Human Aspects of Security

Satya Shiva Sai Ram Kamma
Masters of Information Technology and Analytics
Rutgers Business School
Rutgers University, Newark, NJ, USA
sk2915@scarletmail.rutgers.edu

Sai Madhuri Naralasetty
Masters of Information Technology and Analytics
Rutgers Business School
Rutgers University, Newark, NJ, USA
sn917@scarletmail.rutgers.edu

Abha Tamrakar
Masters of Information Technology and Analytics
Rutgers Business School
Rutgers University, Newark, NJ, USA
at1379@scarletmail.rutgers.edu

***Abstract*—The "Human Aspects of Information Security" study delves into the pivotal role of human behavior and decision-making in the realm of digital information security, examining how factors like psychology, culture, and training impact data and system security. Its primary aim is to enhance our understanding of how to effectively engage and educate individuals about safeguarding sensitive information by exploring these influences. The findings underscore the importance of comprehensive approaches to information security, that consider both technological and human factors. In today's context, information security is a prominent and critical concern for individuals and organizations alike, given the financial losses and disruptions caused by cyber-attacks, including data breaches and production interruptions. These breaches can tarnish reputation, erode customer loyalty, and lead to financial penalties. Additionally, cyber-attacks impede business continuity, prompting organizations to manage information security to mitigate cyber risks, often employing the ISO/IEC 27001 information security management standard with its 114 controls spanning technical and organizational aspects. However, it's crucial not to underestimate the significance of individuals' information security behavior in security management. Relying solely on technology cannot guarantee the safety of information assets.**

***Index Terms*—Information Security, Data breaches, Cyber risks, Human aspects, information, Digital information security**

I. Introduction

In our world today where we are always connected Protecting our information through digital means. is absolutely necessary for individuals and companies. We're talking about protecting sensitive data, such as personal- structure, financial records, and intellectual property, namely Always under threat. equipped with stringent security measures And sophisticated technology is needed to protect this data, . We often overlook the vital role of humans Play in this safe environment. Surprisingly, a large portion. Security breaches can be caused by human error, negligence, or. Even if it is intentionally wrong. However, it is important to know That people can also be the first line of defense against the Internet Threats of various kinds [1]. It highlights these two elements of human involvement The person should be properly diagnosed, evaluated and cared for Aspects of Information Security. In this paper, as, . In our increasingly technology-dependent world, man Attitude, thoughts and decisions are absolutely essential In determining the security of our digital assets.

The literature survey exhibits that whilst full-size interest has been given to technical aspects of information protection. Yet, the importance of human elements has turn out to be an increasing number of diagnosed because technical solutions on my own can not sufficiently mitigate safety vulnerabilities. In addition, we are now connected more than ever and structures are becoming more complicated and if we've got clever devices, we want to have smart people as nicely. Therefore, in order for users to use facts structures securely, they ought to be nicely educated.

In the realm of training for facts protection, there are two number one strategies: the traditional technique and the customised method. The conventional approach, often called the "one-length-fits-all" approach, operates below the assumption that each one customers need to receive the identical training, even though the content material can be customized to suit a particular organisation's desires [1]. However, the traditional approach does not usually fit every situation and often falls short of handing over the desired results. For example, effective training ought to align with the specific necessities of users, thinking of factors like their know-how, attitudes, and behaviors regarding information protection. It have to also stay current with the ever-evolving panorama of cyberspace. Without this adaptability, education can turn out to be irrelevant or luxurious, probably causing customers to view it as an impediment rather than a advantage.

On the other hand, there's the personalized method, which tailors training to the unique desires of man or woman users. While this technique addresses some of the restrictions of the conventional technique, it introduces new challenges. Creating personalised training for all and sundry requires accelerated efforts and charges, which can be prohibitive. Consequently, the customised method is not generally carried out in practice. This paper pursuits to make clear how, in our world wherein we depend so heavily on technology, human behavior, thinking, and decision-making are simply pivotal in figuring out the security of our digital assets.

A. Impacts of Information Security Over the Years

- In 2023, humans were engaged in 70% of data breaches [5].
- In 2022, a data breach typically cost slightly less than $4.35 million. That is a record high [6].
- In 2020, just 1 in 9 organizations (11%) offered non-cyber staff a cybersecurity awareness program.

- Phishing is a factor in 1/3 of data breaches [6].
- Due to remote workers' lack of security awareness, 20% of firms experienced a security breach.
- The Federal Trade Commission was notified of about 1.1 million cases of identity theft in 2022 [4].

B. Human Aspect

Continuing schooling is critical to instill the significance of safeguarding the privateness of private identification information saved on smartphones. Moreover, it's far critical to provide steering on deciding on computer devices that include sturdy security structures. In the dialogue that follows, we are able to emphasize the five human factors that significantly have an impact on give up customers' conduct in this context.

1) Lack of Motivation : The loss of motivation within the realm of human factors of records protection is commonly rooted in a range of things, which includes a lack of knowledge approximately the related risks, the perception that safety features are inconvenient, complacency toward potential threats, an absence of personal duty, constrained get right of entry to to essential resources, resistance to adopting new safety practices, and the overall organizational culture. Effectively addressing this trouble entails businesses making large investments in complete security consciousness applications, simplifying protection protocols to lead them to more user-pleasant, cultivating a way of life where all employees take duty for protection, supplying the crucial tools and assets, placing management examples, and supplying incentives to inspire compliance. Regular education, constant communique approximately security, and the established order of clear consequences for non-compliance are pivotal in maintaining worker motivation and ensuring that facts security keeps its function as a pinnacle priority in the business enterprise.

