iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 Issue: XII Month of publication: Dec 2024

DOI:

Cyber Security Role in Information Technology

K. Neha[1], Mrs. N. Hima Bindu[2]
[1]MBA II Year, [2]Asst. Professor, Sridevi Women's Engineering College, Hyderabad

Abstract: Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against the unauthorised exploitation of systems, networks, and technologies. Cyber security plays a significant role in field of information Technology. Enhancing security for Information has become one of the biggest challenges in the present day. Focussing on how advancements in Technology both necessities and enable enhanced security measures, The research highlights key technological developments, cloud computing, inter of things, supply chain risks, incidents response and recovery. The data was collected through Questionnaires from 50 IT professionals, these findings provide majority of employees consider cybersecurity a top priority.it emphasized the importance of proactive measures cybersecurity awareness and demonstrate that organisation with robust cybersecurity Measures.

Keywords: Cybersecurity, Information Technology, Cyber-attacks, Data protection, Cloud computing, Internet of Things (IoT), Supply chain risks, Cybersecurity awareness

I. INTRODUCTION

Cybersecurity has become the cornerstone of IT in today's digital world. Data is both an important asset and a vulnerability. Cybersecurity is a fundamental component of IT in the modern digital landscape. Where data is of enormous value and poses potential risks. In an increasingly digitally dependent world, businesses, governments and individuals Face increasing cyber threats due to reliance on interconnected devices and digital platforms. Cybersecurity is the practice of protecting systems, networks, and data from digital attacks. It plays an important role in maintaining its integrity. Confidentiality and the availability of information in this area, the impact of cyber-attacks This includes strategies, tools, and protocols aimed at deterring unauthorized access. data breach and other cyber threats It has a wide and deep impact. Such events often lead to financial losses, legal consequences, loss of reputation. and disclosure of sensitive information in today's digital world Cyber security is closely integrated into the IT infrastructure. It plays an important role in protecting and increasing the security of information systems... Rapid advancement of technology in particular, the emergence of the Internet of Things (IoT), cloud computing and artificial intelligence It has expanded the scope of cyber security in IT. In the past few years ransomware, phishing, And the prevalence of Distributed Denial of Service (DDoS) has increased… and effects, cybercriminals are focusing on areas such as finance, healthcare, energy, and government services. This trend has resulted in access to personal information. Intellectual property and even illegal national security information with many claims the need for strong cybersecurity practices in the IT sector has therefore become a priority for both the public and private sectors. Cybersecurity plays a critical role within the area of IT that goes beyond safeguarding man or woman systems. It involves organising a secure environment that fosters user consider and operational efficiency.

II. REVIEW OF LITERATURE

Extension research has been promoted by the rise of cyberattacks has accelerated cybersecurity, highlighting risks from the early days of the Internet (Bellovin, 1993; Cheswick, 1994) and evolving to address modern threats like malware, phishing, and social engineering (Kaspersky, 2020; Verizon, 2020). As security challenges grow, significant research has been dedicated to Cloud security and risk mitigation (Subashini, 2011; CSA, 2020). AI and machine learning advancements now present promising tools for threat detection and response (Huang, 2019; Apprizes, 2020), although human factors like social engineering and errors remain notable vulnerabilities (Kirlappos, 2013; Parsons, 2017). Frameworks such as NIST's Cybersecurity Framework (2014) and Information Assurance models (CNSS, 2015) aid organizations in managing cybersecurity risks. However, challenges remain, including integrating cybersecurity into new technologies and standardizing measurement approaches. Future studies should address these gaps, particularly through AI-driven cybersecurity innovations, awareness strategies, and standardized security metrics.

