International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

The Human Factor: Revolutionizing Cyber Security with Intelligent Hygiene

Vishal Vikram Singh[1], Bineet Kumar Gupta[2], Veena Singh[3], Megha Aggarwal[4]
[1,2,3,4]Shri Ramswaroop Memorial University, Barabanki, India 225003
vishal29.singh@gmail.com, bkguptacs@gmail.com, drveenasingh27@gmail.com, meghaaggarwal.csis@srmu.ac.in

Abstract—In an era where the digital threats evolve at an unprecedented pace, cyber hygiene is proving pivotal and fundamental to organizational and personal data security. This paper presents a comprehensive review of modern practices in cyber hygiene, introducing innovative frameworks and analyzing real- world case studies. We explore the integration of artificial intelligence, blockchain technology, and behavioral biometrics in creating a robust cyber hygiene framework while examining their practical implementations through various case studies. The research culminates in proposing the novel 5P Model for cyber hygiene management, offering a structured approach to digital security in the contemporary threat landscape.
Keywords—Cyber Hygiene, NIST Framework, Colonial Pipeline Ransomware Attack

1. Introduction

The human element within the realm of information security is becoming an attractive target for cyber villains. Significant efforts are underway to enhance "cyber hygiene"—a concept that can be widely interpreted as the establishment and upkeep of online safety protocols. Regrettably, the interpretation of "cyber hygiene" and its associated practices often differ greatly and can even conflict, thus impeding the mission to safeguard vital information assets. Take, for instance, the careless application of the term which can create scenarios where initiatives aimed at bolstering cyber hygiene overlook the specific context, resulting in either overly lenient or excessively stringent outcomes—some organizations may mistakenly believe that simply documenting security-related policies suffices (without any supplementary security training) while in other cases, employees may exercise such extreme caution that they refrain from opening any email attachments at all, even those that are legitimate.

A. Defining Cyber Hygiene

Cyber hygiene embodies a thorough approach to ensuring digital safety and well-being, akin to our understanding of personal hygiene in everyday life. In essence, cyber hygiene entails a methodical process for safeguarding both individual and organizational digital assets through proactive initiatives, well-informed tactics, and flexible security measures. It represents a comprehensive strategy that transcends conventional security protocols, merging human behavior, technological progress, and strategic foresight to establish a strong defense against the ever-changing threats in the digital landscape. surveillance of technological resources, which includes the timely updating of antivirus software.

B. The Growing Cyber Threat Landscape

The Ponemon Institute's Second Annual Cost of Cyber Crime Study has determined that the average financial consequences of cybercrime for organizations in the United States is approximately
$17.36 million. This amount exceeds the figures in Japan ($8.39 million), Germany ($7.84 million), the United Kingdom ($7.21 million), Brazil ($5.27 million) and Australia ($4.3 million). Significantly, these means have demonstrated a consistent rise starting from 2014. The report shows that nearly all organizations have faced malware attacks, with 70% also experiencing phishing and social engineering threats, and 63% encountering web- based attacks. Additionally, 61% were threatened by malicious code, 55% encountered botnet attacks, and 50% documented incidents related to stolen devices. Furthermore, denial of service attacks impacted 49% of the respondents, while 41% faced threats from malicious insiders. Significantly, there was an 8% increase in the number of organizations experiencing phishing and social engineering attacks from 2015 to 2016. This trend underscores the increasing need for enhanced cybersecurity measures, as the threat environment continues to change. Statistics and trends indicate that cyberattacks rank among the most expensive dangers for businesses; however, globally, cybercrime is projected to have cost companies around $8 trillion in 2023 (a shocking figure). This amount is anticipated to soar to almost $24 trillion by 2027, although many organizations struggle to allocate sufficient resources to combat these threats.

2. THEORETICAL FRAMEWORK

This Section shall be discussing with the core components of cyber hygiene and the NIST Cybersecurity Framework Integration.

i. Core Components of Cyber Hygiene

The foundation of effective and robust cyber hygiene can be formalized into four pillars abbreviated as DISP.

a) Digital Asset Management: Semantic inventory and protection of digital resources.
b) Incident Response Readiness: Preparation for and management of security incidents.
c) Security Consciousness: Cultivating awareness and proactive security behavior.
d) Preventive Practices: Implementation of pre- emtive security measures.

