ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14942742

Security Staffing Strategic Plan for Organizations Security Posture Enhancement

[1]Kamal Aldin Yousif Yaseen; [2]Israa Abdulrauof Osman

[1]Department Information System, College of Economics, Management & Information System
University of Nizwa, Oman

[2]Mathematical and Physical Sciences - Computer Sciences Section
College of Arts and Sciences

Abstract: In this paper several key elements will be addressed to enhance the organizations cybersecurity posture and align it with its business objectives, the introductory letter outlined the organizations recent assessment of cybersecurity policies and vulnerabilities, emphasizing the need for a proactive cybersecurity approach to protect critical information assets. The significance of strong cybersecurity measures in the face of evolving cyber threats was underscored, highlighting the potential catastrophic implications of data breaches. The call to action for all stakeholders to embrace and drive best cybersecurity practices, in line with industry frameworks like the NIST Framework, was also emphasized.

Keywords: *Cybersecurity, Phishing, Measures, Incident, Patching, Awareness, Vulnerability.*

How to Cite: Kamal Aldin Yousif Yaseen; Israa Abdulrauof Osman (2025) Security Staffing Strategic Plan for Organizations Security Posture Enhancement. *International Journal of Innovative Science and Research Technology*, 10(2), 909-916. https://doi.org/10.5281/zenodo.14942742

I. INTRODUCTION

The business mission, vision, and values of any organization is articulated to communicate the organizations core identity and goals from a business perspective. The mission statement emphasized the commitment to offering high-quality service to clients at competitive rates while fostering a friendly and competitive workplace. The vision aimed to position Organization as the most empathetic and attentive insurance company, striving to improve skills, offer quality products, and expand customer access. The values of trust, knowledge, connection, teamwork, respect, integrity and professionalism, fun & humor, and commitment underscored the organizations commitment to ethical conduct, continuous learning, customer-centric approach, and teamwork [1][2].

The IT philosophy of Organization outlined guiding principles and values influencing the organizations approach to information technology and cybersecurity. Embracing digital transformation, cybersecurity classification, risk management, security controls, proactive cybersecurity, and business and IT alignment were highlighted as key focus areas. The adoption of outsourcing for various IT services, implementation of data classification schemes, and deployment of technical solutions like email filtering systems and encryption reflected the organizations proactive stance towards cybersecurity [3][4].

The organizational structure of organization's security team was presented, emphasizing the strategic positioning of the Chief Information Security Officer (CISO) and the delegation of responsibilities across various security roles. Justifications for the organizational chart were provided, highlighting the need for efficient team alignment with the organization's cybersecurity requirements. Collaboration with internal and external partners was emphasized to optimize resources and expertise in addressing cybersecurity challenges effectively [5].

Furthermore, the security mission, vision, and core values of Organization were outlined to establish principles and objectives for the organization's security practices. The mission emphasized continuous evolution of cybersecurity capabilities to detect, prevent, and respond to cyber threats, while the vision aimed to position Organization as a leader in crafting and delivering strong cybersecurity practices. Core values of confidentiality, integrity, availability, and accountability underscored the organizations commitment to safeguarding assets, information, and people [6][7][8].

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14942742

II. METHODOLOGY

In this research we are using the performance measurement metrics of phishing resilience rate is calculated as the number of successful phishing attempts divided by the total number of phishing simulation emails sent to enable assess the effectiveness of phishing awareness training and identifies areas for improvement in the organization's defense against phishing attacks by tracking this metric over time, the security team can evaluate the success of training programs and implement targeted measures to enhance employee awareness and response to phishing attempts.

The security team, HR department, and executive management are the primary audience for this metric and data is collected and reported monthly to provide regular insights into the organization's phishing resilience. The Security Awareness Coordinator oversees the collection, analysis, and reporting of this metric as shown below.