III. OBJECTIVES

1) To study the current state of cybersecurity in information technology and identify potential threats and vulnerabilities**.**
2) To Analyse the role of cyber security to provide sensitive information and maintaining trust in technological system
3) To develop strategies for implementing cybersecurity awareness
4) To evaluate the effectiveness of existing cyber security measures

IV. RESEARCH METHODOLOGY

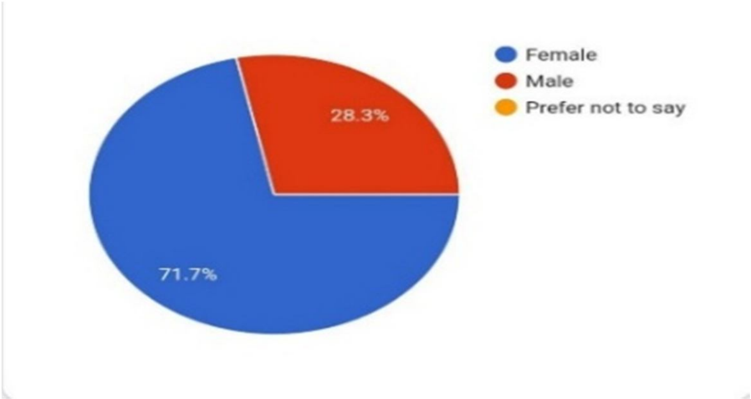
Research methodology refers to the systematic approach and procedures employed to conduct research and gather relevant information. It serves as a blueprint for researchers, outlining the steps they will take to answer specific research questions or achieve research objectives. This study employed a mixed-methods approach, utilizing both primary and secondary data sources to gather information. Primary data was collected through a questionnaire-based survey, which was administered to a sample of 50 participants. The questionnaire was designed to elicit responses on various aspects of cybersecurity and its role in information technology. Secondary data, on the other hand, was obtained from existing literature, including academic journals, books, and online resources. The sampling scheme employed was simple random sampling, which ensured that every member of the population had an equal chance of being selected. This approach helped to minimize bias and ensured that the sample was representative of the population. The sample size of 50 was deemed sufficient for this study, given the specific research objectives and the scope of the investigation. The questionnaire was administered through personal/direct contact, which allowed for clarification of any doubts or questions that respondents may have had. This approach also helped to ensure a high response rate, as respondents were more likely to participate in the survey when approached directly. Overall, the research methodology employed in this study was designed to provide a comprehensive understanding of the research topic, while also ensuring the reliability and validity of the findings.

V. DATA ANALYSIS

My study was strictly based on the primary data collection method by means of questionnaire dealing and involving the overall sample of 50 IT professionals**.**

1) *Gender*

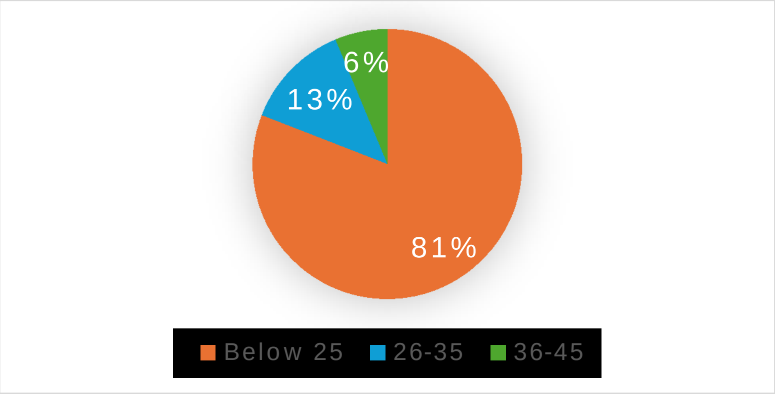
Gender	Percentage
Male	28.3%
Female	71.7%



INTERPRETATION: From above pie chart we can say that 71.7% are female and 28.3% Are male.

