Research Article

Pharmacy Cybersecurity Awareness And Training Programs: Examine The Effectiveness ff Cybersecurity Awareness and Training Programs For Pharmacy Staff, Including Pharmacists, Technicians, and Support Personnel

Dr. Anjaiah Adepu[1], Dr. Mohammed yousuf khan[2], Dr.Dara Raju[3], Dr. N. Arjun[4], Dr. Aakunuri Manjula[5], Md Fasihuddin[6], Mujahid pasha syed[7]

[1]Associate Professor ,CSE, School of Engineering & Technology , Maulana Azad National Urdu University, Hyderabad, Telangana, India. Email-id: anjaniprasad.adepu@gmail.com
[2]Associate Dean,School of Engineering & Technology & Principal,Polytechnic ,Maulana Azad National Urdu University, Hyderabad, Telangana, India. Email-id: yusuf_lect@yahoo.com
[3]Professor, Department of Computer Science and Engineering,Vignana Bharathi Institute of Technology, Aushapur, Ghatkesar, Hyderabad, Telangana, India.Email-id:rajurdara@gmail.com.
[4]Associate Professor, Department of Computer Science and Engineering,Vignana Bharathi Institute of Technology, Ghatkesar, Hyderabad, Telangana, India.Email-id:arjun.nelikanti@vbithyd.ac.in.
[5] Associate Professor, Department of Computer Science and Engineering,Jyothishmathi Institute of Technology and Science, Karimnagar, Telangana, India.Email-id:manjula3030@gmail.com
[6]Assistant Professor,CSE School of Engineering & Technology ,Maulana Azad National Urdu University, Hyderabad, Telangana, India. Email-id: mdfasihuddin@manuu.edu.in
[7]Assistant Professor, CSE, School of Engineering & Technology ,Maulana Azad National Urdu University, Hyderabad, Telangana, India. Email-id: syedmuja@manuu.edu.in

Abstract

In today's internet-driven business environment, security breaches and cybercrime have reached pandemic proportions, with pharmacies being the most recent victims. When committing cybercrime, criminals look for vulnerabilities in computer systems and networks to steal sensitive data, financial assets, and damage the reputation of legitimate businesses. In order to build strong cybersecurity defenses, pharmacies rely heavily on their employees, particularly their technicians and support personnel. This research highlights the need for cybersecurity awareness and training programs, emphasizing that pharmacy personnel play a crucial role in protecting patients' trust and acting as the first line of defense against hackers. A literature review and analysis of real-world case studies were used to assess the effectiveness of cybersecurity training for pharmacy workers. The findings indicate that well-designed training programs have the potential to safeguard sensitive information, promote cybersecurity awareness, and decrease security incidents. This study focuses on identifying ways to adapt training for the increasing number of remote workers in pharmacy operations.A thorough approach to safeguarding sensitive information, including training, organizational rules, and continual technical measures, is necessary to enhance pharmacies' cybersecurity posture in the digital age.

Index Terms: Cybersecurity, training programs, pharmacies, pharmacy staff, digital security, remote work, sensitive data protection, cyber threats, awareness, organizational policies.

I Introduction

The healthcare industry has rapidly shifted from paper-based systems to electronic health records (EHRs) to provide more efficient and cost-effective services. Significant improvements in medical practice, patient care, disease diagnosis, and information accessibility have resulted from electronic health records [1]. The widespread use of healthcare IT systems has led to a rise in cyberattacks. A technical example of this increased vulnerability is the advent of the Internet of Things (IoT) [2]. Insufficient protection of patients' personal information in healthcare IT systems could have catastrophic consequences for patients' health and treatment. Raising data security standards may improve outcomes for individual patients' diagnostics and treatments.