2) Lack of awareness: One of the substantial demanding situations within the human element of information safety is the vast lack of knowledge among personnel. This trouble regularly stems from insufficient schooling and communique regarding the significance of safety features, capacity risks, and the wider consequences of protection breaches. When personnel don't hold close the vital role they play in safeguarding touchy statistics, they may be more likely to have interaction in volatile behaviors like falling for phishing scams, using vulnerable passwords, or mishandling personal information. To address this issue effectively, groups must provide top precedence to non-stop security focus programs, ensuring that employees are well-informed approximately the ever-evolving landscape of threats and their personal obligations in upholding a stable work environment.

3) Belief : Understanding and valuing the function of human factors in records security is important for organising a robust cybersecurity framework. This angle recognizes that people within an business enterprise can either bolster or weaken its security posture. It emphasizes the want for investments in security education, fostering a way of life in which everyone takes security severely, and making sure that employees have the equipment and knowledge to actively protect sensitive records. Without this reputation, companies grow to be greater at risk of cybersecurity risks bobbing up from human mistakes, carelessness, or unawareness, which cyber threats can exploit [2].

4) Behavior: It refers to selections and sports taken through people interior a corporation which have the electricity to improve or compromise cybersecurity. Adhering to hooked up security procedures, growing strong and one-of-a-type passwords, reporting any threats or incidents proper away, and being alert to phishing efforts are all examples of advantageous security behavior. Conversely, sharing passwords, disobeying security recommendations, acquiring files from unreliable resources, and falling for social engineering schemes which include phishing scams are examples of bad safety behavior. Establishing a robust security culture requires an knowledge of and capability to steer those behaviors. Human behavior regularly serves as the muse of an enterprise's safety posture, and coping with it requires a mix of organizational subculture that perspectives protection as a shared obligation, education, attention, and clean policies [3].

5) Inadequate Use of Technology : The hassle of no longer absolutely making use of generation within the context of human information safety is a sizeable difficulty. Even even though companies often spend resources on superior cybersecurity equipment, they occasionally pass over the critical role that generation can play in addressing protection risks related to human beings. Not embracing person-friendly technology answers for responsibilities like steady logins, computerized risk detection, and instructing users effects in protection vulnerabilities that stem from human errors or oversights. Integrating generation successfully can assist to mitigate those risks, providing a proactive defense against ever-changing cyber threats and operating along human efforts to preserve a stable virtual surroundings.

6) Computer security risks : The laptop protection dangers within the human factors of information safety in most cases stand up from the behaviors and movements of humans within an business enterprise. These dangers encompass insider threats, wherein employees might also, either intentionally or by chance, compromise data security, frequently due to carelessness, a lack of information, or malicious rationale. Social engineering attacks, like phishing, make the most human psychology by means of manipulating consider and curiosity to benefit unauthorized get entry to to laptop systems. Common unstable behaviors contain susceptible password practices, sharing touchy facts, and downloading potentially dangerous content, all of which can create protection vulnerabilities. The state of affairs is worsened by insufficient safety cognizance and schooling. The human factor often represents the weakest link in an agency's protection, underscoring the need for non-stop schooling, strict coverage enforcement, and fostering a cybersecurity-aware lifestyle.[1]

C. Human Aspects of Information Security Questionnaire (HAIS-Q)

Traditionally statistics protection has been basically addressed via technical solutions implemented within the later stages of software development This method perspectives protection as an additional characteristic which means that once vulnerabilities floor they're usually dealt with via security patches While technical answers in data protection are undeniably crucial they by myself are not enough to ensure comprehensive security Human factors regularly play an excellent more extensive function in accomplishing strong statistics protection Users of records systems showcase variations in their know-how attitudes and behaviors associated with security To examine facts security performance comprehensively the HAISQ Human Aspects of Information Security Questionnaire was advanced HAISQ evaluates users records protection knowledge attitudes and behaviors in seven key regions password control e mail utilization internet usage social media interest cell device usage incident reporting and data coping with This questionnaire has gained reputation in both scientific and expert circles and has been applied in numerous studies research For example people who scored higher on the HAISQ verified better performance in a phishing test suggesting that it is able to function a treasured predictor of records security behavior Similarly studies indicates that numerous elements assessed by using the HAISQ are associated with improved cyber hygiene Furthermore HAISQ was hired in a take a look at that exposed gender variations in information protection recognition [7].

TABLE I
FOCUS AREAS WITH REPRESENTATIVE AREAS.