2) *Age*

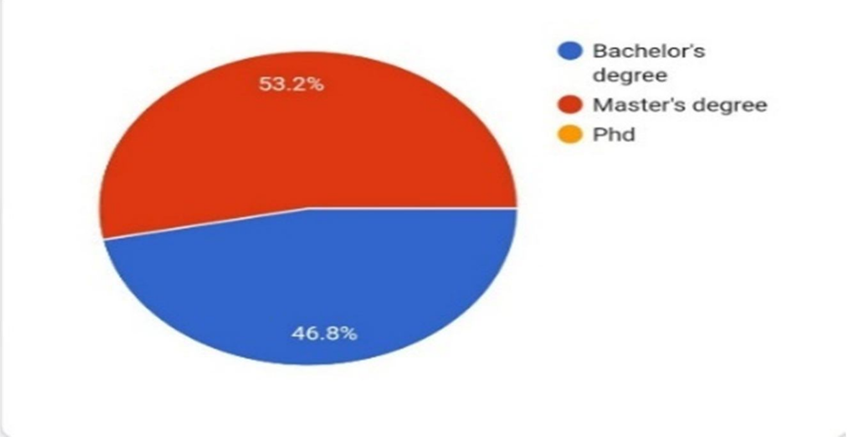
AGE	PERCENTAGE
Below 25	80.9%
26-35	12.8%
36-45	6.3%



INTERPRETATION: 80% employees are from age below 25 and 12% from 36 to 35 and 6 % from age 36 to 45.

3) *What is your education?*

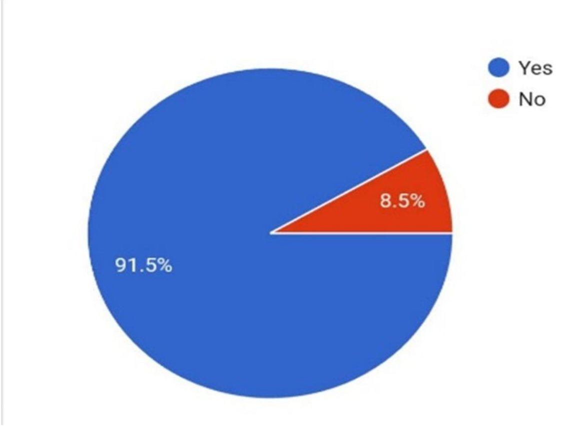
EDUCATION	PERCENTAGE
Bachelor's degree	46.8%
Master's degree	53.2%



INTERPRETATION: 46.8% professionals are with bachelor degree and 53.2% are with master's degree.

4) *Do you know about cybersecurity?*

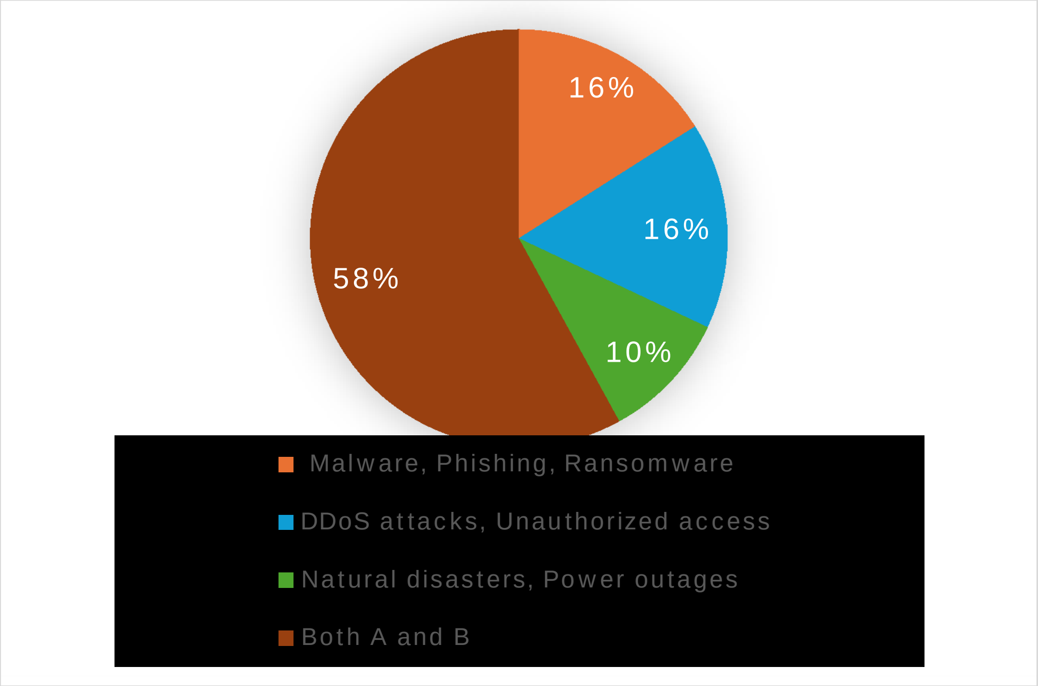
RESPONSE	PERCENTAGE
Yes	91.5%
No	8.5%



INTERPRETATION: 91.5% of the people know about cybersecurity. And remaining 8.5% of the people don't know about the Cybersecurity.

