	Percentage
1	GDPR	15	15
2	HIPAA	17	17
3	CCPA	17	17
4	Local data protection laws	34	34
5	None of the above	17	17
	Total	100	100

Source of Data: Primary Data

Interpretation:

There were 15% respondents' inferences that GDPR (General Data Protection Regulation) is used by the organization to comply data protection, 17% respondents felt with HIPAA (Health Insurance Portability and Accountability Act), 17% felt that CCPA (California Consumer Privacy Act) regulation to comply data protection, 34% felt that Local Data Protection laws is sufficient to comply and 17% of them felt that there are other regulation act for data protection.

Table 4.18 – Data Retention Policies placed in Organisation.

Sl. No	Data retention policies placed in Organisation.	No. of Respondent	Percentage
1	Data deletion after a certain period	23	23
2	Archived data storage	15	15
3	Regular review of stored data	35	35
4	Data minimization practices	13	13
5	None of the above	14	14
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is found that the organization will take necessary measures to retain the data through certain policies in which 23% respondents felt that data deletion after a certain period, 15% of respondents felt that archived data storage would be an option, 35% respondents felt that regular review of stored data would be an another option, 13% respondents felt that the organization has to follow data minimization practices and 14% respondents would prefer other options as a retention policies excluding the above mentioned policies.

Table 4.19 - Employees update towards data security practices.

Sl. No	Employees update towards data security practices.	No. of Respondent	Percentage
1	Regular training sessions	37	37
2	Newsletters	16	16
3	Internet resources	13	13
4	Policy updates	21	21
5	None of the above	13	13
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is inferred that 37% of respondents perceived that regular training sessions would enable employees update towards data security practices, 16% respondents sensed that newsletter, 13% respondents felt that the employees would rely on internet sources, 21% of respondents perceived that the employees get an update through policy updates and 13% of respondents would suggest that employees would be getting updated towards data security practices through other modes expect the modes mentioned above.

Table 4.20 – Risk Assessments performed for Data Security

Sl. No	Risk Assessments performed for Data Security.	No. of Respondent	Percentage
1	Monthly	21	21
2	Quarterly	28	28
3	Annually	12	12
4	As needed	30	30
5	Never	9	9
	Total	100	100

Source of Data: Primary Data

DOI: 10.5281/zenodo.14898083

Interpretation:

In an organization, 21% respondents identified that the risk assessments performed for data security will be done on monthly basis, 28% respondents noticed that the assessment will be done on quarterly basis, 12% felt annually, 30% felt whenever it is required and 9% sensed that the risk assessment will not at all been conducted.

Table 4.21 – Accessibility of Data Security Policies to employees.

Sl. No	Accessibility of Data Security Policies to employees.	No. of Respondent	Percentage
1	Intranet portal	16	16
2	Employee handbook	20	20
3	Regular email updates	45	45
4	Physical copies in common areas	9	9
5	None of the above	10	10
	Total	100	100

Source of Data: Primary Data

Interpretation:

In an organization, 16% respondents perceived that accessibility of data security policies to employees is through Intranet portal, 20% respondents felt that it will be done through employee handbook, 45% respondents sensed that it will be done through regular email updates, 9% respondents would felt that employees rely on physical copies in common areas and 10% respondents would felt that the employees would choose other option other than above mentioned options.

Table 4.22 – Cyber security tools used by the Organisation.

Sl. No	Cyber security tools used by the Organisation.	No. of Respondent	Percentage
1	Antivirus software	20	20
2	Firewall protection	36	36
3	Intrusion detection systems	17	17
4	Security information and event management (SIEM)	16	16
5	None of the above	11	11
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is inferred that in an organization, 20% of the respondents discerned that the employees would go for Antivirus software as a cyber-security tools, 36% of respondents identified that the employee uses firewall protection, 17% of respondents sensed that the employees use intrusion detection systems, 16% respondents felt that the employees opt for security information and event management (SIEM) as a cyber-security tools and 11% respondents felt that employees will choose other cyber security tools other than the above mentioned tools.

Table 4.23 – Frequency of software updates and patches applied.

Sl. No	Frequency of software updates and patches applied.	No. of Respondent	Percentage
1	Immediately upon release	29	29
2	Monthly	24	24
3	Quarterly	12	12
4	As needed	27	27
5	Never	8	8
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is evident that the organization would do regular software updates for the better productivity, in this study it is implied that 29% respondents identified that there will be an immediate update of software right next to the release, 24% respondents perceived that it will be done on monthly basis, 12% respondents felt that the updates will be taken care on quarterly basis, 27% respondents felt it will be done whenever it is required and 8% felt that the organization will not be updating software as well as for patches applied.