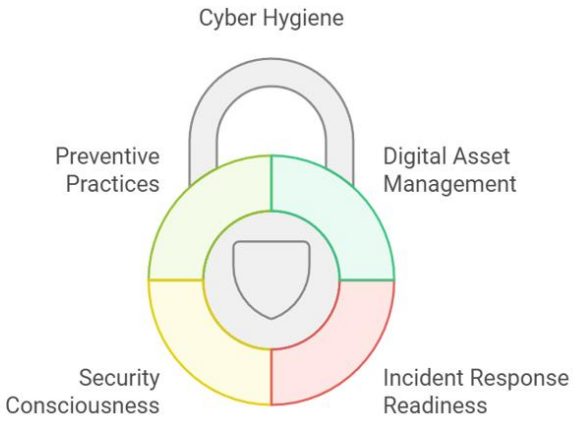

Fig. 1. Core Components of Cyber Hygiene

ii. NIST Cybersecurity Framework Integration

The NIST Cybersecurity Framework (CSF) is a complete guide designed to help organizations manage and mitigate cyber threats. Legitimately, an adaptable exchange formed around the National Institute of Standards and Technology (NIST), this structure was intended to be adaptable for usefulness, thus conceivable that it can serve as best practice for individuals across a wide range of sizes and even types of organizations: governmental organizations, businesses, or instructive organizations. At its heart, the CSF highlights a risk management approach that embeds cybersecurity at the enterprise level into a broader risk management process.

The NIST Cybersecurity Framework is closely aligned with cyber hygiene practices by focusing on continuous risk management and proactive security activities.

The key alignments are as follows: -

a) Risk Assessment: Regular assessments of risks to ensure an organisation identifies its vulnerabilities and focuses efforts in the areas that matter to it most, as both the CSF and cyber hygiene recommend.

b) Preventive Measures: The Protect Function of the CSF emphasises on preventative measures reminiscent to best cyber hygiene practices including strong passwords, software updates and employee security awareness training.

c) Incident Response Planning: This Respond function from the CSF drives organizations to create incident response plans, which is a key cyber hygiene practice—preparing for breaches in advance of when they might occur

d) Continuous Improvement: The CSF encourages organizations to systematically evaluate and adapt their cyber hygiene over time, as threats change.

e) Integration with Holistic Risk Management: The framework promotes integration of cyber hygiene with other areas of risk management, stressing that cyber hygiene is not only a matter of technology but also a people and processes issue.

Therefore, the above mentioned NIST key allignments lay the necessatiy for the folllwing CSF Functions as summerised in the Fig 2.

Fig. 2.CSF Function

iii. Modern Cyber Hygiene Framework

The 5P Model for Cybersecurity represents an innovative approach to cyber hygiene, focusing on proactive and adaptive strategies to enhance cybersecurity practices.

The following are the 5P Model breakdown are as follows-

i. Predict:-This facet entails harnessing artificial intelligence to project potential cyber threats prior to their emergence. Through the analysis of patterns and historical datasets, organizations can delineate vulnerabilities and nascent threats, thereby facilitating proactive preparedness and response.

ii. Prevent:- Automated security controls are pivotal for mitigating human error and ensuring the uniform enforcement of security protocols. This encompasses the implementation of firewalls, intrusion detection systems, and automated patch management solutions that function autonomously, thus diminishing the likelihood of security breaches.

iii. Protect:- Automated security controls are pivotal for mitigating human error and ensuring the uniform enforcement of security protocols. This encompasses the implementation of firewalls, intrusion detection systems, and automated patch management solutions that function autonomously, thus diminishing the likelihood of security breaches.

iv. Persist:- Continuous monitoring is paramount for the identification and mitigation of threats in real-time. By employing tools that facilitate persistent oversight of network activity and system integrity, organizations are positioned to detect anomalies and potential breaches as they transpire, enabling immediate remedial actions.

v. Progress:- The adaptive improvement cycle underscores the imperative for organizations to routinely evaluate and refine their cybersecurity practices. This process entails scrutinizing incident responses, revising security protocols in light of emerging threats, and assimilating insights gained into forthcoming strategies to ensure robust resilience against dynamic cyber risks.

This concludes the theoretical framework and the core understanding required to to addressed one of the most recent cyber security breaches occurred in the year 2021. The next section deals in depth with the same.