Focus Area	Areas
Password Management	Using the same password Password sharing
Email use	Forwarding emails Opening attachments IT department level of responsibility
Internet use	Installing unauthorized software Accessing dubious websites Inappropriate use of internet
Social networking site use	Amount of work time spent on SNS Posting about work on SNS
Incident reporting	Reporting suspicious individuals Reporting bad behavior by colleagues Reporting all security incidents
Information handling	Disposing of sensitive documents Inserting DVDs/USB devices Leaving sensitive material unsecured

II. PROBLEM DEFINITION

One of the most superb challenges inside the realm of human additives of protection is the inherent susceptibility of human behavior to a massive range of threats and assaults. This particular field, the hard dynamics of the way people engage with safety structures, regulations, and tactics. It encompasses a mess of key demanding situations, inclusive of the exploitation of trust and emotions in phishing and social engineering, the prevalence of susceptible password control practices, the insufficient degree of protection reputation amongst people, the tricky complexities surrounding the identification and prevention of insider threats, the impact of cognitive biases on protection-associated selection-making, the delicate equilibrium among supplying a superb purchaser revel in and implementing strong safety features, the demanding situations related to making sure compliance and coverage adherence, the vulnerabilities that get up within the context of cell and faraway artwork, the often underestimated protection implications of IoT devices, and the pivotal function that human elements play in the physical protection location.

In an organization's security setup, it is a widely diagnosed truth that people can frequently be the weakest link in terms of safeguarding records. They are susceptible to manipulation with the aid of attackers who make the most this vulnerability to acquire sensitive records. This susceptibility can occur in numerous approaches, including when human beings open seemingly harmless but truely malicious emails out of interest, recklessness, or negligence. Similarly, users who down load software program from sources which are unverified and now not steady can by chance expose the employer to cybersecurity dangers. These vulnerabilities are frequently a result of a lack of awareness about safe faraway paintings methods, unintended sharing of remote work device with 0.33 events, deliberate actions that could prefer competition, or actually a loss of adherence to protection protocols.

The onset of the COVID-19 pandemic has in addition complex the mission of tracking and ensuring steady worker conduct. The shift to faraway paintings has allowed employees to get right of entry to sensitive records on their personal devices, which has, in turn, multiplied the capability for protection breaches and made systems more susceptible. As a result, even when companies have well-set up policies and programs designed to train users about statistics safety, the assignment of correctly tracking user compliance and protecting touchy records has turn out to be more and more daunting.

It's essential to emphasize that the human detail introduces essential vulnerabilities, which include negative password practices, susceptibility to phishing attacks, and a lack of protection attention. Therefore, addressing those human related vulnerabilities is paramount for preserving the safety of touchy facts and preventing attackers from infiltrating the company's structures thru any viable approach [9].

III. EXISTING SOLUTIONS

The pursuit of solutions for these demanding situations demands a multifaceted strategy that encompasses education and training, the improvement of consumer-pleasant interfaces, the implementation of powerful security regulations, and the cultivation of a way of life deeply rooted in security cognizance inside companies. Recognizing the irreplaceable role that human beings play in the security panorama, it's miles vital to consciousness on each mitigating their vulnerabilities

and empowering them to function the primary line of protection towards a numerous variety of threats.

A. Training and Awareness Program

Many corporations have instituted worker schooling and consciousness tasks designed to reduce safety dangers related to human movements [8]. These applications have the overarching intention of teaching personnel in security great practices and enhancing their expertise of capacity threats. Nonetheless, their success varies, and the sustained retention of security understanding poses an ongoing task.

Organizations have also integrated simulated phishing assaults as a education tool to help personnel in growing the capacity to differentiate between legitimate emails and phishing attempts. These simulations attention on dissecting various factors within emails, consisting of their source and issue strains, to foster a deeper expertise of e-mail security.

B. Phishing Aware Programseness

Phishing attention applications are a essential element of addressing the human factors of protection inside an company. Phishing attacks regularly make the most human vulnerabilities, and educating employees to recognize and reply to these threats is crucial.

An instance of a phishing attack has been parent under, where the attacker sends a fraudulent e mail to an man or woman. When someone clicks on a link or opens an e mail, crucial data are stored and sent to the attacker.

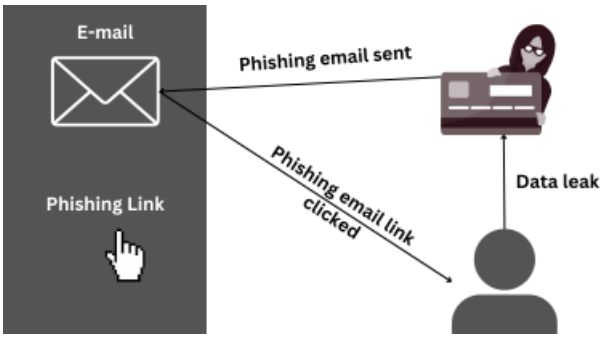

Fig. 1. Phishing Attack

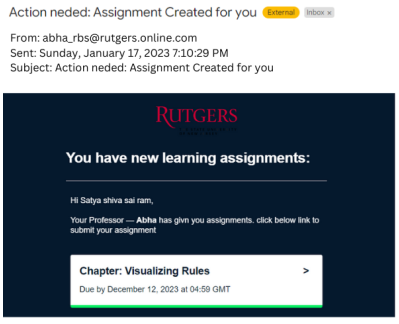

Fig. 2. Phishing Attack E mail Example

1) Example of Phishing Aware Programseness:

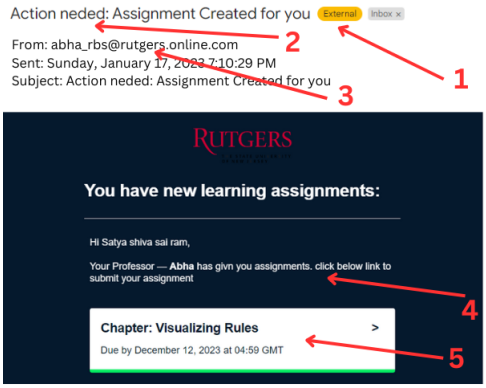

Fig. 3. Phishing Attack E mail Example Points

C. Biometric Authentication

Biometric authentication techniques, inclusive of fingerprint and facial recognition, goal to lessen reliance on traditional password-based systems. While they could beautify security, they are no longer without their vulnerabilities, and ethical concerns surround the gathering and storage of biometric statistics.