Table 4.24 - Performance of data backups.

Sl. No	Performance of data backups.	No. of Respondent	Percentage
1	On-site backups	14	14
2	Cloud backups	47	47
3	Off-site backups	8	8
4	Regular backup schedule	25	25
5	None of the above	6	6
	Total	100	100

Source of Data: Primary Data

Interpretation:

In an organization, 14% respondents perceived that the performance of data backups will be done On-site, 47% respondents inferred that it is through cloud backups, 8% respondents felt it will be through the Off-site backups, 25% respondents felt that it will be through regular backup schedule and 6% of respondents would felt that performance of data backups would be done through other data backups apart from the above mentioned.

Table 4.25 – Secure communication channels used for sensitive information.

Sl. No	Secure communication channels used for sensitive information.	No. of Respondent	Percentage
1	Encrypted emails	24	24

DOI: 10.5281/zenodo.14898083

2	Secure messaging apps	21	21
3	Virtual private networks (VPNs)	38	38
4	Encrypted phone calls	8	8
5	None of the above	9	9
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is found that the organization requires a proper and secure communication channels for sensitive information in which 24% respondents would opt for encrypted emails would be safe, 21% respondents chose secure messaging apps, 38% respondents felt that Virtual Private Networks (VPNs) , 8% would felt that encrypted phone calls would be the secured communication channels and 9% respondents have a different choice apart from the sated above.

Table 4.26 – Measurement of data security standards by the Organisation.

Sl. No	Measurement of data security standards by the Organisation.	No. of Respondent	Percentage
1	Vendor assessments	10	10
2	Compliance certifications	29	29
3	Regular security audits	24	24
4	Service level agreements (SLAs)	26	26
5	None of the above	11	11
	Total	100	100

Source of Data: Primary Data

Interpretation:

In the organization, measurement of Data security standards will be conducted out of which 10% respondents felt it is from Vendor assessments, 29% respondents felt that it is from compliance certifications, 24% respondents felt as it is through regular security audits, 26% respondents felt it will be through Service Level agreements (SLAs) and 11% respondents would felt that there are other measurements of data security apart from the above.

Table 4.27 – Employees awareness on the importance of data security.

Sl. No	Employees' awareness on the importance of data security.	No. of Respondent	Percentage
1	Strongly Agree	43	43
2	Agree	33	33
3	Neutral	19	19
4	Disagree	1	1
5	Strongly Disagree	4	4
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is observed that 43% respondents strongly agree that employees are aware about the importance of data security, 33% respondents agreed, 19% respondents remain neutral, 1% respondents disagreed and 4% respondents strongly disagreed that employees are not aware about the data security.

Table 4.28 – Dedicative performance by the team towards data security in the organisation.

Sl. No	Dedicative performance by the team towards data security in the organisation.	No. of Respondent	Percentage
1	Strongly Agree	32	32
2	Agree	36	36
3	Neutral	26	26
4	Disagree	3	3
5	Strongly Disagree	3	3
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is evident that 32% respondents strongly agreed that dedicative performance is considered by the team towards data security, 36% agreed for the same, 26% respondents remain neutral, 3% respondents disagreed for that and 3% strongly disagree about the performance track maintained by the organizations with respect to the data security.

Table 4.29 – Risk assessments for data security by the Organisation towards their performance.

Sl. No	Risk assessments for data security by the Organisation towards their performance.	No. of Respondent	Percentage
1	Strongly Agree	33	33
2	Agree	30	30
3	Neutral	31	31
4	Disagree	2	2
5	Strongly Disagree	4	4
	Total	100	100

Source of Data: Primary Data

DOI: 10.5281/zenodo.14898083

Interpretation:

It is inferred that 33% respondents strongly agree that organizations are undergoing the risk assessments for data security which resulted in their performance, 30% respondents agreed for the same, 31% respondents remain neutral, 2% and 4% disagreed and strongly disagree respectively that the organization is not considering risk assessment factors for their performance up gradation.

Table 4.30 – Cloud services used by the organization adhere to strict data security standards.

Sl. No	Cloud services used by the organization adhere to strict data security standards.	No. of Respondent	Percentage
1	Strongly Agree	28	28
2	Agree	37	37
3	Neutral	29	29
4	Disagree	3	3
5	Strongly Disagree	3	3
	Total	100	100

Source of Data: Primary Data

Interpretation:

It is observed that 28% respondents strongly agreed that the organizations used the cloud services which will adhere to the strict data security standards, 37% agreed for the same, 29% respondents remain neutral, 3% disagree and 3% strongly disagreed that the organization will not go for an authenticated cloud service.