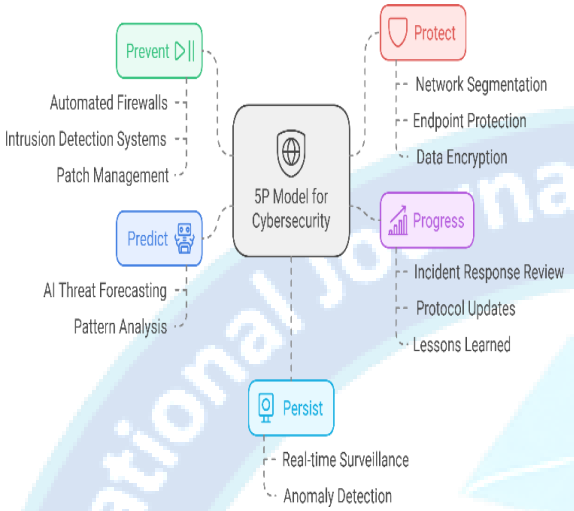

Fig: 3. 5P Model for Cyber Security

3. CASE STUDY- THE COLONIAL PIPELINE RANSOMWARE ATTACK (2021)

1. Incident Background

One significant example in allowing us to understand the cybersecurity risks relating to essential infrastructure is the ransomware attack on the colonial pipeline on 7th May, 2021. The attack was instigated by an illegal use of VPN credentials which facilitated entry into the systems of the company. It is mentioned how the compromised credential's password was already released on the dark web which points at the absence of multi- factor authentication (MFA) being the factor contributing to this breach. The event resulted in a six-day operational stand still, a 45% interruption in fuel supply to the Eastern seaboard and substantial ransom losses of approximately $4.4 million dollars. The consultants attributed inadequate monitoring processes and lack of strong authentication mechanisms as the most probable causes of the event.

2. Attack Timeline Analysis

According to the steps that follow, the timeline concerning the assault can be divided into three phases. First, the attackers used the stolen VPN credentials of users to gain access to the systems. T The weakness of the MFA associated with it became a critical enabler for their penetration. Secondly, the attackers moved around the IT networks and managed to breach the billing and business systems while encrypting some of the core operation data. This lateral movement emphasizes the need for more robust physical access controls and separation of IT and OT networks to mitigate the risks involved. Thirdly, the breach of the billing system led to the complete blockage of the Pipeline system as a result of isolation of operational technology systems so that no further damage would occur. This led to the suspension of almost 5,500 miles of pipeline and related operations which clearly show the devastating impact of cyber-attacks on a nation's critical infrastructure. To prevent something similar to what happened with the Colonial Pipeline attack again, businesses have no choice but to adopt a new health cyber defense approach that focuses on many aspects. These include the deployment of AI solutions.

4. PROPOSED INNOVATIVE SOLUTION

1. AI Powered Personal Security Assistant (PSA)

The adoption of an AI-Powered Personal Security Assistant (PSA) can significantly improve cybersecurity measures. The PSA focuses on two key areas: continuous authentication monitoring and decentralized identity verification.

Continuous Authentication Monitoring includes several key techniques, including real-time credential use analysis, which examines how credentials are used during access; behavioral pattern matching, which identifies deviations from established user behavior; geographic access point verification to ensure that access attempts originate from expected locations; and time-based access anomaly detection to flag unusual access attempts outside of typical operating hours.

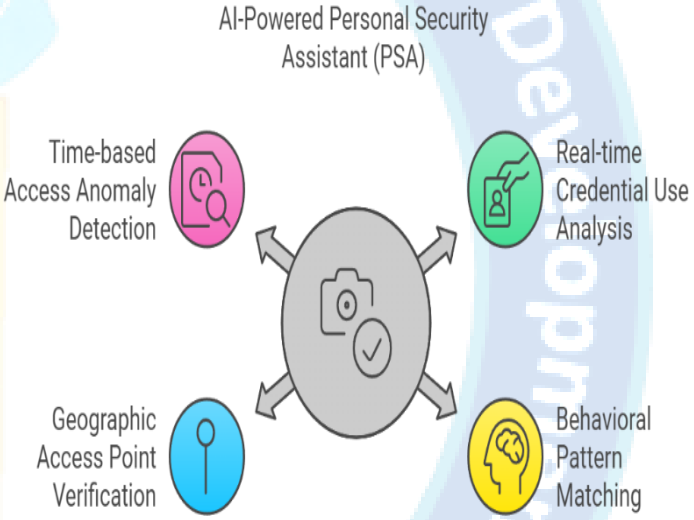

Fig: 4. AI-Powered PSA Implementation

2. Decentralized Identity Management with Blockchain

Decentralized Identity Verification reiterates the need for self-sovereign identity for each employee so that people have control over their own identity data. This approach also concerns the provision of access logs that do not change, so accountability can be achieved, use of multi-factor verification to increase security levels, and implementation of zero- knowledge proofs to verify identity in a non- obtrusive fashion.

