Scientific Research Publishing

Journal of Information Security, 2025, 16(1), 70-77
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

The Risks of the U.S. Cyber Crisis

Theo Lim

Crescenta Valley High School, La Crescenta, USA
Email: theotheolim@gmail.com

How to cite this paper: Lim, T. (2025) The Risks of the U.S. Cyber Crisis. *Journal of Information Security*, **16**, 70-77.
https://doi.org/10.4236/jis.2025.161003

Received: September 8, 2024
Accepted: December 7, 2024
Published: December 10, 2024

Abstract

In today's interconnected world, the ubiquitous influence of digital technology emphasizes the critical need to confront the growing menace of cybercrime. The unrelenting rise of cyber-attacks in the United States poses substantial hazards to individuals, corporations, and nations, jeopardizing economic stability, security, and personal privacy. This study aims to draw awareness of the seriousness of cyber dangers and emphasize employing proactive steps to protect our digital future. This paper stresses the necessity of cybersecurity, digital literacy education, and cybercrime awareness in mitigating these widespread hazards through extensive analysis and empirical research. A more resilient and secure digital environment for current and future generations can be established by cultivating a collective understanding of cyber dangers and developing effective preventative measures.

Keywords

Cybersecurity, Digital Literacy Education, Cybercrime Awareness

1. Introduction

In an era of unprecedented technological growth, the prevalence of digital technology has transformed almost every element of human existence. However, in the middle of this digital revolution, a looming threat: cybercrime exists. Data breaches and cyberattacks have increased in number and have become more sophisticated [1]. The spread of cyber-attacks offers an ever-increasing threat to individuals, organizations, and nations worldwide. These sophisticated and unrelenting assaults not only threaten economic stability and national security but also violate individuals' fundamental rights and privacy. In an increasingly interconnected world, it is crucial to acknowledge the significance of these cyber risks and take decisive actions to reduce their impact.

A case involving the Glendale Unified School District (GUSD) demonstrates

how severely cyber threats can affect local communities by jeopardizing the personal information of students and staff. On 6th December 2023, a cybersecurity ransomware attack started at GUSD by the Medusa ransom gang led to significant disruptions in school operations and exposure of sensitive personal information of students, parents, and staff [2]. As a result, all the GUSD employees and students were asked not to use district or personal devices to access any GUSD accounts or online resources, and they were also not allowed to use GUSD computers or Chromebooks [2] [3]. This incident highlighted the importance of information security in protecting educational institutions and the broader implications such breaches have on personal privacy and institutional integrity. Cases like such advocate for stronger defenses and better preparedness against cyber threats.

Cybersecurity is a crucial aspect of modern digital systems, encompassing a range of techniques and technologies to protect against unauthorized access and data breaches [4] [5] [6]. It is particularly important in the context of the Internet of Things, where growing reliance on computer systems increases vulnerability [4]. The field's multidimensional nature is underscored by its role in risk mitigation and digital fortification [5]. Cybersecurity measures are designed to safeguard Internet-connected devices, networks, and data, ensuring their confidentiality, integrity, and availability [7].

Cybersecurity has emerged as a critical component in today's digital landscape [5], encompassing both software and hardware aspects [7]. It remains a significant concern across various sectors [8], and its importance is underscored by the rapid growth of the digital world [9]. Indeed, industries dealing with substantial volumes of consumer data, such as finance, healthcare, and retail, are experiencing the swiftest rise in demand for cybersecurity professionals [10]. This demand reflects the necessity of safeguarding sensitive information and ensuring the integrity of digital infrastructures against evolving threats in our interconnected environment. As such, understanding and implementing effective cybersecurity measures has become imperative for organizations to mitigate risks and maintain trust in the digital realm.

This study aims to delve deeply into the complex cybersecurity environment, analyzing the internal difficulties confronting cybercrime in the United States. Composed with rigorous analysis and empirical research, the paper sheds light on the varied nature of cyber threats, ranging from phishing scams to ransomware attacks, as well as their negative consequences for society. By delving into the nuances of cybercrime, the paper hopes to highlight the urgent need for comprehensive solutions to protect the digital future.