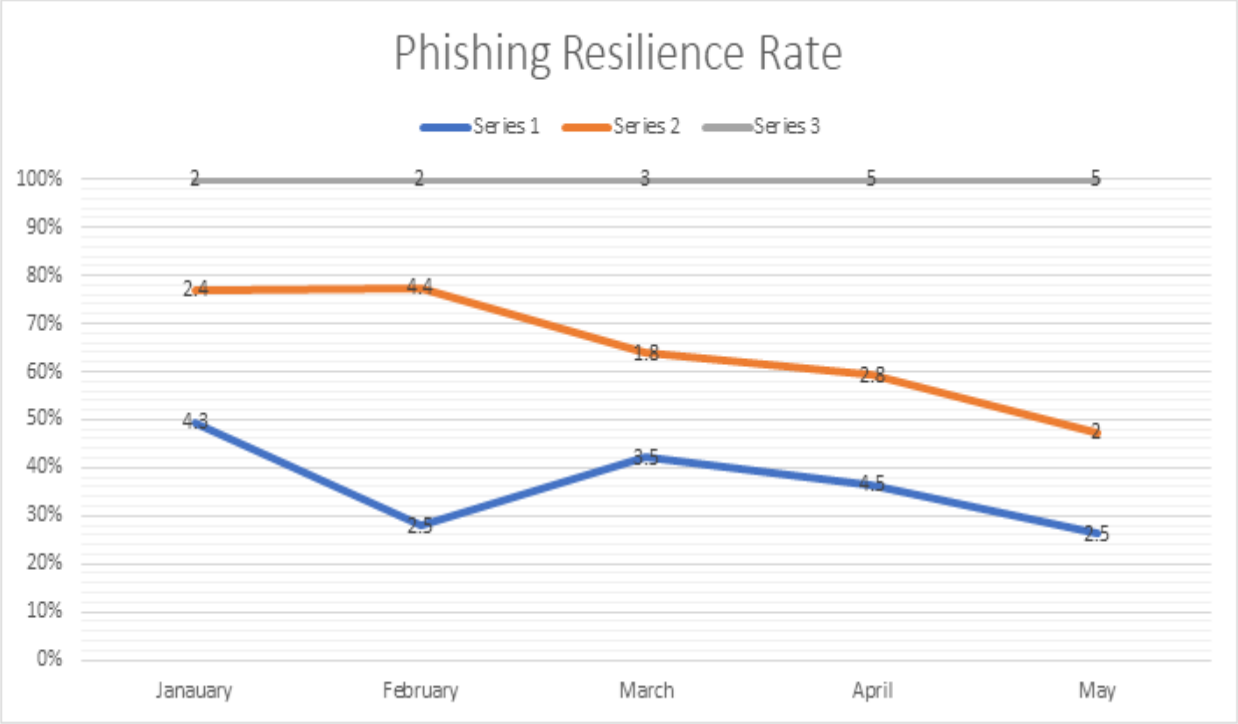

Fig 1: Phishing Resilience Rate

In previous graph each line represents a different component contributing to the phishing resilience rate.

The lines are stacked to show the total Phishing Resilience Rate for each month.

Markers (numbers) are placed at each data point for better visualization and interpretation.

III. INCIDENT RESPONSE TIME:

The incident Response time measures the average duration taken to detect, contain, and respond to security incidents, this metric helps assess the efficiency of the incident response process and aims to minimize the impact of security breaches by reducing response times.

Real-time monitoring of incident response activities allows for timely identification of bottlenecks and optimization of response procedures.

The security team, IT support staff, and executive management are interested in this metric to ensure timely incident resolution. While incident response is monitored in real-time, detailed reports are generated quarterly to track performance over time. Responsibility: Security Incident Responders are responsible for collecting, analyzing, and reporting on incident response times as shown in the following graph.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14942742