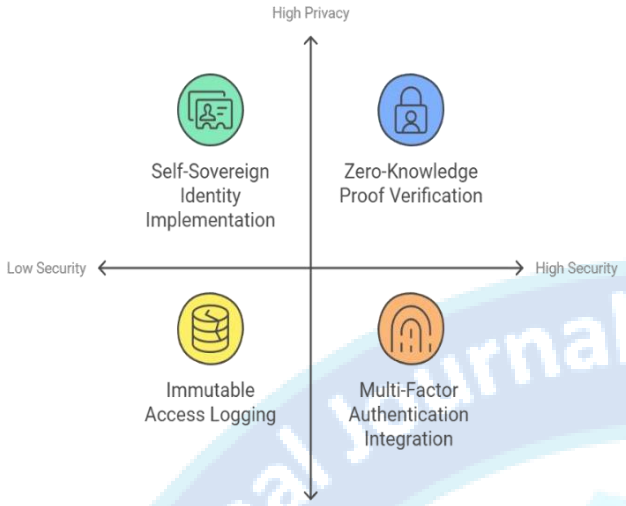

Fig: 5. Decentralized Identity Management Strategies

5. CONCLUSION:

Given the ever-changing cyber threat landscape, an evolving approach to cyber hygiene is warranted. The proposed 5P Model coupled with AI, people and behavior in this domain on Dell Technologies stage the same theme: it offers a complete look at modern digital security practices. Case studies underscore the vital importance of good cybersecurity hygiene, while what lies ahead suggests that there is more to come in this new discipline. The colonial pipeline attack would also have been effectively mitigated if these imaginative approaches had implemented.

For instance, improper use and other security issues arise from the fact that By combining PSA driven by AI, blockchain- based identification certification and behaviorist biometrics, we have created a robust framework for security that will fill in the loopholes exploited in the Colonial Pipeline attack.

People do not recognize secure servers or channels as opposed to those that may happens to not the safest of all the case.

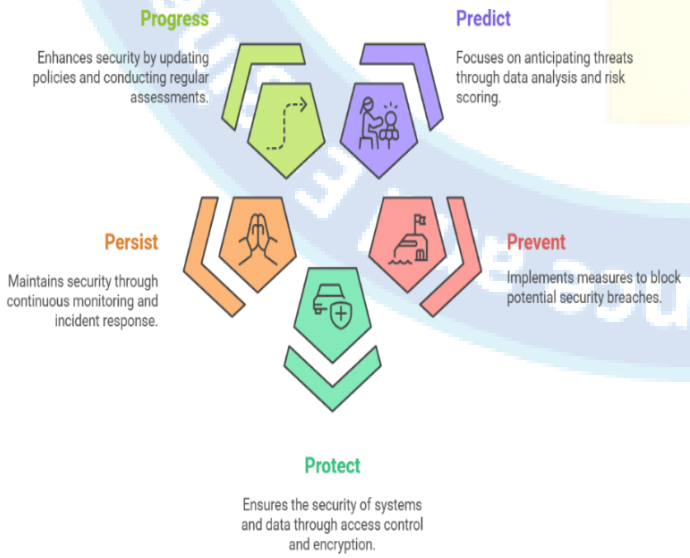

Fig 6. The 5p Model for Cyber Hygiene

REFERENCES:

1. NIST Special Publication 800-53(2023)
2. R. Chivukula, T. Jaya Lakshmi, L. Ranganadha Reddy Kandula and K. Alla, "A Study of Cyber Security Issues and Challenges," 2021 IEEE Bombay Section Signature Conference (IBSSC), Gwalior, India, 2021, pp. 1-5, doi: 10.1109/IBSSC53889.2021.9673270.
3. "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years", Cyber Security & Infrastructure Security Agency.
4. Ncubukezi, Tabisa & Mwansa, Laban & Rocaries, François. (2020). A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses. 1-6. 10.23919/ICITST51030.2020.9351339.
5. Ncubukezi, Tabisa & Mwansa, Laban. (2021). Best Practices Used by Businesses to Maintain Good Cyber Hygiene During Covid19 Pandemic. Journal of Internet Technology and Secured Transaction. 9. 714-721. s10.20533/jitst.2046.3723.2021.0086.