Using biometric authentication guarantees that best authenticated humans enter the premises where sensitive statistics may be accessed. However, unusual times like the COVID-19 pandemic challenged this approach of authentication as the personnel may want to get entry to the information remotely with out requiring any biometric authentication.

D. Access Control

Access manipulate guidelines are implemented to restrict each consumer from gaining access to sensitive facts. Based at the function of a person in an business enterprise, they may be given a few privileges, which decide what statistics the person can be able to access and what operation the consumer can carry out on available statistics.

Fig. 4. Access Control

Organizations regularly use firewalls to limit the get entry to of unverified web sites from the computer systems, which helps them in preventing the down load of any suspicious, unwanted document or software.

E. Social Engineering Training

Social engineering training plays a pivotal position in cybersecurity cognizance and schooling projects. It is instrumental in fortifying defenses against the foxy techniques employed with the aid of cybercriminals who take advantage of human psychology to extract sensitive information, advantage unauthorized gadget get entry to, or manipulate individuals into compromising safety.

F. Continuous Monitoring and Assessment

Continuous monitoring and assessment, particularly from the attitude of human factors of statistics safety, plays a important position in retaining a secure and resilient organizational surroundings. It entails no longer only technological solutions however additionally human attention, vigilance, and behavioral issues.

IV. NEW SUGGESTION

Since the world of information security is always changing, there are always new concepts and techniques that must be taken into consideration. Below are some newly developed information security human aspects:

A. Using Generative AI to provide

Generational artificial intelligence shows opportunities for improving our protection protocols via bringing powerful content scanning capabilities. We can now actively discover and mitigate possible protection troubles by cautiously analyzing and analyzing content thanks to this technology. An organization may additionally beautify its defenses and create an effective and attentive security framework by using utilising the capacity of generative AI. As a end result, we are able to actively look for and deal with new threats in our virtual environment, guaranteeing an increased degree of protection.

1) Threat Alerts & Tips: Large language models (LLMs) can be trained by businesses the use of specialised facts to provide users with real-time notifications. For example, a generative AI device can alert users without delay to phishing or malware attacks and provide steerage on a way to stay steady. Additionally, customers can ask the device protection-related questions, which makes it a useful tool for anybody. In this manner, we rent generation in a clear and approachable way to guard all and sundry from on line threats and to hold each person informed.

2) Reminders & Nudges: We need reminders and forces to live secure whilst using the net. They incorporate important warnings approximately such things as software software updates and stay clean of suspicious internet web sites or downloads. These exceptional prompts serve as beneficial reminders to assist us recall to be cautious and take the desired precautions to protect our on line interest. We can virtually remember to maintain a safe on line environment through making matters clean to recognize.

3) Generate Strong Password: Keeping our debts steady calls for us to create robust passwords, and synthetic intelligence (AI) can help with that. Our enterprise's password rules may be used to train AI models to generate steady passwords. When a consumer attempts to create a password, generative AI gear can take that password and enhance it in a way that the person can nevertheless take into account. By doing this, we will make sure that our passwords are strong and provide our bills with any other level of security.

B. Interactive Training Sessions

Drama, storytelling, and games are used to create an interesting surroundings that matches in-individual group interactions all through the education periods. We want to frequently reveal the situation and create the whole lot with the user in thoughts. We use net channels to speak fulfillment memories and to award recognition and prizes a good way to preserve anyone engaged. To make the schooling applicable and practical, we additionally comprise case studies and scenarios from real-world situations. We've also planned a security attention day a few times per week to provide everybody inside the company with regular updates on safety insights and to make sure they're all aware of the most recent advancements within the area of place of work safety.

1) Gamification: Gamification is the process of incorporating game elements into security training, and it can greatly boost engagement and effectiveness. By creating games, challenges, and simulations, users get to learn about identifying and tackling security threats in a fun and interactive way. Gamification makes security training more immersive and memorable, which is not only engaging but also motivating. Users are put into real-world scenarios, which encourages them to apply security practices in a practical context. There are systems for progression, rewards, and friendly competition to create a sense of accomplishment. Plus, immediate feedback and data analysis help in continuous improvement. All of this contributes not only to engaging security training but also to nurturing a security conscious workforce that is more adept at recognizing and responding to threats effectively.

2) Understanding Behavior of User by Story: Organizations can detect and track irregularities in user behavior, which may serve as precursors to possible security risks, by utilizing the potential of behavioral analytics. This meticulous process entails a thorough examination of user behavior inside an organization's digital environment, considering variables such as access points, login duration, and the particular information that users tend to interact with. These analytical insights are essential for spotting security flaws, especially those involving compromised accounts and insider threats. When a trusted entity or person deviates from their usual usage patterns, behavioral analytics can identify this and warn the possibility of an insider threat. It can also quickly identify sudden and unusual changes in account activity, which could indicate that the account has been compromised. Basically, by identifying abnormal behavioral patterns, this technique strengthens an

organization's overall security posture by enabling proactive identification and mitigation of security vulnerabilities.

