Towards Human-Centric Framework to promote Cybersecurity-Hygiene for the Future of the Healthcare

Abstract: In healthcare, the lack of protection for important systems has led to a growing problem of cybersecurity threats. It is crucial for individuals to prioritize actions like regularly updating software and using strong passwords to strengthen their online security. However, many users lack knowledge about effective cybersecurity practices. This paper emphasizes the importance of educating people about cybersecurity, with a focus on human behavior. It provides valuable insights into user habits and offers appropriate cybersecurity protocols for healthcare organizations, highlighting the important role humans play in finding solutions.

1. Introduction

Our world's vital infrastructure elements, hugely significant in our everyday life, have increasingly become susceptible to digital dangers. This has emerged as a high priority international worry especially for defense departments everywhere. Web centered crimes and intrusive online spying are specific issues disrupting the financial sector causing substantial destruction. Such developments leave organizations perpetually uneasy about future security infringements.

Over recent decades, ground breaking strides within digital innovation have significantly reshaped how we interact with one another from far distances; operational systems of administrations, businesses alongside societies at large haven't been spared this transformation either. But just like any silver lining comes saddled with dark clouds, the uplifting perks that accompany internet accessibility come hand-in-hand with notable security predicaments too. The discomforting frequency increase of irritating spam messages together with complex Distributed Denial-of-Service (DDoS) hostilities underlines these cyber problems further amplifying their destructive potential even more alarmingly now than before.

In light of such escalations on an international level regarding safety breaches occurring digitally over time nations globally recognize there remains little room left anymore barring cyberspace integration into strategic planning overall. This calls thusly for formulating designated national safeguards along restructuring military tactics specifically addressing said susceptibilities head-on theological distinctions between standard versus combat readiness becoming vaguer each day henceforth due to it all inevitably.

In essence then arises two pressing realities urgently call upon additional securing measures. The advent wherein previously developed technologies spawn present-day areas requiring immediate protection. Where traditional methodologies must ultimately integrate themselves seamlessly amidst updated digitized trajectories unfolding currently kindles deep assertion across western civilization coupled broader global counterparts towards acknowledging inherent risks looming ominously right around once' predictable corners. These emerging scenarios unfalteringly insist urgent legislation construction accompanied proper policy development align coherently blending diverse factors enveloped inside cybersecurity modulation intricacies steadfastly moving forward nevertheless. Societies including economic structures can only adapt reasonably survivable navigating hazardous disturbances wrought cyber disorders maintaining vigilance enhance greater agility shielding against potential dire implications effectively. A present reality

increasingly more so than ever before, no prediction anymore, Assuaging securitizing measures upheld synonymous wanting to fight off threatening digital problems are seen less luxury items saved only for financially abundant nations but rather acquire necessity status intended securing nation-states' respective survival thus prosperity regardless.

Cybersecurity now marks an indisputably pivotal element constituting secured statehood in addition strives retaining competitive global standing advantageously. With technology persistently innovating onwards inexhaustibly remains of striking importance emphasis on detective abilities combined equally well assertive active precautionary strategies keeping step successively susceptible expanding vulnerability landscapes proactively too. Wrapping up, we just can't ignore how deeply digital evolution has sculpted our lives. Communication and day-to-day processes have taken a profound spin due to the presence of internet it's like living in an entirely fresh world. But every rose comes with its thorns; this case being considerable security hurdles brought forth by cyberspace advent. The need for countries to ramp-up their cybersecurity game is apparent now more than ever, securing crucial cyber defensive strategies must be marked urgent on national agendas as well as pouring investments into safety precautions that guarantee both societal and economic victories.

2. Literature Review

In the perspectives of entities such as NATO and EU, cybersecurity is a critical element affecting member nations' defense and safety measures. These organizations prioritize cyber preparedness, safeguarding not only their own systems but also those linked to their membership group [1]. The medical field is filled with new terminologies like healthcare 4.0, Health 4.0, Medical Industry 4.0 and Healthcare Industry 4.0 that distinctly refer to the transforming effect of the Fourth Industrial Revolution on health-related services and procedures [2]. 4IR technologies encompass manufacturing processes, cloud-based creation tools and the Industrial Internet of Things. A prevalent concern with these digital advancements is ensuring cyber security measures and data privacy provisions are practical and effective [3].

It's crucial for individuals to adopt commendable cyber hygiene practices, such as frequent software refreshing and designing distinctive passwords. This approach serves as a strong shield against web-based attacks. Cyber cleanliness involves adhering strictly to appropriate procedures and standards - nurturing beneficial habits in the digital realm protects precious data from unwanted infiltration by online pirates [4]. Despite the myriad of online attacks, it's clear that several digital citizens still show careless web rituals. We can see this in situations where individuals scatter their private data across virtual community spaces or casually swap passcodes [5]. Cyber rogues, in their resourceful knowledge, realize the simplest gateway into a system through spotting technical flaws or pilfering personal data. It is an immediate call to action for enhancing people's behavioral adjustments and elevating digital cleanliness. Society pays dearly as slack cybersecurity exacts heavy economic bills. To be precise, analysis by the Ponemon Institute [6] the Second Annual Cost of Cyber Crime Study revealed that cyberattacks incur an average expense of $17.36 million for US organizations, contrasted by Japan's estimated cost at approximately half the amount - 8.39 million dollars to be precise. Strikingly, two apparent culprits behind this pricey dilemma are malware (affecting a staggering majority: 98%) and social engineering or phishing schemes accounting together for seventy out so every hundred instances. Moreover web-based strikes have proven quite dominant too with claiming responsibility in around sixty-three percent cases studied under analyses. Noteworthy is also dynamics which indicated escalation observed among incidents comprehended via socio-technic manipulations

reflected as 'engineering' combined with digital traps popularly known as "phishing" showing eight percent up tick from year2015 onwards next cycle; tending indicatively towards a future where they could become increasingly prevalent actors within such cybersecurity breach occurrences.