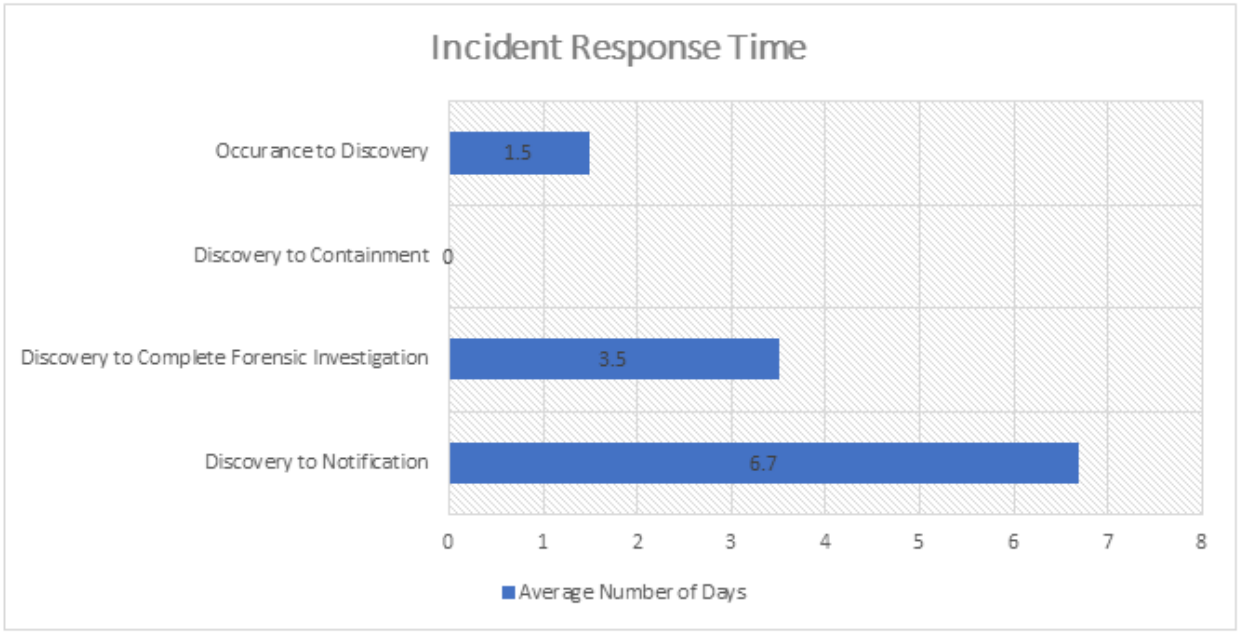

Fig 2: Incident Response Time

In this representation, each bar represents the incident response time for a specific time period. The height of the bar indicates the duration of the response time in hours, while the x-axis denotes different time periods.

IV. PATCH COMPLIANCE RATE:

The patch compliance rate methodology used to ensure adherence and evaluates compliance with organizational and regulatory patching standers also the patch compliance rate measures the percentage of systems and software that have been patched within the defined timeframe to ensuring timely patch deployment is crucial for addressing vulnerabilities and reducing the risk of exploitation by cyber threats By weekly monitoring of patch deployment across all systems and software helps maintain compliance with security policies.

The IT department, security team, and executive management rely on this metric to assess the organization's vulnerability management practices, frequently the data on patch compliance is collected and reported weekly to provide up-to-date insights into the organization's security posture the information security manager responsibilities are oversees the collection, analysis and reporting of patch compliance data.

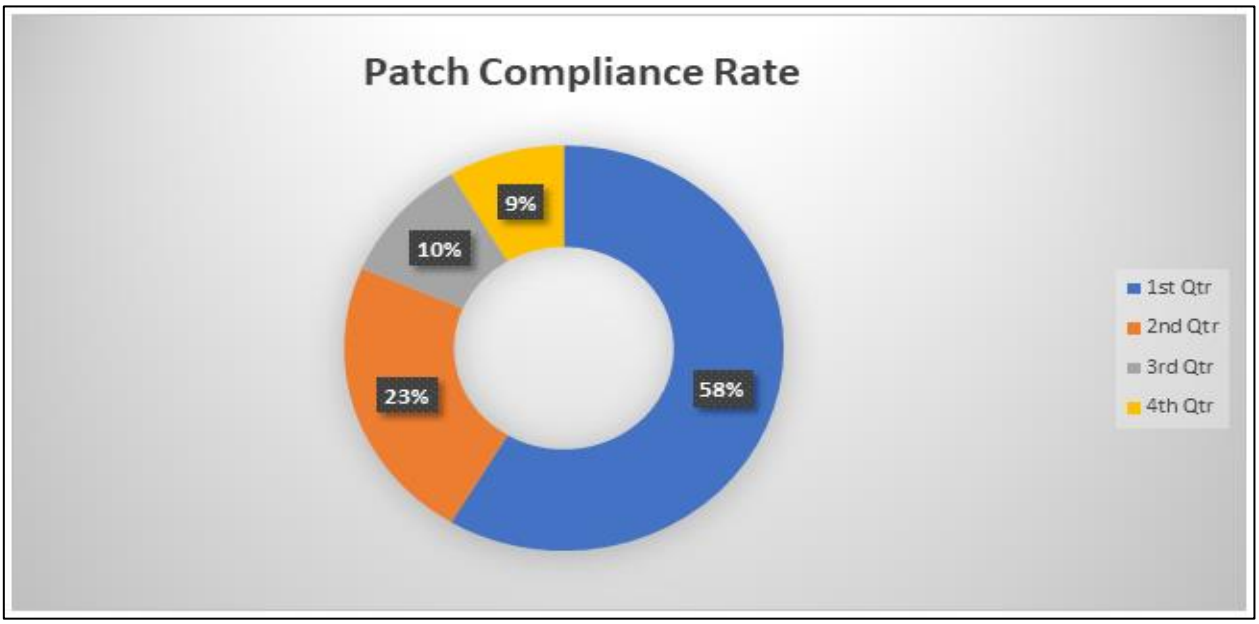

Fig 3 In this Representation, Each Slice of the Pie Chart Represents a Category of Patch Compliance Rate. The Size of Each Slice Corresponds to the Percentage of Patches that are Compliant within each Category.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14942742