3) User-Centric Security Training: Conventional security training typically places a strong focus on policies, technical protocols, and adhering to compliance standards, all of which are undeniably important in safeguarding an organization's digital assets. However, this approach tends to overlook a critical aspect of security – the human element. A more effective approach to cybersecurity training involves a paradigm shift, placing users at the center of the security equation. This strategy acknowledges that users, whether they are employees, contractors, or even customers, often serve as the initial line of defense against security threats. By instilling a profound sense of individual responsibility and stressing that security is a collective concern, organizations can cultivate a pervasive culture of security awareness. Furthermore, by imparting practical skills and knowledge for identifying and responding to security threats, users are equipped with the tools they need to actively contribute to safeguarding sensitive information and systems. This approach transcends the mere adherence to policies and transforms users into proactive, vigilant protectors of their digital environments, thus fortifying an organization's security posture, making it more resilient and robust.

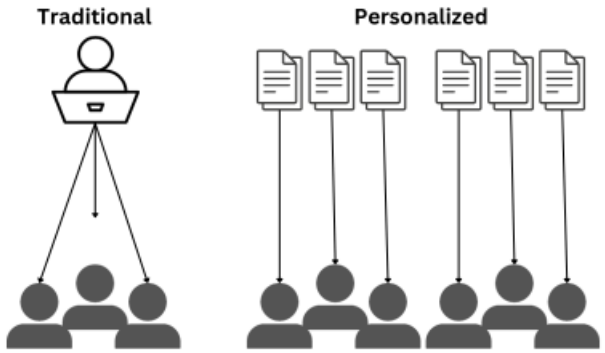

Fig. 5. User-Centric Security Training

C. DevSecOps

When contemplating the human dimensions of security, our focus typically gravitates towards application users. However, a critical component of this realm encompasses the developers and testers responsible for crafting the code that drives these applications. Therefore, it is imperative to prioritize the human element concerning developers, testers, and individuals involved in code creation, as their actions can potentially expose the entire application to security vulnerabilities. Because of our growing dependence on generation, it's miles essential that we hire stable code. Some teams have a selected information protection institution that approves and monitors gadgets with the intention to do that. DevSecOps is one approach this is turning into an increasing number of commonplace, in which protection is included into the operations and improvement approaches. This approach makes use of techniques and gear to guarantee that the code is secure from the beginning. A crucial factor of this is stable code, which enables to close protection holes that might permit assaults like SQL injection and cross site scripting (XSS) to occur. In order to make sure that this system is much less prone to ability assaults, it's far important to become aware of and endorse alternatives to the harmful code if there exist vulnerabilities.

V. IMPLEMENTATION

A. Generative AI Tool for Support

Generative AI has become ubiquitous, allowing us to harness the capabilities of AI. Despite comprehensive training and workshops, individuals may occasionally act carelessly, inadvertently clicking on suspicious links or downloading content from unverified sources. The integration of this generative AI tool introduces an additional layer of protection. The tool assists users in various ways listed below, thereby reducing the likelihood of unintentional security breaches. The following use cases were determined after a comprehensive review of the organization's data and identification of areas where users require assistance. 1. Threat Alert and Tips: This ensures that users receive real-time alerts and tips concerning potential security threats. For instance, when a new email is received, the AI tool conducts an initial scan based on the conditions and models it has been trained on. It assesses whether the email exhibits signs of being suspicious. If it does, the user receives an alert prompting them to report the email to the IT security team. Otherwise, the email is treated as normal, allowing the user to proceed with their usual actions. The alert will also furnish the user with informative points, detailing specific parameters that render the email suspicious. This information equips users with knowledge they can apply in similar situations in the future. One such use case is shown in the result section. 2. Reminders and Nudges: Our research underscores the vulnerability posed by outdated software that ceases to receive support or security patches. Users may inadvertently neglect timely updates, exposing the system to potential risks. Additionally, user behavior, such as carelessness while browsing insecure websites and downloading executables from the internet without scrutiny, can pose substantial threats. It is crucial to recognize that these activities can jeopardize the security of not only the system but also applications and the entire network. As the saying goes, it takes just one weak link to compromise the entire chain. Our tool adds an additional layer of protection in this context by offering reminders and nudges to users. This helps enhance user awareness and vigilance, reducing the likelihood of security lapses such as delayed software updates or careless online behavior. 3: Strong Password Generation: From our day-to-day experiences, we often set numerous login passwords, and in an effort to make them easy to remember, we may opt for simplistic passwords. However, this practice poses a significant risk to the entire system's security. Our tool is designed to enhance the strength of your passwords. It seamlessly reviews the password you are attempting to set,

assesses its strength, and then offers you a more robust version to bolster the security of your credentials.

Now that we have a clear understanding of the use cases and possess all the necessary data to train our large language models, the subsequent steps involve training the models, rigorously testing them on real-world data, and ultimately releasing the models for user utilization. This iterative process ensures the models are well-tuned, effective, and capable of delivering reliable performance in real-world scenarios. Since we don't have AI expertise in the group, we haven't built the tool end to end, however a use case is shown in the result section.