5) *Can you name some common cybersecurity threats that organizations face?*

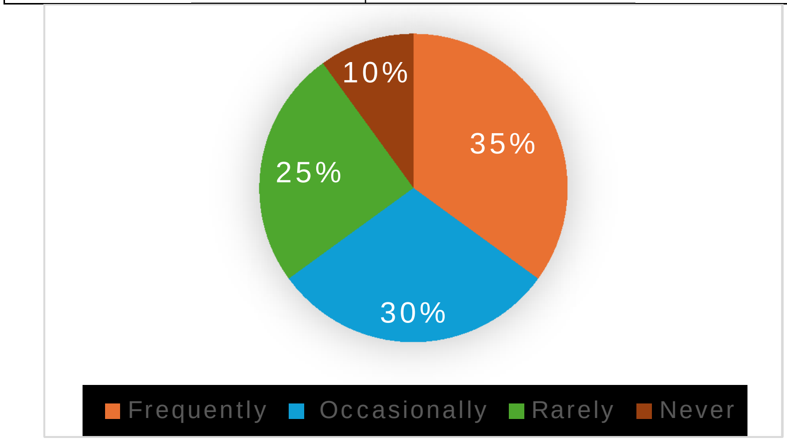
RESPONSE	PERCENTAGE
Malware, Phishing, Ransomware	16%
DDoS attacks, Unauthorized access	16%
Natural disasters, Power outages	10%
Both A and B	58%



INTERPRETATION: Most common cybersecurity that organizations face Malware, Phishing, Ransomware and DDoS attacks, Unauthorized access of 58%. And Natural disasters, Power outages is 10%.

6) How often do you encounter or hear about cybersecurity incidents in your organization or industry?

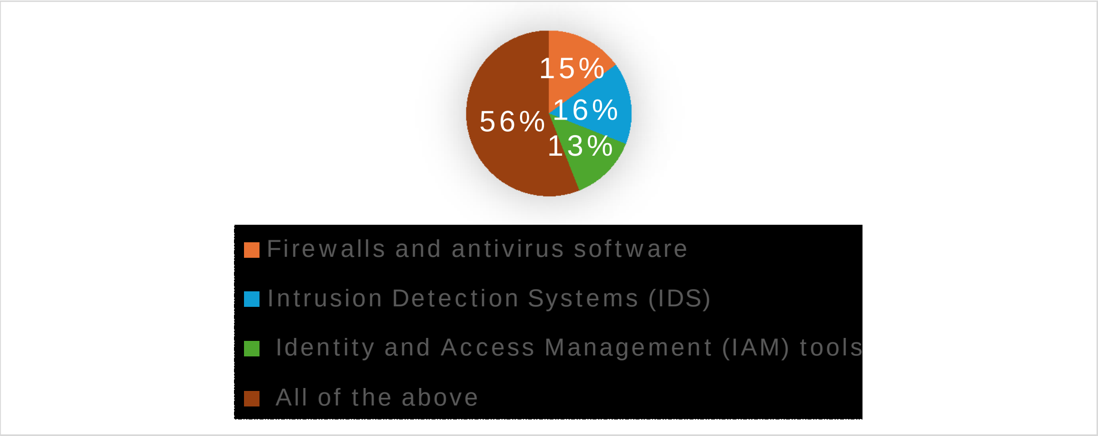
RESPONSE	PERCENTAGE
FREQUENTLY	35%
OCCASIONALLY	30%
RARELY	25%
NEVER	10%



INTERPRETATION: From the pie chart we can say that most of the organisations encounter or hear about cybersecurity incidents frequently is 35%, Occasionally 30%, rarely 25%, and never is 10%

7) What cybersecurity tools or frameworks does your organization use?