V. USER ACCESS REVIEW COMPLETION:

The user access review completion measures the percentage of user access reviews completed within the scheduled timeframe and maintaining the security and integrity an organization digital assets and sensitive information.

The regular user access reviews are essential for maintaining proper access controls and mitigating the risk of unauthorized access to sensitive data by monthly tracking of user access review completion ensures adherence to security policies and regulatory requirements.

The security team, information technology (IT) support staff, and executive management are interested in this metric to ensure compliance with access control policies. Data on user access review completion is collected and reported monthly to track progress and identify any delays or issues also, the compliance and risk analyst is responsible for overseeing the completion, analysis, and reporting of user access reviews.

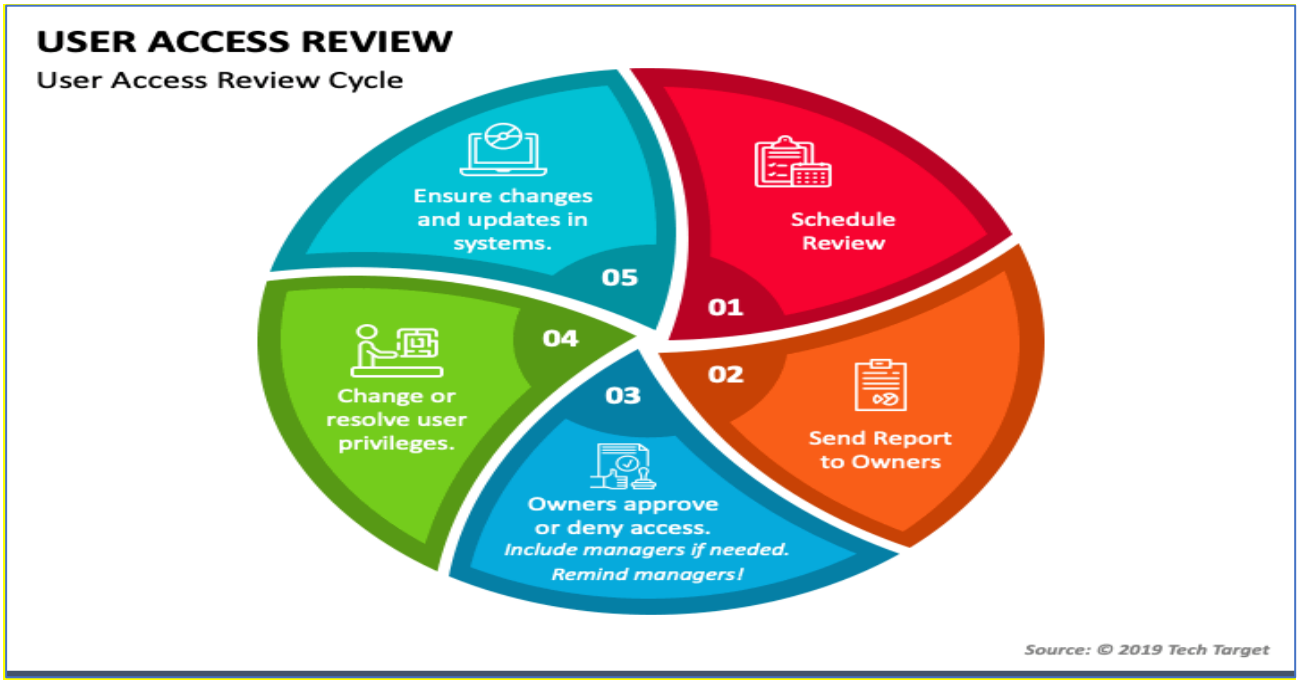

Fig 4: User access review cycle

As shown in the above graph, each slice of the pie chart represents a category of user access review completion rate. The size of each slice corresponds to the percentage of completion within each category.