B. Interactive Training Sessions

Through the use of gamification and understanding user behavior through storytelling, we are introducing User-Centric Security Training. Every user will receive training based on their interests, making the learning experience personalized and engaging

1) Gamification: With the help of artificial intelligence (AI), we are developing a gaining knowledge of internet site. You might also learn about protection by taking interesting quizzes at the website. There are numerous classes for the quizzes, and you can select the only that interests you. You then continue to the quiz questions after deciding on a set. The plus facet is that you may get hold of a special certificate as a prize in case you carry out properly on the quiz! However, we might not prevent there. In order to make mastering approximately safety even extra interesting, we're additionally thinking about including informative stories and games.

2) Understanding Behavior of User by Story: Firstly, we will create an artificial intelligence (AI)-trained learning platform. With various screens where you can read stories and learn about staying safe online, it's going to be entertaining. We'll divide the stories into many categories so you may select your favorite. After selecting a group, you will be directed to the story screen, where you will read a narrative and respond to certain questions. You will receive a certificate of completion as proof of your excellent performance after completing the story and answering the questions correctly.

C. DevSecOps

In order to promote secure coding practices among individuals involved in code development, it is essential to establish both tools and teams dedicated to the ongoing monitoring, review, and approval of code before its deployment into the production environment. The following steps were involved in implementing DevSecOps The following use cases were collected to create the tool that will review and approve the code. 1. Input Parameter Validation When employing methods that involve writing information to the database, it is crucial to validate inputs thoroughly. Unvalidated inputs can potentially enable attackers to inject malicious code, which, if stored in the database without validation, may be retrieved and displayed on the user interface. Clicking on such content could lead to the installation of viruses, posing a significant risk to the security of the machine, application, or network. 2. Review Dynamic Queries: Dynamic queries are database queries that resolve the values of some parameters dynamically. If the value of these parameters is not validated, the can release sensitive information from the database to unauthorized people, which can put the organization and it's clients at risk. 3. Provide Issue Description: In addition to code reviews, it holds equal significance to educate individuals engaged in coding. This education should encompass an understanding of why certain code is deemed insecure, identification of existing gaps, and exploration of potential solutions to address these vulnerabilities. Individuals often learn valuable lessons from their personal experiences, reducing the chances of repeating a mistake they have addressed in the past.

Now that the requirement analysis is done, next steps would be to implement these use cases and carry out testing and finally release it for the users to use. We haven't built the tool end to end, however, we have implemented some of these use cases that'll be shown in the results section.

Additionally, following policies were created for the information security team to review code. 1. External Libraries: This is implemented to guarantee the exclusive use of approved libraries and tools for code development and test cases. The utilization of external libraries, if discovered to be vulnerable later on, poses a significant risk to the organization, jeopardizing revenue, reputation, and client relationships. If usage of such libraries is found, IS team would reject the code, asking for improvement. 2. Near Obsolete Code: This is performed to identify soon-to-be-obsolete methods, ensuring the use of firm-approved versions of libraries that offer the latest features and bug-free code. This practice ensures that the code remains functional for an extended period, eliminating the need for frequent updates to maintain compliance. If such methods are used, IS team would reject the code, asking for improvement. 3. Data Encryption: This process aims to pinpoint sensitive data that necessitates encryption or masking. Additionally, it establishes protocols to prevent unauthorized visibility of this data, ensuring stringent controls and privacy measures. If such data is not encrypted or masked, IS team would reject the code asking for improvement. 4. Secure User Session Management The IT security team will also assess whether the code has the capability to maintain secure user sessions resistant to hijacking. If this criterion is not met, the IT security team would reject the code, requesting the inclusion of code dedicated to secure user session management.

With our objectives clearly defined, the subsequent steps involve the recruitment of an IT security team to implement these policies. We advocate for the establishment of a dedicated IT team, as our research indicates that many security breaches stem from organizations lacking a proactive information security strategy. In such cases, security measures tend to be reactive, with organizations addressing breaches after they occur rather than implementing preventive measures.

We strongly recommend aligning the information security strategy closely with the corporate strategy. This alignment ensures that security considerations are integrated into the

core business objectives from the outset, rather than being an afterthought. The proposed IT security team should work diligently and continuously on refining and implementing this strategy, aiming to create a robust and proactive security posture for the organization.

VI. Results

A. Generative AI Tool for Support

Use case 1:

```
validateMessage(message){
whiteList = {"rutgers.edu",
    "morganstanley.com", "amazon.com"};
String senderDomain =
    message.extractSenderDomain();
if(!whiteList.contains(senderDomain)){
sendAlert(Mail originated from an
    unrecognized domain,
do not click the attachment, please report
    it);
}
}

Input:
abc@xyz.com

Output:
Mail originated from an unrecognized domain,
    do not click the attachment, please
    report it
```

The above code demonstrates a scenario where the tool generates an alert if the sender's domain is not present in the organization's whitelist of approved senders. This mechanism helps enhance security by flagging potential unauthorized or suspicious senders based on their email domains. eg if the sender is abc@ally.com, user will get an alert, if the sender is among rutgers, morganstanley or amazon, no alert will be sent to the user.