The sensitive information pharmacies possess, including patients' medical data, insurance details, and payment information, makes them a prime target for cybercriminals. Cybersecurity risks such as phishing, ransomware, and data breaches are on the rise in the healthcare sector. Both patient confidentiality and business continuity are jeopardized by these attacks [3]. Human error is the greatest threat, even when technology safeguards are necessary. All pharmacy team members, including technicians, support personnel, and pharmacists, should be aware of the importance of cybersecurity and participate in individualized training programs [4]. A critical skill for pharmacy personnel is the ability to identify and mitigate cyber threats. Well-designed training programs foster this skill. Key focus areas include safe password practices, phishing attempt identification, and protecting patient data in compliance with regulations such as HIPAA [5]. Proactive measures encouraged by regular, hands-on training can reduce the likelihood of costly security breaches and disruptions to patient care. These programs promote a security-first mindset in the workplace and teach defensive tactics as an added bonus. These activities impact not only individual behaviors but also help improve the pharmacy's overall security posture [6]. Well-trained personnel can act as a first line of defense, preventing issues from escalating. A continuous learning approach ensures employees remain vigilant

against new threats, supported by frequent updates and reinforcement through simulations. Pharmacy cybersecurity awareness and training programs are crucial for preserving patient trust and ensuring seamless operations in the face of cyber threats [7].

HEALTHCARE CYBERATTACKS

Respected scholarly papers and tech news pieces have reported cyberattacks on healthcare institutions throughout Asia. In below survey shows the data that were used to identify the five main types of cyberattacks. The purpose of this study is to thoroughly examine the benefits and downsides of these five forms of assault. Recent assaults have prompted us to review the basics of the NIST risk assessment methodology, which is widely utilized [7], [8]. A comprehensive assessment of the dangers presented by these intrusions is immediately necessary in light of the fact that information risk management is still in its early stages in healthcare organizations throughout Asia. Neither the Global nor the Cyber Maturity indices were kind to the Asia-Pacific region in terms of cybersecurity. Because healthcare facilities in Asia are often unprepared to handle cyberattacks, we decided to concentrate on that region for our study. The exposure of 1.5 million patient health information in Singapore was one of the largest data breaches of 2018. Hackers gained access to the patient database after infecting one SingHealth machine with malware and obtaining privileged account credentials [9]. This event exposed the lack of antimalware security. Another common kind of hack on healthcare companies in Asia is the phishing attack. To trick their targets into divulging vital information, criminals in this kind of assault pose as reputable organizations. With 47,500 reported phishing URLs in 2019, the Cyber Security Agency of Singapore (CSA) was busy. Two Indonesian hospitals were the targets of the WannaCry ransomware, which encrypts any data kept in IT systems and demands payment to decrypt it. There is a lack of oversight and management of cyber risks by the majority of Asian firm boards, according to the Global State of Information Security Survey (GSISS 2016) [10]. Data collected from public records and scholarly articles shows that many Asian nations had cyberattacks on their healthcare systems in the years between 2018 and 2020. This category includes the following countries: Saudi Arabia, the Philippines, Indonesia, Malaysia, Singapore, and Thailand [11].

The prevalence and sophistication of cybersecurity breaches and attacks are on the rise, endangering both persons and organizations (Hussain et al., 2020). Cybersecurity education and awareness has helped businesses strengthen their cybersecurity posture and reduce cybersecurity risk over time. According to Bada et al. (2019), developing capacity has the potential to decrease the related risk by 45–70% [12]. Cybersecurity is a rapidly evolving subject with unintended repercussions due to the rapid development of new technologies, which makes it even more challenging to identify threats due to the complexity of these technologies (Nobles, 2019). Although technology has been effective in reducing cybersecurity risks in the past, it is crucial to tackle this complicated issue directly since people are fundamentally naive (Yan et al., 2018). Human resources should spearhead fortification efforts and cybersecurity threat protection in order for any company to be robust. Fairburn et al. (2021) [14] emphasized four aspects—safety, usability, habits, and culture—that lead to cybersecurity resilience. Cybersecurity training and education is one approach to dealing with this resilience (Rajamäki et al., 2018) [15]. According to Angafor et al. (2020), the goal of this program is to aid with threat management and responding to cybersecurity incidents by increasing individual awareness and competence. To improve cybersecurity awareness initiatives, academics will study existing data, theoretical frameworks, and industry best practices to identify gaps and provide solutions [16].