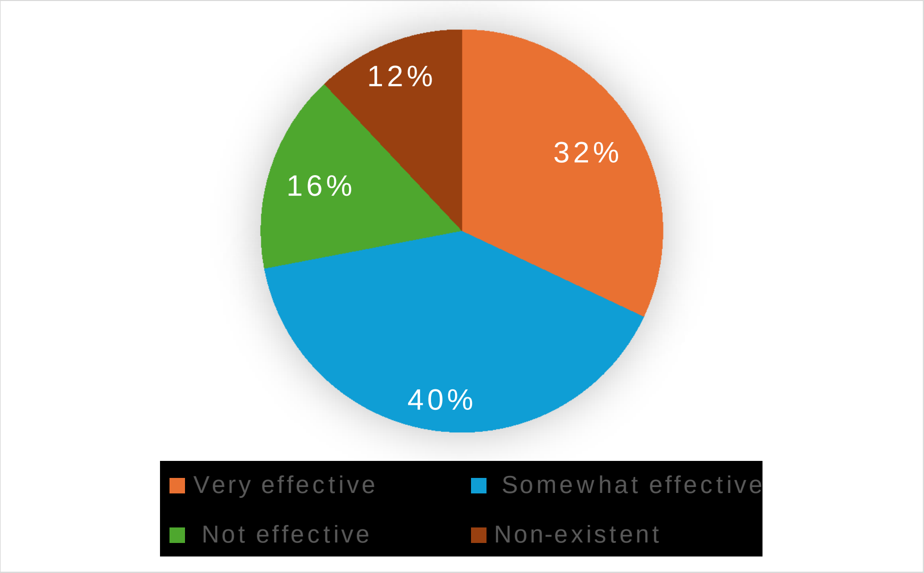
RESPONSE	PERCENTAGE
Firewalls and anti-virus software	15%
Intrusion detection system (IDS)	16%
Identify and access management (IAM) tools	13%
All of the above	56%



INTERPRETATION: From the above pie chart we can conclude that firewalls and antivirus software, intrustion detection systems(IDS),identity and access management(IAM) tools cybersecurity tools or frameworks does your organization use?

8) *How effective do you think your organization's cybersecurity awareness programs are?*

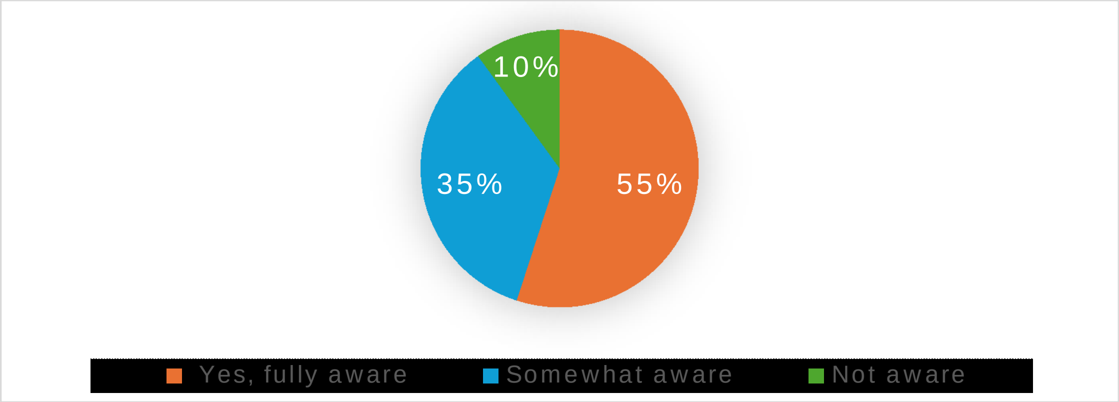
RESPONSE	PERCENTAGE
Very effective	32%
Somewhat effective	40%
Not effective	16%
Non-existent	12%



INTERPRETATION: From the above pie chart we can say that organization's cybersecurity awareness programs are somewhat effective.