Use case 2:

```
validatePassword(userPassword){
Boolean isWeak = checkPassword(userPassword);
if(isWeak){
String strongPwd =
    generateStrongFromGivenPwd(userPassword));
}
return strongPwd;
}

Input:
value of user entered password = Password1
Output:
Suggested strong password = P@$$w0rd1
```

In this case, when a user attempts to set a simple password for login, the tool will assess the password's strength. If the password is deemed weak, the tool will suggest a more robust version. The user then has the option to either adopt the suggested password or choose another one from their end. This process aims to encourage the use of stronger and more secure login credentials. For instance, if the user entered 'Password1' as password then the tool will suggest {Pssw0rd1} a stronger version of that password.

B. Interactive Training Sessions

Here is a more thorough and intricate illustration of the gamification-ready user interface.

Screen 1: Start Screen Screen 2: Category selection screen Screen 3: Certification Screen

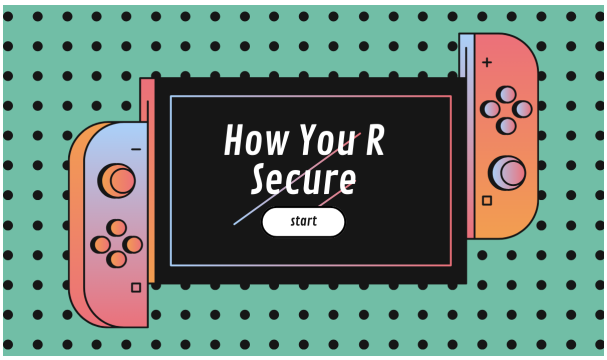

Fig. 6. Screen 1

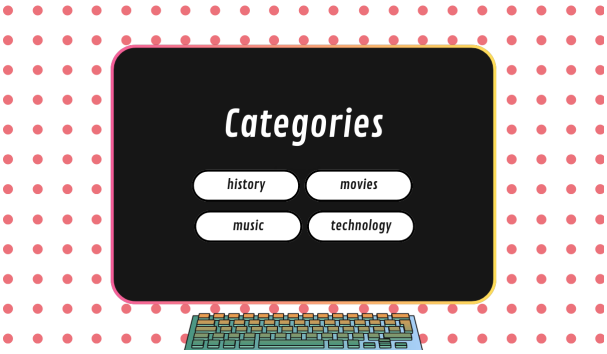

Fig. 7. Screen 2

Fig. 8. Screen 3

Screen designed for Understanding Behavior of User by Story Screen 1: Screen 2: Screen 3: Screen 4: Screen 5:

Fig. 9. Screen 1

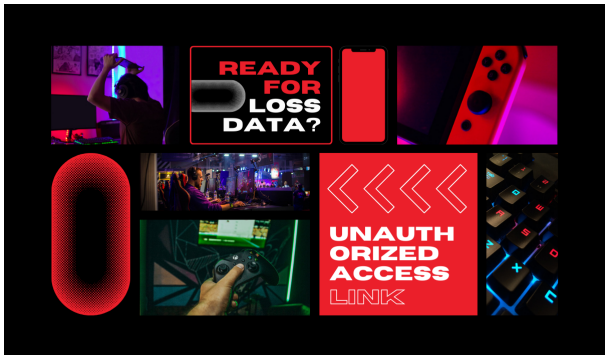

Fig. 10. Screen 2

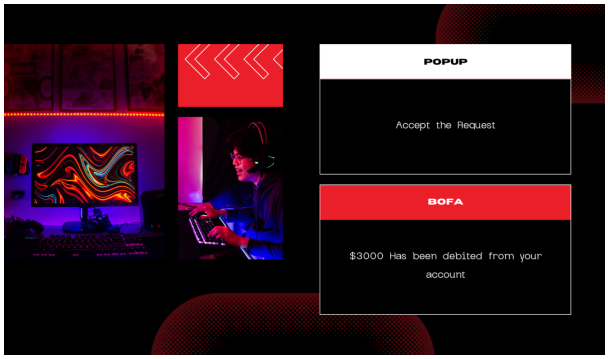

Fig. 11. Screen 3

Fig. 12. Screen 4

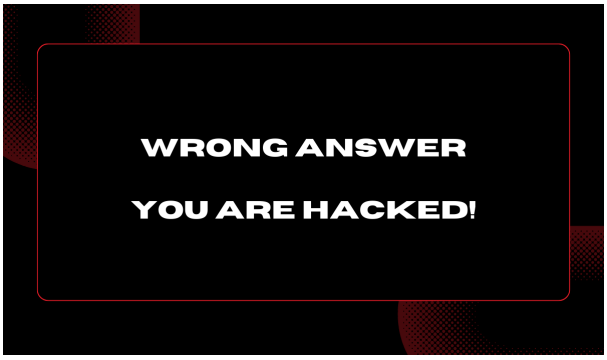

Fig. 13. Screen 5

C. DevSecOps

Vulnerable code written by a developer:

```
public class Products {
   public static void main(String args[]) {
     String country = "United States";
     String isReleased = "0";
     Map<String, List<String>> result = new
         HashMap<>();
     result = getProductDetails(country,
         isReleased);
   }
      Map getProductDetails(country,
          isReleased){
      return
          dbService.getProductDetails("Select
          * from Products where country in "
          + country + "and isReleased = "+
          isReleased);
   }
}
```

The provided code exhibits two potential security vulnerabilities that could lead to unauthorized data exposure: No Validation in getProductDetails Method: The code does not validate the input value for the 'country' parameter in the getProductDetails method. If an user intentionally sends a value such as 'Select * from countries,' and the query is executed successfully, it could return sensitive information for all countries. Implementing proper input validation is crucial to prevent SQL injection attacks.