II Survey Of Research

(1) "Securing Patient Trust: Advancing Cybersecurity and Training in Health-System Pharmacies" authored by Shawn Bookwalter, MSHI, MS, BCPS, and Mike Hennessy Jr.This article provides an overview of healthcare cybersecurity best practices, including encryption, access limitations, and initiatives led by pharmacists, to protect sensitive patient information and foster trust. In order to increase cybersecurity education in healthcare institutions, it gives suggestions on how to overcome barriers.
[2] "Cyber Security Primer for Pharmacists"

A pharmacist from the US, This research covers the cyber dangers associated with electronic health records (EHRs) and mobile devices. This paper provides an extensive explanation of security measures, including password management, role-based data access, and phishing attack awareness training, among many others. A high focus is educating pharmacy staff about the importance of cybersecurity.
[3] "Navigating Cybersecurity Training: A Comprehensive Review" (Page 73), by Saif Al-Dean Qawasmeh, Ali Abdullah S. AlQahtani, and Muhammad Khurram Khan.This article dives into the significance of artificial intelligence in cybersecurity training while also examining several traditional and contemporary approaches. Methods for addressing implementation challenges and increasing cyber awareness and response among pharmacy staff are the primary foci.
[4] Collaborative Research Team at MDPI, "Towards an Innovative Model for Cybersecurity Awareness Training" [4]This research

introduces the iCAT method, which uses knowledge graphs and gamification to enhance cybersecurity education. It focuses on adaptive learning and real-time feedback to promote a proactive cybersecurity culture, boost engagement, and keep pharmacy professionals.

[5] "Developing Cybersecurity Resilience in Pharmacy Practice" by Antoine Al-Achi, PhD; Laurie Pennell, PharmD; and Jessi Dennis, PharmD candidate " [5]This research focuses on the training that pharmacists provide about data security and medication reconciliation. Results showed that training enhanced data handling accuracy, lending credence to the idea that continuing education might help pharmacies maintain cybersecurity.

III The Importance Of Cybersecurity Training And Awareness

One way to lessen the effect of human factors a big cybersecurity risk is to raise cybersecurity awareness and provide cybersecurity training. For many reasons, actual humans—the "human factor" are the cybersecurity setup's Achilles' heel. According to Sabillon et al. (2021), their main function is to cover the current gaps. Cyber incidents may arise from a variety of sources, including insider threats, malware infections, phishing, and data breaches (Bandari, 2023) due to human error, malevolent intent, or lack of knowledge. Improving people's online safety skills may decrease the incidence of cybersecurity accidents. Programs that aim to raise awareness and provide training may help cultivate positive security cultures. The cybersecurity culture of a business may be described as the collective knowledge, beliefs, and actions of its executives and employees (Bada et al., 2019). According to research by Amankwa et al. (2018), a strong security culture increases the likelihood that employees will be well-informed about cybersecurity, have a favorable attitude towards the field, and take appropriate measures to protect the company's data and assets. Workers and management must trust one another, cooperate together, and communicate effectively to address cybersecurity challenges (Ioannou et al., 2019). When employees have proper training, they are more likely to follow all applicable laws and regulations. For example, in Nigeria, the National Data Protection Bureau is responsible for enforcing the NDPR and penalizing non-compliance with fines and other sanctions [20], [21].

CYBERSECURITY TRAINING AND AWARENESS

Cybersecurity training and education may be either formal or informal. What we call "formal training" is really a systematized approach to learning cybersecurity-related ideas and techniques [22]. Cybersecurity education may take many forms, including online classes, webinars, seminars, simulations, exams, and certifications. Contrarily, unstructured training may be presented in a variety of ways, such as via personal experiences, news articles, or websites that provide cybersecurity advice[23].

EHR data breaches can result in patient privacy violations, legal liabilities, financial costs, and erosion of trust in healthcare systems:

When unauthorized parties gain access to patients' medical records, diagnoses, treatments, and personal identifiers due to data breaches in electronic health records (EHRs), patients lose trust in the healthcare system and are unable to receive the treatment they require.

Criminals may use compromised electronic health records to perpetrate a variety of crimes, including medical fraud, financial fraud, and identity theft, which may have devastating effects on both patients' and healthcare providers' bank accounts, professional credibility, and legal positions.