VI. HYBRID APPROACH (CLOUD BACKUP AND COLD SITE)

Regarding to the data backup and recovery procedure the plan outlines detailed procedures for backing up critical systems and data to both cloud-based storage solutions and physical backup devices includes regular backup schedules, verification processes, and protocols for restoring data in the event of data loss or corruption [9].

- *Activation Procedures For The Cold Site:*

if the institution been hacked or event of a disaster happened that renders the primary site unavailable, the plan specifies the activation procedures for the cold site. This includes steps for transporting backup data to the cold site, configuring infrastructure and systems at the cold site, and establishing connectivity to ensure continuity of operations [10].

- *Communication Protocols:*

For ensuring continuity of the operations our plan defines communication protocols for informing stakeholders, including employees, clients, partners, and regulatory authorities, about the incident and its impact on operations that includes channels of communication, contact lists, and escalation procedures to ensure timely and accurate dissemination of information.

- *Roles And Responsibilities:*

It's very vital to define and determine the key personnel and to ensure that are assigned specific roles and responsibilities during continuity operations this includes the CISO and other standers, who has overall responsibility for the business continuity plan, the information security manager, who coordinates continuity efforts and activates the cold site, the IT team, responsible for executing data backup and recovery procedures, and the communications team, responsible for stakeholder communication [11].

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14942742

VII. INCIDENT RESPONSE PLAYBOOK FOR RANSOMWARE INCIDENTS:

Include the technologies critical for detection, containment, and remediation as following:

- *Endpoint Detection And Response (EDR):*

Based on the security policies and rules organization relies on advanced (EDR) solutions to continuously monitor endpoints for any signs of ransomware activity this proactive approach enables swift detection and response to potential threats, safeguarding critical data and systems [12].

- *Network Intrusion Detection/Prevention Systems (Nids/Nips):*

Normally the firewall is using as a first defiance line to filter the in/out bound signal in additional to this in this paper we proposed network security infrastructure includes robust NIDS/NIPS solutions that actively scan network traffic for indicators of ransomware activity by promptly detecting and blocking malicious traffic, we can contain the threat and prevent further propagation within organization network.

- *Backup And Disaster Recovery Solutions:*

After system crashed or disaster event the organization has to maintains comprehensive backup and disaster recovery mechanisms to ensure data resilience and business continuity in the face of a ransomware attack. Regularly tested backup procedures allow for the timely restoration of encrypted data, minimizing operational disruptions [13].

VIII. SECURITY STAFFING STRATEGY RECRUITMENTS:

- *Internal Recruitment:*

The organization internal promoting is beneficial as it leverages existing knowledge of company culture, processes, and policies, employees who are already familiar with the organization are likely to require less time for training and onboarding. Additionally, internal promotions can boost morale and motivation among existing employees, demonstrating opportunities for career growth and advancement.

- *External Recruitment:*

To create a business alliance or cooperation with reputable recruiting agencies and utilizing online job platforms broadens the talent pool and allows the organization to attract candidates with diverse experiences and skill sets, external recruitment is essential for bringing in fresh perspectives and expertise, especially for specialized roles or when internal talent is not available [14] [15].

- *Technical Proficiency:*

Candidates should possess a strong understanding of cybersecurity principles, including but not limited to network security, endpoint security, threat intelligence, and incident response. Technical proficiency ensures that security staff can effectively identify, analyze, and respond to security threats and incidents.

- *Communication Skills:*

Effective communication is crucial for security professionals to convey technical concepts to both technical and non-technical stakeholders. Security staff must be able to articulate security risks, findings, and recommendations clearly and concisely to management, employees, clients, and external partners [16] [17].

IX. INTERVIEWING AND ONBOARDING PROCESS:

- *Technical Assessment:*

Conducting technical interviews and assessments allows the organization to evaluate candidates' skills and knowledge in cybersecurity and also technical assessments may include practical exercises, scenario-based questions, and knowledge tests to assess candidates' capabilities accurately.

- *Cultural Fit Evaluation:*

to assessing candidates' alignment with company goals, values, culture, and team dynamics during the interview process ensures that new hires will integrate well into the organization cultural fit evaluation helps maintain a positive work environment and promotes collaboration and teamwork among security staff [18].

- *Comprehensive Onboarding:*

Very important and vital for providing thorough onboarding programs is essential to familiarize new hires with company policies, procedures, tools, and systems. Comprehensive onboarding ensures that new security staff understand their roles and responsibilities and have the necessary resources to succeed in their positions.

