INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

THE HUMAN FACTOR IN CYBERSECURITY: UNDERSTANDING AND MITIGATING THE ROLE OF HUMAN BEHAVIOUR IN SECURITY VULNERABILITY

AUTHORED BY: ANUSHKA SHARMA

Abstract:

In the domain of cybersecurity, technological solutions and protocols have traditionally been the focus of research and development efforts. However, the human factor plays a crucial role in the efficacy of security systems, often serving as the weakest link in cybersecurity defenses. This paper explores the multidimensional impact of human behavior on cybersecurity, analyzing how psychological, behavioral, and organizational factors contribute to security breaches. We examine various case studies that demonstrate the prevalence of social engineering attacks, poor security hygiene, and the failure to adhere to security protocols due to human error or oversight.

Additionally, we discuss the psychological tactics employed by attackers, such as phishing and pretexting, which exploit human vulnerabilities. The paper proposes a holistic approach to cybersecurity, recommending strategies to enhance human factors engineering and advocating for continuous education and training programs to reinforce security-aware behavior among users. By integrating behavioral science with cybersecurity practices, the paper aims to offer insights into developing more robust security frameworks that consider both technological and human elements. The goal is to shift the paradigm from a solely technology-centric to a more human-centric approach in cybersecurity strategies, thereby reducing risk and enhancing overall system resilience.

 ISSN: 2582-6433

Introduction

In the dynamic field of cybersecurity, where threats seem to be lurking around every digital bend, it is easy for most businesses to focus on providing solutions to technological challenges.[1] The National Initiative for Cybersecurity Careers and Studies defined cybersecurity as the activity, process, ability, capability, or state by which information and communication systems and the information contained therein are protected from and/or defended against damage, unauthorized use, modification, or exploitation. In the face of an increasingly complex and dynamic cyber threat landscape where 57% of businesses now anticipate an IT security breach, most organizations in the world are more focused on developing cutting-edge software on a regular basis to fend off external threats. Today, most businesses and organizations still rank cybersecurity as their top issue. But in the complex web of firewalls, encryption methods, and intrusion detection systems, the human factor is frequently overlooked. The human factor serves as the weakest link in the cybersecurity chain and also a critical component, however public awareness of cybersecurity and its accessibility to regular users remain low.[2] Either deliberately or not, anyone can fall victim of cybersecurity breach posing harm to oneself or their organization. By using social engineering tactics to exploit cybersecurity specialists' human weaknesses, attackers can also target these professionals.

Many businesses prioritize technology advancements and regulations over employee training

[1] https://www.upguard.com/blog/human-factors-in-cybersecurity
[2] https://securityscorecard.com/blog/the-human-factor-in-cybersecurity/

 ISSN: 2582-6433

or increasing cybersecurity awareness when it comes to cybersecurity. As a result, both technology and policy fail. Even with top-notch security systems, just one misplaced password or click on the wrong link can cause a ton of trouble. To safeguard our digital universe, we need to prioritize getting into the heads of cybercriminals and mastering the ways that humans behave and think.

From unintentionally falling prey to phishing scams and accidentally revealing sensitive data through insecure habits, human error continues to play a major role in cybersecurity breaches.

Understanding the importance of human elements in cybersecurity is not about pointing fingers or making excuses; it is about recognizing the depth of human nature and incorporating this insight into cybersecurity plans. In this paper, we investigate the many aspects of human factors related to cybersecurity, including user behaviors, training, awareness, and also explore several ways to curb cybersecurity threats. Our goal is to build a stronger, longer-term defense against cyber-attacks by understanding the human side of security and, ultimately, changing people's behavior. By exploring the aforementioned, proper strategies to mitigate against the human errors and manipulation in cyber security can be analyzed.