Errors in medical diagnosis and treatment: There is a higher chance of medical errors, inappropriate treatments, and bad patient outcomes due to the possibility of tampering or unlawful access to electronic health record data, which puts patients at risk of having their records filled up erroneously.

Possible Regulatory and Legal Repercussions: If there is a breach of electronic health records (EHRs), healthcare organizations could face investigations by regulatory agencies, fines and penalties for noncompliance with privacy regulations such as GDPR and HIPAA, and possibly even patient lawsuits seeking damages for privacy invasion or harm caused by the breach.

Health Insurance Portability and Accountability Act (HIPAA) - United States

HIPAA Security Rule: Protected health information (ePHI) stored electronically must adhere to strict administrative, physical, and technological guidelines set forth by the law in order to avoid unauthorized access, disclosure, or alteration.

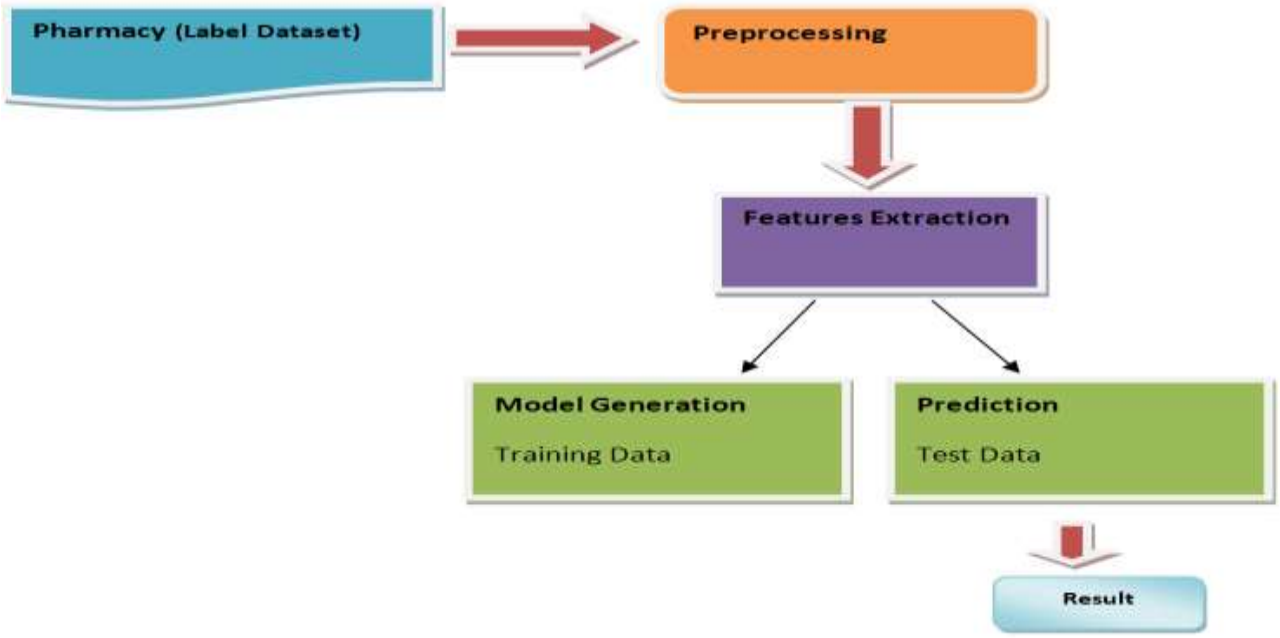
HITECH Act: Increases the scope of HIPAA's privacy and security regulations to include business partners, makes penalties for noncompliance more severe, and creates real usage incentives to encourage the use of certified electronic health record systems.

Incident Response Planning: To better recognize, contain, and mitigate cybersecurity events, such as data breaches and ransomware attacks, healthcare companies may benefit from the assistance of cybersecurity specialists in creating strong

incident response strategies and processes. In order to minimize the impact on patient care and data integrity, companies should collaborate with specialists to ensure that they are prepared to react quickly and effectively to security breaches.
Compliance Assistance: Compliance with applicable legal obligations, such as HIPAA and GDPR, as well as industry standards, such as the NIST Cybersecurity Framework, may be achieved and maintained with the help of cybersecurity professionals. Organizations may better secure patient data and fulfill regulatory requirements when they work with professionals to implement the appropriate measures.