9) *Are you familiar with the cybersecurity regulations your organization must comply with?*

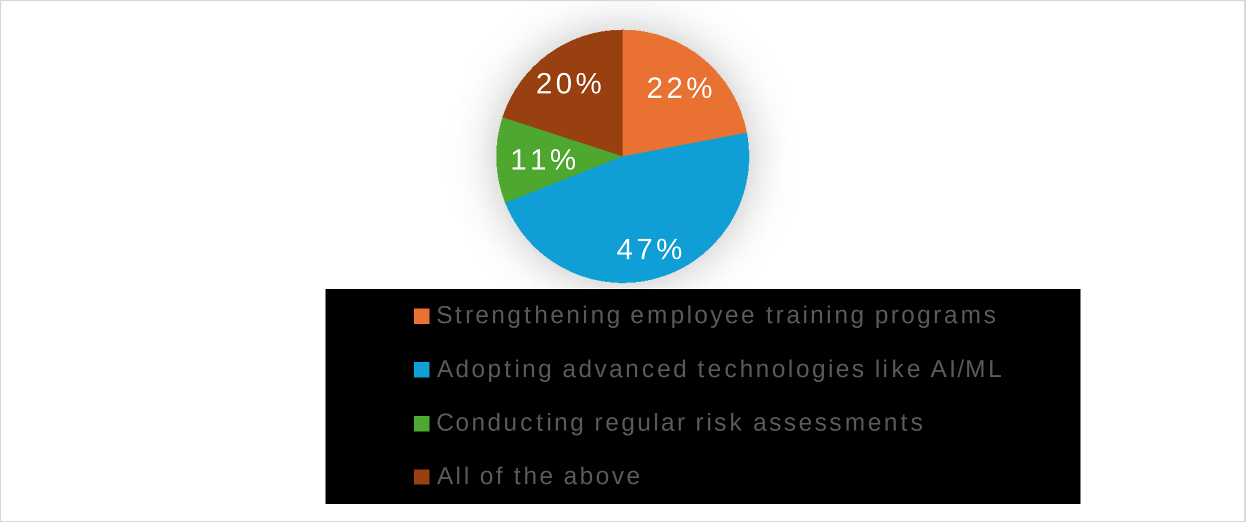
RESPONSE	PERCENTAGE
Yes, fully aware	55%
Somewhat aware	35%
Not aware	10%



INTERPRETATION: From the above pie chart we can say that organisations are familiar with the cybersecurity regulations

10) What cybersecurity measures would you recommend to improve IT security in your organization?

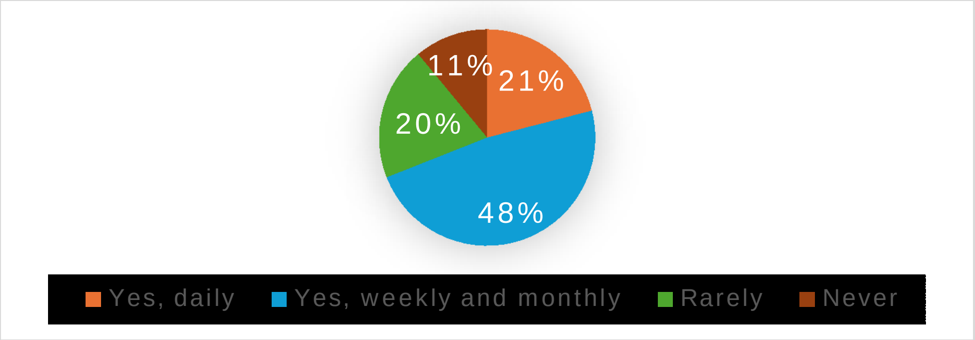
RESPONSE	PERCENTAGE
Strengthening employee training programs	22%
Adopting advanced technologies like AI/ML	47%
Conducting regular risk assessments	11%
All of the above	20%



INTERPRETATION: From the above pie chart we can say that adopting advanced technologies like AI/ML is the one of the cybersecurity measures would you recommend to improve IT security in your organization

11) Do you regularly back up your personal or professional data?