User Behavior in Cybersecurity

The actions and activities of users on their various digital platforms is an essential part of cybersecurity. In the context of cybersecurity, user behavior denotes the actions, choices, and routines that influence the safety of digital systems, networks, and information.[3] The

[3] https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf

 ISSN: 2582-6433

relationship between the actions taken by people and technological defenses is extremely important and must be properly understood to formulating secure strategies and cutting risk moments. Though advances in encryption and intrusion detection systems may increase overall digital security, what users do still is the crucial factor to either building a strong cyber defense against attackers or exposing businesses to several risks. Verizon's 2021 Data Breach Investigations Report revealed that 85% of data breaches are caused by human errors, especially those associated with phishing attacks. Verizon also found that a third of breaches incorporate phishing as a tactic.

In recent cybersecurity incidents, cyber attackers typically target users' minds rather than the computer system itself. For instance, they may use social engineering— which involves tricking users into divulging passwords—and cognitive hacking—which involves disseminating false information—as methods of hacking into a network or computer system an ongoing danger, taking advantage of how users are inclined to believe and communicate with messages that seemingly appear genuine. By clicking on these messages, cyber attackers get access to the sensitive information of users/organizations. These messages are known as threat vectors, as seen by the Cybersecurity and Infrastructure Security Agency (CISA), which stated that 91% of data breaches succeed after a phishing email is received (CISA, n.d.). IBM Security's study found that the average expense for a data breach post-phishing email is $4.24 million (IBM Security, 2021). Additionally, according to APWG, social media accounted for 42.8% of all phishing assaults in Q42023, making it the most targeted industry sector.

In today's digital world, people often share sensitive information over the internet without worrying about the risks involved. This happens despite the rules and policies of the companies and organizations they work for that specifically prohibits sharing sensitive information through unprotected channels such as email or chat platforms. A recent survey conducted by

 ISSN: 2582-6433

Symantec, an online security company, has revealed that 68% of the interviewed employees admitted to sharing sensitive information with coworkers who were not supposed to have access.[4]

The dangerous consequences of this behavior have yet to be fully realized. It is clear that companies and organizations still need to combat threats from the people they already trust. When sensitive information is shared, the fallout can be worse than internal breaches. There are financial penalties, and sensitive breaches within the organization can result in reputational damage. Unauthorized disclosure of customer information or proprietary data can lead to legal liabilities, regulatory penalties, and consumer trust erosion. On top of all of this, security lapses are used by malicious actors to take advantage of data breaches in cyber-attacks to make the risks associated with these infidelities worse.

Prioritizing security awareness training and implementing strong data protection measures are crucial for mitigating the risks that come with sharing sensitive information. This comprises encrypting data at rest and during transmission, setting up various access controls and authentication mechanisms, and fostering a culture of accountability and adherence to rules among workers. By taking care of both technological and human factors, organizations can strengthen their defenses against insider threats, keeping sensitive information safe from unauthorized access and leaks.[5]

To effectively reduce cybersecurity risks, it is crucial to comprehend the cognition and behavior of users. Because of the cognitive bias and the social engineering method, human behavior in most situations is the element with the largest risk factor in the safety system. [6]By understanding and taking advantage of these cognitive biases and designing a system that is easy for users to use, we can drive users to adhere to the safest practices. Furthermore, when users are taught about societal manipulation ideas and how to combat them, they are more able to drive them away. To keep updated on proper training methods, negative feedback is put in.

This keeps updates and is an easy way to go through routine maintenance of security

[4] https://www.researchgate.net/publication/379430784_THE_HUMAN_FACTOR_IN_CYBER_SECURITY
[5] https://blog.checkpoint.com/security/the-human-factor-of-cyber-security/
[6] https://securityscorecard.com/blog/the-human-factor-in-cybersecurity/#:~:text=Humans%20are%20susceptible%20to%20cognitive,to%20mitigate%20human%20error%20effectively

 ISSN: 2582-6433

techniques. Finally, by integrating human understanding of danger into business models, the value of safety will and will always be present with work and assets.

Training and Awareness Programs

In the current era of digital technology, with significant dangers from cyber threats and widespread, skilled attacks—especially in developed countries—the necessity of training and awareness for users can barely be overstated. Training and awareness programs can play a significant role in forming a culture that values safety for users of electronic technology within organizations, and can also provide the necessary reinforcement for individuals to recognize, assess, and control risks effectively.