Working Methodology using SVM Classifier
System Model:
The pharmacy cybersecurity model begins by collecting labeled cybersecurity data from pharmacy sources, forming the foundational pharmacists dataset. This raw data then undergoes preprocessing, which involves essential cleaning and transformation to prepare it for analysis. Next, relevant features are extracted from the processed data to facilitate effective model training and predictions. Finally, the trained model makes predictions, delivering insights based on the cybersecurity analysis conducted on the pharmacy dataset.

Figure 1. System Model



Dataset info:
Data on cybersecurity awareness and training programs in American pharmacies would normally include the following: the number of trained staff members, the types and frequency of training sessions, the subjects covered (such as phishing, secure handling of electronic health records, regulatory compliance, and password management), and the utilization of simulated cyber-attack exercises. Data on the effectiveness of training programs, including changes in cybersecurity incident rates or advances in staff cybersecurity knowledge and practices over time, as well as demographic information about the participating pharmacies (location, size, and type), may also be included. Dataset potential additions include staff confidence levels in reacting to cybersecurity threats, compliance rates with state and federal cybersecurity rules affecting healthcare and pharmacy operations, and survey results.

Data Collection and Preprocessing:
At the outset, the research team asks pharmacists and other pharmacy staff to complete out surveys or provide cybersecurity awareness performance measures. Both quantitative and qualitative factors could be considered; for example, survey results about the perceived phishing attempts and the percentage of correct answers are examples of quantitative factors. As part of getting ready, you have to encode category variables, normalize numerical data, and deal with missing values. To prevent overfilling and provide a more realistic picture of performance, divide the sample in half.

Picking Out Features and A Training Model:

We use demographics, knowledge scores, and behavior assessments as important metrics to predict how well the training program will work. The optimal choice for data processing with several dimensions or many classes is a support vector machine (SVM) classifier. When building a support vector machine model, a suitable kernel function, such an RBF or linear one, is required for training. To differentiate between classes (such "trained" and "untrained" or "effective" and "ineffective" outcomes), the approach finds the optimal hyperplane to use during training. Grid search or cross-validation are used to fine-tune the hyperparameters in order to increase the model's accuracy.

A model's efficacy after training on new data is evaluated and understood using metrics like as F1-score, recall, accuracy, and precision. A confusion matrix may be used to find metrics that measure the program's performance, including true positives, false positives, and others. Results show that awareness training has a good effect on understanding and behavior, but it won't be enough to keep people safe online without targeted or ongoing cybersecurity education. By highlighting which areas of staff knowledge or practices should have improvement, the model's feature significance insights could direct adjustments to future training sessions.

SVM Classifier In Cyber Security:

SVM classifier to assess the effectiveness of pharmacy cybersecurity awareness programs. The model is trained on a dataset and tested to predict outcomes, with performance evaluated using an accuracy score. By leveraging machine learning, this approach aids in classifying and analyzing cybersecurity data. Below is the code implementing this process:

Algorithm 1: SVM Classifier with Accuracy Score

```
Step1: Load and Preprocess Data
inputx,inputy=load_dataset()
Step2: Spilt train and test data
X_dtrain, X_dtest, Y_dtrain, Y_dtest = train_test_split(inputx,inputy,test_size=0.3, random_state=42)
Step3:Standardize(scaling)
scdata = StandardScaler()
X_dtrain = scdata.fit_transform(X_dtrain)
X_dtest = scdata.transform(X_dtest)
Step4: Train SVM classifier
svm_model.fit(X_dtrain, Y_dtrain)
Step5: Make predictions
Y_pred = svm_model.predict(X_dtest)
Step6: Evaluate Accuracy Score (AS)
Ascore = accuracy_score(Y_dtest, Y_pred)
Step7:Result
print("Accuracy Score (AS):", Ascore)
```