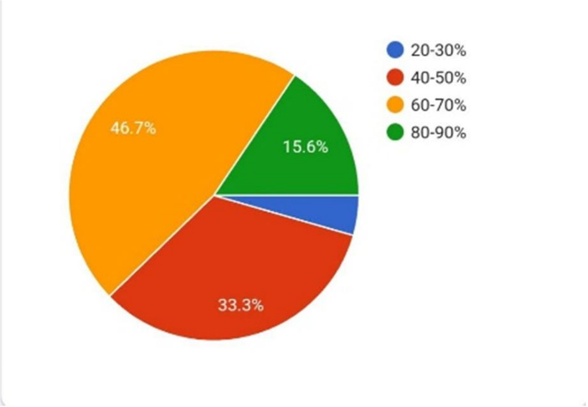
RESPONSE	PERCENTAGE
Yes, daily	21%
Yes, weekly and monthly	48%
Rarely	20%
Never	11%



INTERPRETATION: From the above pie chart, we can say that most of the organisations back up their personal or professional data weekly and monthly

12) What percentage of organization consider cybersecurity a top priority?

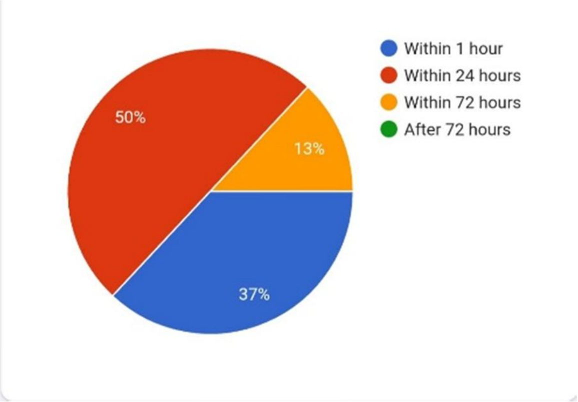
20-40%	4.4
40-50%	33.3%
60-70%	46.7%
80-90%	15.6%



Interpretation: 15.6% of organization consider cybersecurity a top priority (80-90%) 46.7% of organization consider cybersecurity (60-70%) 33.3% of organization consider cybersecurity (40-50%) 4.4 of the organisation consider cybersecurity (20-30%).

13) How quickly do organizations respond to cybersecurity incidents?

With in 1 hour	37%
With in 24 hours	50%
With in 72 hours	13%



Interpretation: 50% of the organizations respond to cybersecurity incidents with in 24 hours,37% of the organizations respond to cybersecurity incidents with in 1 hour and 13% of the organization respond to cybersecurity incidents within 72 hours.

VI. FINDINGS

1) Data was collected from 50 IT profesionals. A majority of the sample (71.7%) were female, while 28.3% were male.

2) Age Distribution: The workforce is predominantly young, with 80.9% under the age of 25, 12.8% between 26-35, and 6.3% between 36-45.

3) Most of the respondents (53.2%) held a master's degree, while 46.8% held a bachelor's degree.
4) The majority of the respondents (91.5%) were aware of cybersecurity, while 8.5% were not.
5) The most common cybersecurity threats faced by organizations were malware, phishing, ransomware, and DDoS attacks, with 58% of respondents selecting both options.
6) The majority of the respondents (56%) used a combination of firewalls and anti-virus software, intrusion detection systems (IDS), and identity and access management (IAM) tools.
7) The majority of the respondents (40%) believed that their organization's cybersecurity awareness programs were somewhat effective.
8) The majority of the respondents (35%) encountered or heard about cybersecurity incidents frequently, while 30% encountered them occasionally.
9) The majority of the respondents (50%) reported that their organizations responded to cybersecurity incidents within 24 hours.
10) The majority of the respondents (46.7%) believed that their organizations considered cybersecurity a top priority (60-70%).
11) The majority of the respondents (47%) recommended adopting advanced technologies like AI/ML to improve IT security.
12) The majority of the respondents (22%) recommended strengthening employee training programs to improve IT security.