A variety of instructional programs can be used for security awareness training. However, the ultimate objective of these programs is to provide employees with the knowledge and abilities required to safeguard sensitive data and their organizations against hacking, phishing, and other security breaches; doing so will safeguard the IT infrastructure of the business. Also, because social engineering and human mistake can lead to a great deal of cybersecurity breaches, businesses must make sure that their employees are aware of their vulnerability to attacks and breaches and are equipped to mitigate these risks to the greatest extent feasible.

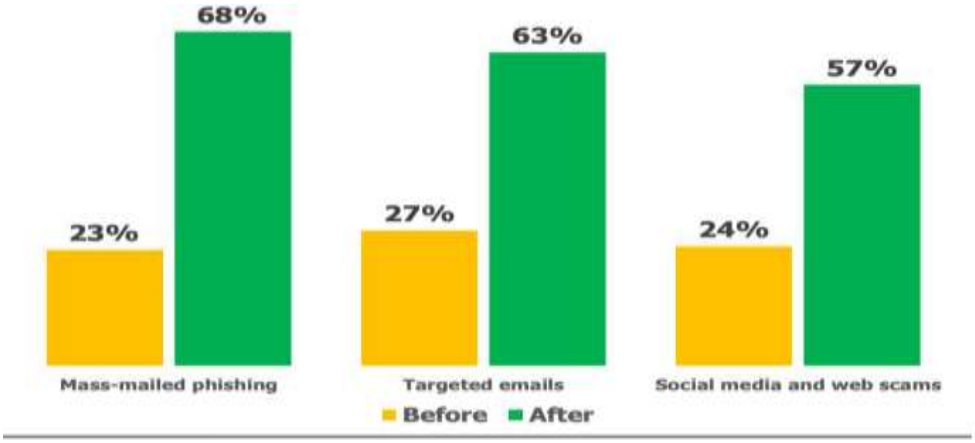
Employee security awareness training is essential because of this. Efficient cyber awareness training informs staff members about potential risks to the organization, equips them with knowledge about cybersecurity threats, and teaches them how to spot warning signs, prevent breaches and attacks, and handle incorrect or unclear decisions. Many businesses will also need to put cybersecurity training into place to make sure it complies with legal requirements.[7]

To establish and maintain a proactive cybersecurity stance among users, it is critical that organizations provide thorough training programs. These programs are not only vital for imparting the knowledge, skills, and awareness necessary to navigate the treacherous cyberspace with confidence, but, essential in instilling the proper habits, caution, or reflexive reactions against potential threat scenarios.[8] Without such preparation, employees might accidentally and unknowingly expose their organization to risks—such as engaging with phishing emails, divulging sensitive information, or inviting compromise due to other patterns

[7] https://blog.checkpoint.com/security/the-human-factor-of-cyber-security/
[8] https://www.kaspersky.com/blog/human-factor-360-report-2023/

 ISSN: 2582-6433

of insecure conduct.



Designing Resilient Software Systems

Cybersecurity is dynamic. This nature of cybersecurity has made it essential to design software systems that are able to resist and withstand all form of challenges caused by human errors and manipulations. While it is necessary to have a thorough understanding of security awareness, it is just as crucial to implement the right strategies to mitigate human errors and manipulations. To achieve this, it is imperative for organizations to incorporate solid security principle by design software systems that are user centric. This will strengthen organizations' security systems making it difficult for cyberattacks to breach the added level of security system. Organizations have a lot of options and strategies for designing resilient software systems against cyberattacks.

The following are some recommended strategies:

Principle of Least Privilege (PoLP)

By integrating measures like least privilege access, organizations can effectively reduce the likelihood of human error and manipulation and thereby minimize potential risks. Least privilege is the idea and practice of limiting user, account, and computer process access privileges to only those resources that are absolutely necessary to carry out lawful tasks. The term "privilege" inherently describes the right to get beyond some security measures. This means that users who have least privilege access are only given access for the tasks they need to do.[9]

[9] https://telefonicatech.com/en/blog/human-factors-in-cybersecurity

 ISSN: 2582-6433

One essential best practice to lower security risk and minimize business disruption from mistakes or malicious intent is to enforce least privilege access.