Potential Data Exposure with isReleased Flag: The 'isReleased' flag is used as input, where a value of 1 represents products already released, and 0 represents products to be released in the future. However, if someone sends the value 0, the code returns sensitive information related to unreleased products. To mitigate this, access controls should be implemented to ensure that sensitive information is not disclosed to unauthorized users.

The tool will not pass approval checks on this code and will recommend the following improvements to enhance security: Add validation for country field: Implement validation for the 'country' field using a valid regex pattern. Additionally, scan the input against a predefined list of valid countries to ensure

that only legitimate values are accepted. Dynamic setting of isReleased value: Instead of taking the 'isReleased' value directly from the input, set it based on the user's level or role. This ensures that users with different privileges have access to the appropriate information and prevents unauthorized access to sensitive data. Exception Handling: Add robust exception handling to gracefully handle unexpected input parameters. This helps prevent unintended errors and enhances the overall resilience of the code.

By incorporating these suggestions, the code can be strengthened against potential security vulnerabilities and improve its overall reliability.

Here is secure version of above code:

```
public class Products {
  public static void main(String args[]) {
    String country = "United States, Mexico";
    String userLevel =
    Map<String, List<String>> result = new
        HashMap<>();
    result = getProductDetails(country,
        userLevel);
  }
     Map getProductDetails(country,
         userLevel){
     String isReleased = 1;
    if(userLevel >= 5){
    isReleased =  0 ;
    }
   validateCountry(country);
  return dbService.getProductDetails("Select
      * from Products where country in " +
      country + "and isReleased = "+
      isReleased);
  }
  }
  validateCountry(country){
  String inputCountries =
      country.toCharArray(,);
  forEach(String country : inputCountries){
  if(!validCountryList.contains(country)){
  Throw validationException(Provided country
      list is not valid);
  }
  }

  Output:
  Provided country list is not valid
```

That's a positive step towards enhancing security. By validating the input countries against a list of valid countries, you are mitigating the risk of unauthorized queries and potential data exposure. This measure ensures that the code will only proceed with the database query if the input countries match the predefined list of valid countries, adding an additional layer of protection against malicious input. Keep in mind to maintain and update the list of valid countries to reflect any changes over time.

VII. Conclusion

Information security requires a deep information of how individuals act. The human aspect of the security of data calls for cautious attention and can not be overlooked. Providing appropriate training and elevating humans's cognizance of security features can assist lower the possibility of a facts leak. In addition to advances in technology come new techniques for stopping errors made by using humans from becoming problems. Thus, maintaining a watch on how people engage with statistics safety, supplying them with best training, and making sensible use of era can all make contributions to the protection of our records.

VIII. Work Load Distribution

To properly manage the project, we carefully considered how to assign the tasks to the members of our team. We examined various project components and delegated responsibilities according to individual skill levels. Once we had assigned roles, we convened to discuss our findings. We had a great discussion, exchanged ideas, and challenged each other's presumptions. Working together, we were able to figure out the problems and analyze the advantages and disadvantages of different solutions. We effectively distributed the work and ensured that all suggestions were taken into consideration by assigning jobs based on strengths. The project was effective because of this careful technique, which also enhanced our knowledge of the subject and our ability to solve problems. We often utilized the internet to get some basic ideas to proceed with this project.

References

[1] W. A. Cram, J. G. Proudfoot and J. D'arcy, "Organizational information security policies: a review and research framework", European Journal of Information Systems, vol. 26, no. 6, pp. 605-641, 2017.

[2] R. von Solms and J. van Niekerk, "From information security to cyber security", Computers & Security, vol. 38, pp. 97-102, 2013.

[3] R. Torten, C. Reaiche and S. Boyle, "The impact of security awarness on information technology professionals' behavior", Computers & Security, vol. 79, pp. 68-79,

[4] U.S. News. (2022, December). Identity Theft Fraud Survey. U.S. News & World Report. https://www.usnews.com/360-reviews/privacy/identity-theft-protection/identity-theft-fraud-survey

[5] Verizon. (2023). "Data Breach Investigations Report." Verizon. https://www.verizon.com/about/news/2023-data-breach-investigations-report

[6] IBM. (2023). "Data Breach Investigations Report." IBM. Available: https://www.ibm.com/reports/data-breach

[7] McCornac,A., Calic,D., Parsons,K., Zwaans,T., Butavicius,M., & Pattinson,M.(2016). Test- check trustability and internal thickness of the mortal Aspects of Information Security Questionnaire(HAIS- Q). Australasian Conference on Information Systems.

[8] B. S. Tolley, "Identifying users through a segmentation study", J. Marketing, vol. 39, no. 2, pp. 69-71, Apr. 1975.

[9] D. Fujs, S. Vrhovec and D. Vavpotič, "A novel approach for acquiring training and software security requirements", Proc. Eur. Interdiscipl. CyberSecur. Conf., pp. 1-2, Nov. 2020.