IV Output Discussion

This part of the work examines the results of the latest research on how to encourage the projected user behavior in connection to the study issue. A lot of research has focused on this exact question. The following are some potential instances of "Cybersecurity Training and Education Programs in enhancing user behaviour": The three primary parts of the suggested paradigm are input, processing, and output. When we talk about "input," what we actually mean are details on the people who will be enrolling in the cybersecurity program, including their background, goals, character attributes, and motivation level. In the second part of the picture, you can see all the different parts of cybersecurity training programs. These parts include things like the design, delivery, methodology, content, length, frequency, and feedback. The cybersecurity training program exemplifies a fire component product that may bring about changes in user behavior, knowledge, skills, and awareness.

In order for the cybersecurity awareness effectiveness model you just read about to be useful, the input must have a major impact on the process. Secondly, the model's prediction is affected by the process variable. Better user behavior could be the result of cybersecurity measures that center decision-making on the interdependence of inputs and processes.

An important aspect of any successful cybersecurity training program is doing a needs assessment to identify user weaknesses and potential areas for further training. The training program might be improved using a variety of approaches and

media, including videos, case studies, simulations, games, quizzes, and lectures. Accurately assessing training necessitates collecting feedback from participants. A better assessment is achievable in the long term with a task that can be revisited to analyze the learning goals. The most current information may be derived from training program evaluations by combining quantitative and qualitative methods. The effectiveness of cybersecurity training programs is highly dependent on the engagement level of patients, the program's relevancy, and the learners' existing knowledge and skills. While the specific amount of influence may vary between program kinds, approaches, and durations of time, the general agreement is that cybersecurity training and education programs do influence user behavior. Awareness campaigns on cybersecurity are good at getting people talking about it, but they don't do much to get people to really do something. While skill-based training does increase user confidence and performance on cybersecurity tasks, it is more expensive and time-consuming to execute. It is essential to provide feedback and incentives to promote these changes for behavior modification programs to successfully influence users' outlooks and intentions towards cybersecurity behavior.

SVM OUTCOME:

The SVM classifier predicts how well cybersecurity awareness and training programs for pharmacy employees will work. Labels (like "Effective" or "Ineffective") produced by the model are based on input features (such demographics, behavioral metrics, pre- and post-training scores, etc.).

This becomes a straightforward binary classification problem, which we then simplify:

A good indicator is the staff's secure behavior after training.

Negative (0): Employees continue to behave in a non-secure manner after training.

The support vector machine (SVM) model will determine whether staff behavior improves based on the input variables. The confusion matrix summarizes these predictions by showing the amount of successful predictions, the number of ineffective predictions, and the number of errors, broken down into false positives and false negatives. Key performance indicators provide a comprehensive evaluation of the model's reliability; these include **accuracy**, **precision**, **recall**, and the **F1-score**, which is the balance between recall and precision. **Accuracy** is the proportion of correct predictions. **Precision** is the reliability of "effective" predictions. **Recall** is the ability to identify all effective cases.

Using pre- and post-training data, you will construct a support vector machine (SVM) model to ascertain whether the workers' conduct has improved.

Evaluation Metrics:

Accuracy:

$$\frac{TP+TN}{TP+TN+FP+FN}$$

Precision:

$$\frac{TP}{TP+FP}$$

Recall:

$$\frac{TP}{TP+FN}$$

F1-Score:

$$2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

Where:

TP: True Positives, TN: True Negatives, FP: False Positives, FN: False Negatives

Following the SVM model's training using 80% training data and 20% testing data, we get the following outcomes:

Confusion Matrix:

Predicted / Actual	Effective (1)	Ineffective (0)
Effective (1)	35	5
Ineffective (0)	3	17

Output results explanation:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{35 + 17}{35 + 17 + 5 + 3} = 86.67\%$$

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{35}{35 + 3} = 92.1\%$$

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{35}{35 + 5} = 87.5\%$$

$$F1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} = 2 \cdot \frac{0.921 \cdot 0.875}{0.921 + 0.875} = 89.7\%$$

The statistics can tell us more about how the training program affected the cybersecurity expertise of the pharmacy personnel. The training seems to be effective in preparing employees to deal with cybersecurity threats, as shown by the model's high recall and accuracy rates. Looking at the relative importance of features might help you find the training gaps and fix a poorly performing model. Data analysis may also show if regular reviews or tailored training are needed to strengthen cybersecurity safeguards.