- *Career Growth Opportunities:*

for offering clear paths for career progression and advancement within the organization motivates security staff to stay engaged and committed to their roles and career growth opportunities can include promotions, lateral moves, cross-training, and leadership development programs tailored to cybersecurity professionals.

- *Recognition And Rewards:*

Recognizing and rewarding employees for their contributions and achievements fosters a culture of appreciation and loyalty within the organization, this recognition can take various forms, including performance bonuses, awards, public acknowledgment, and opportunities for increased responsibility and visibility this could help the organization to eliminate the social engineering attack hence emphasizing the security posture [19].

X. HANDLING EMPLOYEE DEPARTURES:

- *Exit Interviews:*

Conducting exit interviews allows the organization to gather feedback from departing employees, identify areas for improvement, and address any concerns or issues that may have contributed to their departure. Exit interviews provide valuable insights into organizational strengths and

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14942742

weaknesses and help identify opportunities for enhancing employee retention.

- *Knowledge Transfer:*

to implementing knowledge transfer processes ensures a smooth transition and continuity of operations when employees leave the company. Knowledge transfer may involve documenting processes, procedures, and best practices, conducting training sessions for replacement staff, and facilitating mentorship or shadowing opportunities to transfer knowledge from outgoing employees to their successors.

XI. SECURITY AWARENESS AND EDUCATION PLAN:

- *Interactive Workshops:*

In order to enhance the security posture, the institutions should conduct regular interactive workshops where employees can learn about cybersecurity best practices, identify potential threats, and understand their role in maintaining a secure work environment.

- *Online Training Modules:*

Organize and develop a series of online training modules covering various cybersecurity topics such as phishing awareness, password management, data protection, and social engineering these modules will be accessible to all employees through the organizations learning management system [20].

- *Simulated Phishing Campaigns:*

The companies and organizations should implement simulated phishing campaigns to test employees' ability to recognize and report phishing attempts. These campaigns will provide valuable feedback and reinforce the importance of staying vigilant against email-based threats.

- *Security Awareness Materials:*

Distribute and create educational materials such as infographics, posters, and newsletters to raise awareness about cybersecurity issues and promote best practices among employees.

- *Employees Engagement Activities:*

Develop and organize engaging activities such as quizzes, contests, and role-playing exercises to make cybersecurity training more interactive and enjoyable for employees.

XII. COMMUNICATION AND TRAINING TECHNIQUES:

- *Email Campaigns:*

Notify and inform the employees and staff via regular email updates and reminders about cybersecurity best practices, upcoming training sessions, and recent security incidents and threats to keep employees informed and engaged [21].

- *In-Person Sessions:*

Organize and host face-to-face training sessions led by cybersecurity experts to provide in-depth knowledge and address employees' questions and concerns directly to solve the cybersecurity awareness issues, based on last studies 17.6% of cybersecurity problems coming due to the lack of awareness or uunintentional reasons.

- *Webinars:*

Conduction a regular webinar on specific cybersecurity topics, inviting guest speakers and industry experts to share insights and best practices with employees, this method very cheap and it will not delay employee’s activities also it will emphasize their knowledge and skills to prevent the risk.

- *Interactive Online Platforms:*

Utilize interactive online platforms such as discussion forums and chat groups, where employees can ask questions, share experiences and collaborate on cybersecurity-related issues.

XIII. GENERAL CYBERSECURITY TIPS:

This paper advises the organization to apply and practice the following techniques to avoid the cybersecurity issues and prevent the attacks based on the approved security policies:

- *Phishing Awareness:*

Recognizing and avoiding phishing emails, links, and attachments or any spam contents.

- *Password Security:*

Creating strong and complicated passwords, using multi-factor authentication, and safeguarding login credentials, the cybersecurity staff used to determine the period of passwords periodically.

- *Data Protection:*

The employees and IT staff used to ensure that and handling sensitive information securely, encrypting files, and following data retention policies.

- *Devices Security:*

Ultimate goal of physical security is to securing work devices, updating software regularly and protecting against malware, viruses and other threats.

- *Social Engineering:*

Cybersecurity staff should identify social engineering tactics such as pretexting and baiting and avoiding manipulation by malicious actors.