Multi-Factor Authentication (MFA)

MFA is a tiered method of data and application security in which a system asks a user to provide a combination of two or more credentials in order to authenticate them and confirm their identity before allowing them to log in. MFA prevents unauthorized access to users' application and data by providing an extra level of authentication that goes beyond passwords, thereby increasing the difficulty for hackers to infiltrate user accounts (Microsoft, 2021). According the US Cyber Security & Infrastructure Security Agency, the use of MFA on accounts makes it 90% less likely to be hacked (CISA, n.d.). [10]Because unauthorized individuals won't be able to fulfill the second authentication criterion and get access to the targeted physical location, computer equipment, network, or database, multi-factor authentication (MFA) enhances security even in the event that one credential is compromised.

Virtual Private Networks (VPNs)

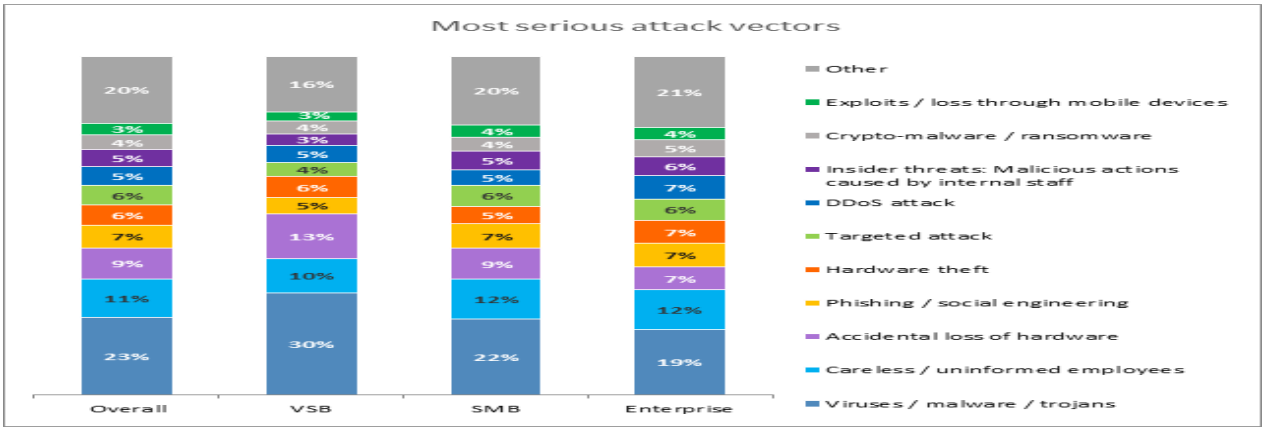
The use of Virtual Private Networks (VPNs) is an essential component in building a strong resilient software against cyberattacks. Utilizing VPNs by users can considerably augment data privacy and security. VPNs entail the encryption of Internet traffic, thereby constructing secure channels between end-user devices and VPN servers, effects. mitigating risks of information cloning and unauthorized data access. This encryption guarantees confidentiality of information exchange, even when it involves insecure networks or public Wi- Fi spots. VPNs are also about anonymity for users who do not want nosy marketers, intrusive ISPs, or repressive governments to spy on what they do online. Additionally, VPNs are important for ensuring secure remote access, especially in the context of the current trend towards working from home and the decentralization of corporate networks. They allow users to securely connect to corporate networks and resources from anywhere in the world, ensuring data integrity and confidentiality. Organizations emphasize user privacy and build customer trust with their customer base by incorporating VPN capabilities into software systems.[11]

It is however imperative that the use of VPNs is in conjunction with other cybersecurity

[10] https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf
[11] https://securityscorecard.com/blog/the-human-factor-in-cybersecurity/

 ISSN: 2582-6433

strategies for effective results.