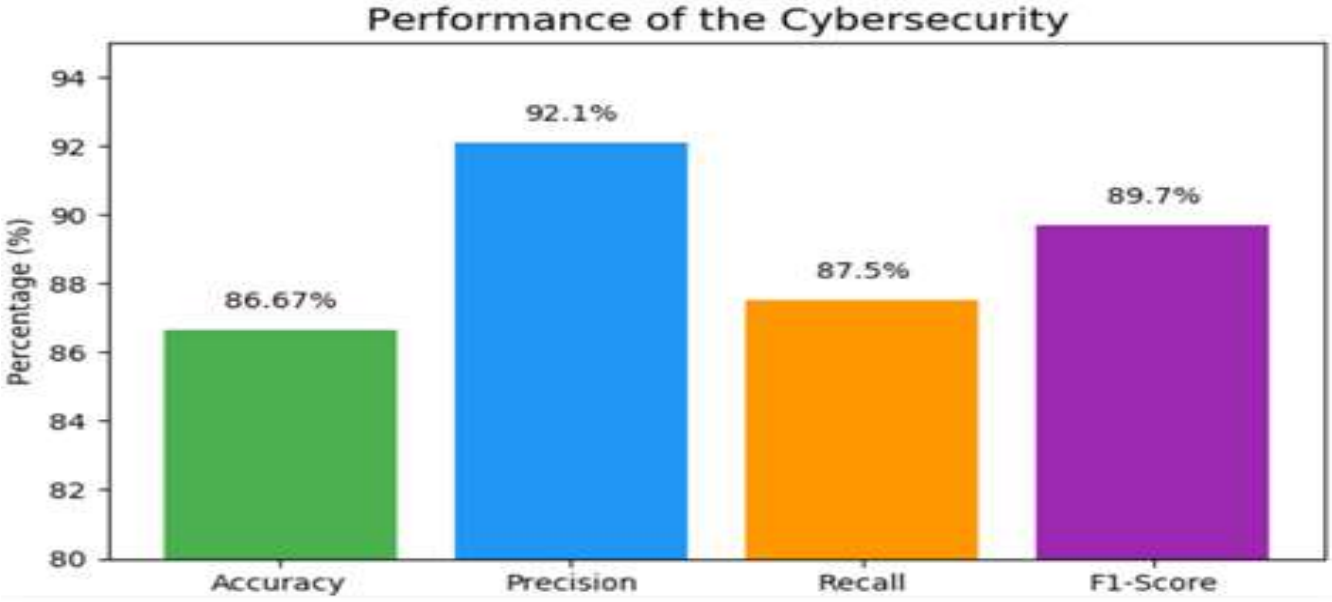
The algorithm has an impressive 86.67% success rate when it comes to predicting an employee's activities regarding security.

The algorithm accurately anticipates helpful actions with a 92.1% accuracy rate.

An impressive 87.5% accuracy rate indicates that the system can reliably anticipate that 87.5% of workers would exhibit a notable shift in behavior after training.

The model is well-balanced and performing well in terms of accuracy and recall, as shown by an F1-Score of 89.7 percent.

Figure 2. Performance of the Cyber Security



Here is the bar graph (Figure 2) illustrating the performance of the cybersecurity. It highlights key metrics such as accuracy, precision, recall, and F1-score. The chart clearly demonstrates the algorithm's high accuracy and balanced performance across these areas.

V. Conclusion

By conducting a thorough literature analysis, this study has accomplished several things: it has highlighted major findings, identified knowledge gaps, and proposed options for future research. The study's authors argue that cybersecurity curricula should reflect practical experience. Because of its depth and breadth, this training program could help businesses enhance the delivery of executive programs. By revealing the successes and failures of cybersecurity training programs, this kind of study may help improve their design and implementation. This technique has an impact on the efficacy of the training program, thus paying careful attention to it will greatly enhance a company's cybersecurity posture. With the use of a model that details how to develop and evaluate intervention programs, we were able to show how cybersecurity training affected user behavior. Organizations may potentially improve the effectiveness of staff training by taking into account the interplay between user characteristics, program design and delivery, and targeted objectives.