VII. SUGGESTIONS

1) Implement regular training programs to educate employees about cybersecurity best practices, phishing attacks, and other common cyber threats.
2) Conduct awareness campaigns to educate employees about the importance of cybersecurity and the role they play in preventing cyber-attacks.
3) Implement Firewalls and Ensure that all systems and networks have firewalls and anti-virus software installed and regularly updated Implement IDS to detect and prevent unauthorized access to systems and networks.
4) Use IAM tools to manage user identities and access to systems and networks.
5) Develop a comprehensive incident response plan to quickly respond to and contain cyber-attacks.
6) Conduct regular risk assessments to identify vulnerabilities and take steps to mitigate them.
7) Implement advanced technologies like AI/ML to improve IT security and detect cyber threats.
8) Use encryption to protect sensitive data both in transit and at rest.
9) Develop a comprehensive cybersecurity policy that outlines the organization's approach to cybersecurity.
10) Establish incident response procedures to quickly respond to and contain cyber-attacks.
11) Continuously monitoring systems and networks for signs of cyber-attacks and take swift action to respond to incidents.
12) Regularly update software and systems to ensure that they have the latest security patches and updates.

VIII. CONCLUSION

The study of cybersecurity and its role in information technology has revealed the critical importance of protecting digital assets from various threats. As technology advances and becomes increasingly integrated into our daily lives, the need for robust cybersecurity measures has never been more pressing. Cybersecurity is an Increasingly critical concern in today's rapidly evolving digital Landscape. Organizations of all sizes and industries must Prioritize cybersecurity efforts, recognizing the growing Importance of protecting their digital assets, intellectual Property, and customer data. Failing to do so can be severe, With significant financial, operational, and reputational Damage at stake. At the same time, organizations must adopt proactive and Risk-based approaches to cybersecurity management, Integrating security best practices into their organizational Culture and decision-making processes. This involves fostering A culture of cybersecurity awareness and training among Employees and engaging executive leadership in driving and Supporting cybersecurity initiatives. By doing so, organizations Can create a more resilient and security-conscious environment, better equipped to face the challenges of the evolving threat Landscape. In addition, this study has demonstrated the importance of staying up-to-date with the latest cybersecurity threats and trends. The cybersecurity landscape is constantly evolving, and organizations must be proactive in their approach to cybersecurity to stay ahead of emerging threats.

REFERENCES

[1] Adhikari, Jeevan & Kumar, Arvind & Publications, Research. (2017). AN INTRODUCTION TO CYBER CRIMES AND ROLE OF CYBER- SECURITY IN INFORMATION TECHNOLOGY. SSRN Electronic Journal. 5. 13-20.

[2] Boyes, Hugh & Higgins, Matthew. (2024). An Overview of Information and Cyber Security Standards. Journal of ICT Standardization. 95-134. 10.13052/jicts2245-800X.1215.
[3] "Cybersecurity 101" by Mark Stanislav (2017)
[4] "Cybersecurity Trends and Insights" by Deloitte (2020)
[5] "Cybersecurity Threats and Trends" by Symantec (2020)
[6] "Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina God bole
[7] Goncharenko, G. (2024). To the problem of defining and distinguishing the definitions of "information security" and "cyber security". Analytical and Comparative Jurisprudence. 466-471. 10.24144/2788-6018.2024.05.73.
[8] Journal of Cybersecurity (Oxford University Press)
[9] Rowe, Dale & Lunt, Barry & Ekstrom, Joseph. (2011). The role of cyber-security in information technology education. 113-122. 10.1145/2047594.2047628.
[10] The Cybersecurity Landscape" by Symantec (2020)
[11] "The Importance of Cybersecurity in the Digital Age" by Cybersecurity Ventures (2020)
[12] "The Role of Cybersecurity in Protecting Sensitive Information" by Techopedia (2020)
[13] "2020 Cybersecurity Report" by Cybersecurity Ventures (2020)
[14] https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security