Around the globe, not only are institutions grappling with cyber invasions but individuals also end up bearing the brunt of these security infringements. Mounting casualties stemming from digital cracks in our defenses have been documented by sources like the FBI's Internet Crime Complaints Center (IC3) [7] in an unsettling revelation, American citizens reported 288,012 cybercrime incidents to the FBI in 2015. The financial damages wrought by these offenses were staggering —amounting approximately $1 billion with individual victims suffering average losses of about $8,421 per event. Curiously enough age and gender did not significantly affect victimization rates; both men (aged between 50-59 years representing as many as 31,473 victims) and women aged from 40-to-49 years (29,559 victims), fell prey to cybercrimes. The shocking part is monetary damage inflicted impacted individuals across all demographics harshly—even crossing over a daunting million-dollar threshold for some. This metric provides compelling insight into the susceptibility of humans towards cybersecurity hazards regardless one's station within society or personal details [8,9]. Stirring the pot of personal computing environments, where a staggering 95% of malicious cyber onslaughts find their mark - an alarming testament to our interconnected digital world [10]. The absence of on-site security personnel responsible for updating software and hardware could account for the vulnerability of personal and home computing equipment [11]. With the escalating trend of cyber threats and attacks, it has become fundamentally necessary for users to impose defensive safeguards. This is due to the fact that despite a system appearing impenetrable on its surface, often times unsuspecting users unknowingly represent vital gateways through which access can be gained into protected data systems and extensive networks [12]. Digital infiltrators tirelessly seek out weak spots to manipulate. Often, these vulnerabilities emerge from online users who skimp on robust cyber upkeep - making their virtual homesteads prone to attack by casually unveiling private details or allowing known security practices fall by the wayside [5]. In our hyper-connected age, ensuring digital safety is paramount. Yet strikingly, while most netizens are cognizant of the fact that their actions can leave them vulnerable to cyber-attacks; sadly, not all have been schooled in smart online etiquette like preserving password privacy. Amidst a plenitude of protective measures on offer for users they often find themselves at sea - clueless about how or where these security shields even exist let alone making sense and taking advantage of such provisions provided by the waves within this overwhelming ocean called cybersecurity landscape [13]. Moreover, there's an alarming gap in understanding for end users when it comes to the crucial steps they can take towards cyber security. This inadequate knowledge often leads them down a perilous path of ill-advised actions and attitudes [14]. In spite of everything, maintaining high-level cyber cleanliness boosts secure practices and fortifies our defenses against the looming perilous assaults [15].

References

1. Liaropoulos, A. A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia. *J. Inf. Warf.* **2015**, *14*, 15–24.

2. Javid, T.; Faris, M.; Beenish, H.; Fahad, M. Cybersecurity and data privacy in the cloudlet for preliminary healthcare big data analytics. In Proceedings of the 2020 International Conference on Computing and Information Technology, Tabuk, Saudi Arabia, 9–10 September **2020**; pp. 1–4. [CrossRef]
3. Thuemmler, C.; Bai, C. Health 4.0: Application of industry 4.0 design principles in future asthma management. In *Health 4.0: How Virtualization and Big Data Are Revolutionizing Healthcare*; Springer: Berlin/Heidelberg, Germany, **2017**; pp. 23–37.
4. Singh, D.; Mohanty, N.; Swagatika, S.; Kumar, S. Cyber-hygiene: The key Concept for Cyber Security in Cyberspace. *Test Eng. Manag.* **2020**, *83*, 8145–8152.
5. Cain, A.; Edwards, M.; Still, J. An exploratory study of cyber hygiene behaviors and knowledge. *J. Inf. Secur. Appl.* **2018**, *42*, 36–45. [CrossRef]
6. Ponemon Institute. 2016. Available online: http://www.ponemon.org/li-brary/2016-cost-of-cyber-crime-study-the-risk-of- business-innovation (accessed on 1 January 2023).
7. FBI. 2015. Available online: https://www.ic3.gov/media/annualreports.aspx (accessed on 15 December 2022).
8. Long, R. Using Phishing to Test Social Engineering Awareness of Financial Employees. Ph.D. Thesis, Eastern Washington University, Cheney, WA, USA, 2013.
9. Russell, J.D.; Weems, C.F.; Ahmed, I.; Richard, G.G. Self-reported secure and insecure cyber behaviour: Factor structure and associations with personality factors. *J. Cyber Secur. Technol.* **2017**, *1*, 1–12. [CrossRef]
10. Talib, S.; Clarke, N.L.; Furnell, S.M. An analysis of information security aware-ness within home and work environments. In Proceedings of the International Conference on Availability, Reliability, and Security, Krakow, Poland, 15–18 February 2010; Volume 1, pp. 196–203.
11. Anderson, C.L.; Agarwal, R. Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Q.* **2010**, *34*, 613–643. [CrossRef]
12. Konieczny, F. USAFR NJT. SEADE: Countering the futility of network security. *Air Space Power J.* **2015**, *29*, 1–11.
13. Furnell, S. Why users cannot use security. *Comput. Secur.* **2005**, *24*, 274–279. [CrossRef]
14. Henshel, Q.; Hart, P.; Cooke, D. The role of external influences on organizational information security practices: An institutional perspective. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences 2006, Kauia, HI, USA, 4–7 January 2006; Volume 6, pp. 1–10. [CrossRef]
15. Almeida, V.A.F.; Doneda, D.; Abreu, J.S. Cyberwarfare and digital governance. *IEEE Internet Comput.* **2017**, *21*, 68–71. [CrossRef]