Intuitive Authentication

A crucial milestone in securing cyberspace today is the rise of intuitive authentication. Recognizing security discretion from user convenience, intuitive authentication capitalizes on experienced and friendly user interfaces to lighten the burden on the user and drive a wide range of accessibility while maintaining a reasonable level of security. Among these systems, biometric measures and one-click authentication are the most common, each with its exclusive compromises in that they tend to escape cyber threats.[12]

Biometric authentication is leading the way through using one's exclusive biological traits, just like a person's fingerprints, face, or eye patterns, to verify their unique individuality. They help in getting rid of the use of passwords or a PIN once and for all and authenticate more correctly and more effectively to the extent never seen before. In the same way, a streamlined and simple approach to user authentication is the one-click authentication, allowing users to access protected resources with a single touch or click. This method is used especially in the environment of the single- sign-on (SSO) where the user can verify himself by using a connecting set of credentials in multi-application or platform.

The International Journal of Advanced Computer Science and Applications' research indicates biometric authentication as an effective tool in reducing authentication-related errors and enhancing user satisfaction. Moreover, biometric authentication enhances security by minimizing the possibility of credential theft or unauthorized access, as biometric traits are peculiarly elemental for every individual. Also, as outlined in an article from the Journal of

[12] https://www.upguard.com/blog/human-factors-in-cybersecurity

 ISSN: 2582-6433

Global Research in Computer Science,[13] the acceptance of one-click authentication has proven to drastically decline authentication exhaustion while simultaneously enhancing the output of users (Kumar, 2020). Simplifying the steps it takes for an individual to be authenticated, one-click authentication does not only enhance convenience for the user, but it helps to reduce the risk of authentication errors and security breaches. Integrating intuitive authentication methods into software systems is a crucial step in improving cybersecurity resilience and providing a smooth user experience.

Human Factors in Cybersecurity

Human factors in cybersecurity encompass the ways in which human behavior, psychology, and social interactions influence the security of information systems. While technical defenses are crucial, the human element is often considered the weakest link in cybersecurity. Here's an elaborate exploration of human factors in cybersecurity:[14]

Social Engineering

Social engineering is the manipulation of individuals to divulge confidential information. Attackers exploit human psychology to bypass technical security measures. Common techniques include:

- **Phishing**: Fraudulent emails or messages that appear legitimate, designed to trick users into revealing sensitive information.
- **Spear Phishing**: Targeted phishing attacks on specific individuals, often using personal information to appear more credible.
- **Pretexting**: Creating a fabricated scenario to obtain information or access.
- **Baiting**: Offering something enticing to lure victims into a trap, like malware-infected USB drives.
- **Tailgating**: Gaining physical access to a restricted area by following an authorized person.

User Awareness and Training

Employees' lack of cybersecurity awareness can lead to unintentional security breaches. Training programs aim to:

- **Educate**: Inform employees about potential threats and safe practices.

[13] https://telefonicatech.com/en/blog/human-factors-in-cybersecurity
[14] https://www.mdpi.com/2624-800X/2/3/29

 ISSN: 2582-6433

- **Simulate**: Conduct mock phishing attacks to assess and improve user responses.
- **Update**: Keep training current with evolving threats and new technologies.

Password Practices

Weak or reused passwords are a significant vulnerability. Effective password practices include:

- **Complexity**: Using strong, unique passwords that combine letters, numbers, and special characters.
- **Management**: Employing password managers to handle and generate secure passwords.
- **Multi-Factor Authentication (MFA):** Adding an extra layer of security beyond just passwords, such as a biometric or a one-time code.

Insider Threats

Insiders, whether malicious or negligent, pose a serious risk:

- **Malicious Insiders**: Employees or contractors who intentionally harm the organization.
- **Negligent Insiders**: Well-meaning employees who make mistakes, such as falling for phishing scams or mishandling sensitive data.

Human Error

Simple mistakes can lead to significant breaches:

- **Misconfigurations**: Incorrectly set up systems can leave vulnerabilities.
- **Data Mishandling**: Accidentally sending sensitive information to the wrong person or leaving data exposed.
- **Improper Disposal**: Not securely deleting or destroying data when it's no longer needed.

Behavioral Economics

Understanding how people make decisions can improve security policies:

- **Nudging**: Designing systems and processes that encourage secure behavior by default.
- **Cognitive Biases**: Addressing biases like overconfidence, where employees might underestimate their risk, or the diffusion of responsibility, where security is assumed to be someone else's job.