VI. References

[1]. Al-Ghamdi, M. I. (2021). Effects of knowledge of cyber security on prevention of attacks. Mater. Today Proc, 10.

[2]. Alkhazi, B., Alshaikh, M., Alkhezi, S., &Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. IEEE Access, 10, 132132–132143. https://doi.org/10.1109/ACCESS.2022.3230286

[3]. Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organisations. Information & Computer Security.

[4]. Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. Security and Privacy, 3(6), e126.

[5]. Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? ArXiv Preprint ArXiv:1901.02672.

[6]. Bandari, V. (2023). Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organisation Types. International Journal of Business Intelligence and Big Data Analytics, 6(1), 1–11.

[7]. Creutzburg, R. (2018). Cybersecurity and forensic challenges-a bibliographic review. Electronic Imaging, 2018(6), 100-1-100–116.

[8]. Crick, T., Davenport, J. H., Irons, A., & Prickett, T. (2019). A UK case study on cybersecurity education and accreditation. 1–9.

[9]. Dawson, A. (2019). Exploring strategies for implementing information security training and employee compliance practices. Walden University.

[10]. Fairburn, N., Shelton, A., Ackroyd, F., & Selfe, R. (2021). Beyond Murphy's Law: Applying Wider Human Factors Behavioural Science Approaches in Cyber-Security Resilience: An Applied Practice Case Study Discussing Approaches to Assessing Human Factors Vulnerabilities in Cyber-Security Systems. HCI for Cybersecurity, Privacy and Trust: Third International Conference, HCI-CPT 2021, Held as Part of the 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings, 123–138.

[11]. Falco, G. (2018). The vacuum of space cyber security. 2018 AIAA SPACE and Astronautics Forum and Exposition, 5275.

[12]. He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2020). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. Journal of Intellectual Capital, 21(2), 203–213.

[13]. Hussain, A., Mohamed, A., & Razali, S. (2020). A review on cybersecurity: Challenges & emerging threats. Proceedings of the 3rd International Conference on Networking, Information Systems & Security, 1–7.

[14]. Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 1–4.

[15]. Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. Journal of Organizational Computing and Electronic Commerce, 28(3), 269–282.

[16]. McLaughlin, K. L. (2023). DEFENSE IS THE BEST OFFENSE: THE EVOLVING ROLE OF CYBERSECURITY BLUE TEAMS AND THE IMPACT OF SOAR TECHNOLOGIES. EDPACS, 1– 7.

[17]. Nasir, S. (2023). Cybersecurity Awareness: Prerequisites for Strategic Decision Makers. In Cybersecurity for Decision Makers (pp. 383-393). CRC Press.

[18]. Nobles, C. (2019). Establishing Human Factors Programs to Mitigate Blind Spots in Cybersecurity. 7.
[19]. Rader, E., & Wash, R. (2015). Identifying patterns in informal sources of security information. Journal of Cybersecurity, tyv008. https://doi.org/10.1093/cybsec/tyv008
[20]. Rajamäki, J., Nevmerzhitskaya, J., & Virág, C. (2018). Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF). 2018 IEEE Global Engineering Education Conference (EDUCON), 2042–2046.
[21]. Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2021). An effective cybersecurity training model to support an organisational awareness program: The cybersecurity awareness training model (catram). A case study in canada. In Research Anthology on Artificial Intelligence Applications in Security (pp. 174–188). IGI Global.
[22]. Trim, P. R. J., & Lee, Y.-I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. Industrial Marketing Management, 83, 224–238. https://doi.org/10.1016/j.indmarman.2019.04.003
[23]. Trim, P. R., & Lee, Y.-I. (2021). The Global Cyber Security Model: Counteracting cyber attacks through a resilient partnership arrangement. Big Data and Cognitive Computing, 5(3), 32.
[24]. Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387.
[25]. Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? Computers in Human Behavior, 84, 375–382.
[26]. Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. Decision Support Systems, 108, 107–118.