FINDINGS, SUGGESTIONS AND CONCLUSIONS

Findings of the Study

1. In the study, the employees have the awareness of the data security through regular training sessions (46%), E-mail reminders (28%), Posters and Banners (1%), Intranet resources (11%). Hence, employees knew the importance of data security.
2. There are several modes to train the employees towards data security in which online training is of 29%, In-person workshops are of 33%, webinars are of 17%, self-study materials is of 11%.
3. Data security updates must take place in an organization on regular basis, the respondents felt that 30% monthly, 27% quarterly, 8% annually.
4. Employees awareness towards the risk of data breaches have the following consequences of which 14% is of financial loss, 33% is of legal consequences, 22% is of reputation damage, 17% is of operational disruption.
5. From the study, it is implied that the organizations have implemented data security measures of which 27% goes to firewalls, 18% antivirus software, 35% is to data encryption, 14% to the intrusion detection systems.
6. With respect to Data Breach Response Management, the organizations have taken numerous measures and training is being provided towards the response of data breach. In this study, the reporting of data breaches is being delegated in which respondents felt that 43% reported to Internal security team, 14% of it to local authorities, 22% of it to regulatory bodies and 13% of it to the affected customers/clients.
7. There are various regulations used by the organization to comply with data protection in which 15% belongs to General Data Protection Regulation, 17% belongs to Health Insurance Portability and Accountability Act, 17% belongs to Central Consumer Protection Authority and 34% belongs to Local Data Protection Laws.
8. In the organizations to communicate sensitive information there are various channels used of which respondents felt 24% is through encrypted emails, 21% is through secure messaging apps, 38% is through Virtual Private networks, 8% is through encrypted phone calls.
9. From the study, it is implied that employees are having awareness on the importance of data security as it is crucial in an organization to protect sensitive information from cyber threats, ensuring confidentiality, integrity, and availability. Strong security measures prevent financial losses, reputational damage, and legal consequences.
10. In the study, the risk assessment with respect to data security shows as highly given importance as it directly impact on the overall performance of the organization.

Suggestions:

Based on the findings, organizations should enhance data security awareness through diversified training methods, including online sessions, in-person workshops, and self-study materials. Regular security updates, preferably monthly or quarterly, should be implemented to ensure robust protection. Strengthening security infrastructure by increasing investments in firewalls, antivirus software, and data encryption is essential. Organizations should also streamline their data breach response by clearly defining reporting protocols and ensuring compliance with relevant data protection laws. Additionally, secure communication channels such as encrypted emails and VPNs should be prioritized to safeguard sensitive information.

Conclusions

Based on the analysis and interpretation, it is evident that organizations have made significant strides in implementing data security measures and raising awareness among employees. The study highlights the importance of regular training sessions, various security tools, and compliance with data protection regulations to safeguard sensitive information. Despite these efforts, challenges such as inconsistent policy updates, varying levels of employee awareness, and the need for more advanced security technologies persist. To enhance data security, organizations must prioritize periodic risk assessments, strengthen breach response mechanisms, and encourage a culture of security consciousness across all levels. By doing so, businesses can mitigate risks and ensure the integrity, confidentiality, and availability of critical data.

Bibliography

1. Adedoyin Tolulope Oyewole1, B. B. (2024). Adedoyin Tolulope Oyewole1, Bisola Beatrice Oguejiofor2, Nkechi Emmanuella Eneh3,. 23.

DOI: 10.5281/zenodo.14898083

2. Aized Amin Soofi, M. I.-e.-A. (2014). A Review on Data Security in Cloud Computing. 9.
3. Bandari, V. (2023). Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types. 11.
4. Dolantina Hyka *1, A. H. (2023). Data security in public and private administration: Challenges, trends, and effective.
5. Ishu Gupta 1, (. I. (2022). Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis and Future Directions. 31.
6. Karim Abouelmehdi, A. B.-H. (2017). Big data security and privacy in healthcare: A Review. ScienceDirect, 8.
7. Lakshmi Nivas Nalla, 2. M. (2023). Lakshmi Nivas Nalla, 2Vijay Mallik Reddy. 16.
8. Nathanael David Christian Barus, N. F. (2024). Natasha Fedora Barus. 12.
9. Oluwatoyin Ajoke Farayola1 & Oluwabukunmi Latifat Olorunfemi2, &. P. (2024). Data Privacy And Security in IT: A Review.
10. Ricardo Raimundo 1 and Albérico Rosário 2. (2021). The Impact of Artificial Intelligence on Data System Security: A Literature Review. 19.
11. Umair Khadam, 1. M. (2020). Text Data Security and Privacy in the Internet of Things: Threats, Challenges, and Future Directions. 15.

DOI: 10.5281/zenodo.14898083