- *Frequency of Communication and Training:*

Conducting monthly training sessions covering different cybersecurity topics to ensure continuous learning and reinforcement of key concepts and organize quarterly interactive workshops to provide more in-depth training and hands-on experience for employees, also send bi-weekly email updates with tips, reminders, and resources to keep cybersecurity top-of-mind for employees.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14942742

- *Creators, Distributors, and Audience Roles:*

The cybersecurity plan commonly includes all the stakeholder in order to meet security final goals, creator's cybersecurity team, in collaboration with HR and IT departments, will develop and create training materials and workshops also distributors training materials will be distributed through the organizations LMS, email newsletters, intranet, and physical displays in office spaces, lastly the audience all employees across departments and levels within the organization will participate in the security awareness program.

XIV. MEASURING IMPACT:

Conducting a pre-training and post-training assessments to evaluate and asses employees' knowledge and understanding of cybersecurity concepts and measure improvement over time are very vital to meet protection requirements, phishing simulation results to monitor the results of simulated phishing campaigns to track employees' ability to recognize and report phishing attempts accurately, collect feedback from employees through surveys and feedback forms to gauge the effectiveness of training sessions and identify areas for improvement, incident response metrics so important to track metrics related to security incidents, such as the number of reported incidents and response times, to assess the overall impact of the awareness program on reducing security risks and improving incident response capabilities [22].

Apply and implementing this comprehensive security awareness blueprint organization aims to empower employees with the knowledge and skills needed to effectively mitigate cybersecurity risks and protect the organizations digital assets.

XV. DISCUSSION & RESULTS

In spite of the verity tools and techniques applied by the cybersecurity staffs but the information security posture still suffering a several issues, hence despite the prevalence of cybersecurity strategies across the different institutions cybersecurity breach incidents persist due to various factors that challenge the efficacy of existing measures, one significant reason is the evolving nature of cyber threats which constantly outpace traditional defense mechanisms, cybercriminals continually devise sophisticated tactics, exploit vulnerabilities, and capitalize on human error, making it difficult for organizations to stay ahead of the curve moreover, the expanding attack surface resulting from digital transformation cloud adoption and the proliferation of connected devices further complicates cybersecurity efforts [23].

Another contributing factor is the lack of comprehensive understanding and awareness of cybersecurity risks among employees at all levels of the organization. Despite the implementation of security training programs, employees may not fully grasp the importance of adhering to security protocols or recognize the implications of their actions on the organization's security posture, this gap in cybersecurity literacy leaves organizations vulnerable to insider threats, social engineering attacks, and inadvertent data breaches.

Furthermore resource constraints including limited budgets, understaffed security teams, and inadequate technology investments, hinder organizations from implementing robust cybersecurity measures effectively, without sufficient resources organizations struggle to deploy advanced security solutions, conduct regular risk assessments, and maintain a proactive security posture, leaving them susceptible to cyber threats to ensure the success of this paper of the cybersecurity strategy, organization must provide comprehensive support across several key areas. Firstly, there needs to be a commitment from senior leadership to prioritize cybersecurity as a core business function and allocate adequate resources to support security initiatives, this includes sufficient budgetary allocations for cybersecurity investments, staffing, and training programs.

Secondly, there must be a cultural shift towards promoting cybersecurity awareness and accountability throughout the organization, this involves fostering a security-conscious culture where employees understand their roles and responsibilities in safeguarding sensitive information and are empowered to report security incidents promptly.

Additionally, cross-functional collaboration between the cybersecurity team and other business units is essential for aligning security objectives with broader business goals by integrating security considerations into strategic decision-making processes, such as product development, supply chain management and customer engagement, the organization can proactively address security risks and minimize vulnerabilities.

Lastly, ongoing evaluation and adaptation of the cybersecurity strategy are crucial to keep pace with evolving threats and technology trends, regular assessments, audits, and incident response exercises help identify weaknesses, refine security controls, and ensure continuous improvement in the organization's security posture.

XVI. CONCLUSION

Lastly in conclusion our security strategy and methodology play a pivotal role in aligning security objectives with broader business goals by prioritizing proactive risk management, employee education, and strategic investments in cybersecurity, we not only protect our organization from potential threats and risks but also enhance our operational efficiency and reputation, this alignment ensures that security initiatives are integrated seamlessly into our overall business strategy, reinforcing our commitment to safeguarding our assets, maintaining trust with stakeholders, and sustaining long-term success in an increasingly complex threat landscape. Through cohesive collaboration between security and business teams, we can effectively mitigate risks while driving innovation and

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14942742

growth, thus ensuring the resilience and prosperity of our organization for years to come.