 ISSN: 2582-6433

Organizational Culture

The overall culture of an organization influences security practices:

- **Tone from the Top**: Leadership commitment to cybersecurity can foster a security-conscious culture.
- **Policies and Procedures**: Clear, enforced policies and procedures guide behavior.
- **Open Communication**: Encouraging reporting of potential threats without fear of punishment.

User Interface Design

Poorly designed interfaces can lead to mistakes:

- **Clarity:** Clear prompts and error messages help users make informed decisions.
- **Consistency**: Familiar patterns and predictable interactions reduce errors.
- **Error Prevention and Recovery**: Designing systems that prevent errors and offer easy recovery options when mistakes occur.

Stress and Fatigue

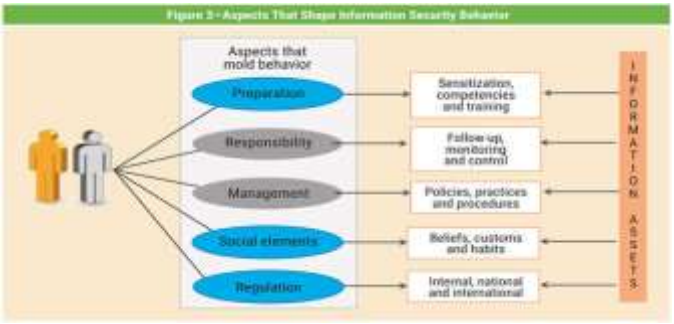
Employees under stress or fatigue are more likely to make errors:

- **Workload Management**: Balancing workloads to prevent burnout.
- **Mental Health Support**: Providing resources to support employees' well-being.

Trust and Verification

Balancing trust with verification is crucial:

- **Zero Trust Models**: Verifying all requests, regardless of their origin, reduces reliance on assumed trust.
- **Least Privilege Principle**: Granting only necessary access rights to minimize potential damage.



 ISSN: 2582-6433

Conclusion

In conclusion, this essay has been able to demonstrate the close relationship between cybersecurity and human factors and the necessity of adopting a broad approach in order to successfully lower cyberattacks. By concentrating on user behavior, training, awareness campaigns, and software design resilience, organizations may create robust and long-lasting defenses that can withstand the challenges posed by cyber threats. Additionally, this article has demonstrated the pervasive risks associated with regular human behavior, such as the misuse of passwords and vulnerability to phishing, and has emphasized the need of comprehending human psychology in order to defend against cybersecurity breaches. Focusing on the ever-changing and developing nature of technology, it is absolutely critical for businesses to put an emphasis on human-oriented cybersecurity strategies to be able withstand the kind of cyber threats and attacks that could come with the advancement of technology.

To maintain a secure operating environment, organizations must merge training programs, user behaviors, resilient software design, and security awareness initiatives into their cybersecurity frameworks. With this comprehensive approach, a culture of security awareness and resilience is created, empowering organizations and individuals to navigate the constantly evolving threat landscape with confidence and effectiveness. With cyber threats developing into more advanced forms and becoming increasingly widespread in their reach, organizations must take immediate action and start putting people at the center of all cybersecurity efforts if they want to safeguard the security of their most important assets and data.

In addition, the growing popularity of remote work alongside the pervasive influence of digital platforms underscores the increasing importance of cybersecurity awareness. It is especially crucial for remote workers, who often face distinctive hazards and weaknesses, to receive

 ISSN: 2582-6433

specialized training in order to ensure the security of a company's resources.

BIBLOGRAPHY

1. https://blog.checkpoint.com/security/the-human-factor-of-cyber-security/
2. https://securityscorecard.com/blog/the-human-factor-in-cybersecurity/#:~:text=Humans%20are%20susceptible%20to%20cognitive,to%20mitigate%20human%20error%20effectively
3. https://telefonicatech.com/en/blog/human-factors-in-cybersecurity
4. https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf
5. https://www.kaspersky.com/blog/the-human-factor-in-it-security/
6. https://www.livingsecurity.com/blog/how-to-measure-the-human-factor-in-cybersecurity