Finaly the security issues and challenges faced by many organizations including data privacy and compliance cyber insurance risks phishing and social engineering, and supply chain security, were identified, the recommendation for overcome the security issues concentrate on the awareness and training program for employees, enforcing security policies and combine the human factor inside cybersecurity strategies emphasized the security posture and mitigate the risk associated with human errors.

REFERENCES

[1]. Anderson, Ross, and Tyler Moore. "The economics of information security." science 314, no. 5799 (2006), 610-613.

[2]. Buchanan, Ben. "The cybersecurity dilemma Hacking, trust, and fear between nations", Oxford University Press, 2016.

[3]. Ciampa, M., "Security Awareness: Applying Practical Security in Your World", Cengage Learning, 2017.

[4]. Vasiliki Tzavara, Savvas Vassiliadis, "Tracing the evolution of cyber resilience: a historical and conceptual review", International Journal of Information, 2024.

[5]. ENISA, Definition of cybersecurity gaps and overlaps in standardization (2015). https://www.enisa.europa.eu/publications/definition-of-cybersecurity

[6]. Lewallen, J., "Emerging technologies and problem definition uncertainty", the case of cybersecurity, Regul, Govern, (2020). https://doi.org/10.1111/rego.12341

[7]. Accenture., "The nature of effective defense", shifting from cybersecurity to cyber resilience (2018). https://www.accenture.com/_acnmedia/accenture/conversion-assets/dotcom/documents/local/en/ accenture-shifting-from-cybersecurity-to-cyber-resilience-pov.pdf

[8]. Gunderson, L., Holling, C, Panarchy, "Understanding Transformations in Human and Natural Systems", Bibliovault OAI Repository, p. 114. The University of Chicago Press, (2003)

[9]. International Telecommunication Union., "Cybersecurity, dataprotection and cyber resilience in smart sustainable cities", (2015)

[10]. Holling, C.S., "Resilience and Stability of Ecological Systems", Annual Reviews Inc. (1973)

[11]. Fiering, M.B., "Alternative indices of resilience", Water Resour.Res. Resour. Res. 18(1), 33–39 (1982). https://doi.org/10.1029/WR018i001p00033

[12]. Holling, C.S., "Engineering resilience versus ecological resilience", In: Schulze, P.E. (ed.) Engineering within Ecological Constraints, pp. 31–43. National Academy Press, Washington DC (1996)

[13]. Benjamin, R., Gladman, B., Randell, B., "Protecting IT systems from cybercrime", Comput. J.. J. 41, 429–443 (1998)

[14]. Luthar, S.S., Cicchetti, D., Becker, B., "The construct of resilience, a critical evaluation and guidelines for future work", Child Dev, 71(3), 543–562 (2000). https://doi.org/10.1111/1467-8624.00164

[15]. Jorgensen, J., Rossignol, P., Takikawa, M., Upper, D., "Cyber ecology: looking to ecology for insights into information assurance", vol. 2, pp. 287–296 (2001). https://doi.org/10.1109/DISCEX, 2001.932180

[16]. Saagar Makwana, 2002, "IBM Global Services Resilient infrastructure: Improving your business resilience", IBM Global Services.

[17]. Zahri, Y., Ahmad, N.M.Z, "Future Cyber Weapons. National ICT Security and Emergency Response Centre" (2003)

[18]. UK Cabinet Office, "Transformational Government—Enabled by Technology" (2005)

[19]. Gordon, L.A., Loeb, M.P, "Managing Cybersecurity Resources, A Cost-Benefit Analysis", McGraw-Hill Inc, New York (2006)

[20]. Hollnagel, E., Woods, D., Leveson, N, "Resilience engineering, concepts and precepts Resilience engineering concepts and precepts" (2006)

[21]. Chai, S., Sharman, R., Patil, S., Satam, S., Rao, R., Upadhyaya, S., "Surface transportation and cyber-infrastructure an exploratory study", pp. 124–128 (2007). https://doi.org/10.1109/ISI.2007.37 9544

[22]. Ulieru, M., "Design for resilience of networked critical infrastructures", In Proceedings of the 2007 Inaugural IEEE-IES Digital EcoSystems and Technologies Conference, DEST 2007, pp. 540–545 (2007). https://doi.org/10.1109/DEST.2007.372035

[23]. Banatre, M., Pataricza, A., van Moorsel, A., Palanque, P., Strigini, L., "From Resilience-Building to Resilience-Scaling Technologies", Directions—ReSIST NoE Deliverable D13.