Furthermore, this study aims to highlight the critical role of cybersecurity education and knowledge in empowering people to traverse the digital realm safely. By providing individuals with the knowledge and skills required to identify and mitigate cyber threats, a cyber resilience culture can be developed and defenses against hostile actors can be strengthened.

This journey to investigate the concerns of cybersecurity is motivated by a

shared desire to ensure the integrity and security of digital infrastructure. By cooperating and implementing creative solutions, a secure digital environment can be made.

2. Materials and Methods

2.1. Survey

A customized survey assessed cybersecurity opinions and experiences across age groups. The study covered various topics, including awareness levels, contact with cybercrime, and experience with cybersecurity education.

2.2. Data Collection

The survey was distributed electronically through multiple channels, including social media, email lists, and community outreach. This strategy ensured the inclusion of different respondents from various age groups, professions, and geographic areas, resulting in a varied sample.

To supplement the insights gained from private polls, data from credible sources such as USAFacts and the FBI was rigorously incorporated into the study framework [11]. Furthermore, references from authoritative agencies such as the FBI's Internet Crime Complaint Center and Bischoff's research were included, providing the study with complete and accurate data [12]-[14]. This research provides a detailed and full view of the current cyber threat scenario by combining direct views with reliable sources.

2.3. Cybersecurity Issues in the United States

This section of the research delves into the examination of the present condition of cybersecurity in the United States based on data from 2022. Through rigorous analysis, the study delineates the types and rates of cyber-attacks in the country, including threats such as phishing, ransomware, and data breaches. Furthermore, it examines the changing nature of cyber risks, emphasizing the growing sophistication of cyber-attacks enabled by technical breakthroughs. This section provides profound insights into the numerous challenges of cybercrime, allowing for more informed tactics to handle these issues effectively.

3. Survey Results and Data

Study Regarding Enhancement of Cyber Education

A research study was developed which highlighted the critical need to enhance and expand cyber-education. This study drew conclusions from an all-age survey that was distributed to volunteers without a specific sampling method, highlighting awareness and education gaps, and was motivated by earlier research.

As shown in **Figure 1**, out of sixty-eight respondents in total, only five of the individuals—who were directly or indirectly familiar with cyber threats—were able to attest to having taken a course on cybersecurity or ways to stop these kinds of attacks. Not one of them was older than fifty.

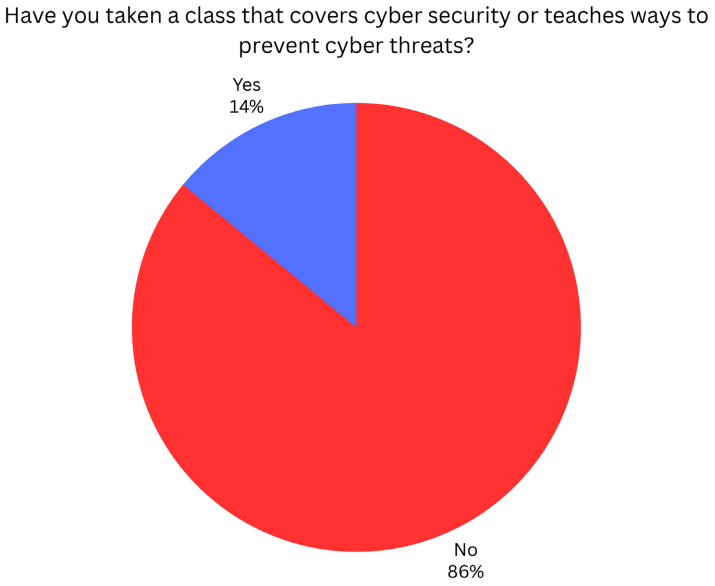

Figure 1. Graphical representation of survey regarding familiarity of classes covering the topic of cybersecurity.

Statistics of the last five to six years have reported that internet crime complaints have considerably increased, showing 515,612 complaints in 2020, while 162,091 complaints were reported previously. In the year 2021, phishing and allied cyberattacks, business emails, and malware were the main sources of data breaches. According to recent statistics, in 2022, ransomware cyberattacks surpassed phishing attacks due to the primary reason for data compromises. As end users, individuals play a vital role in defending against cyberattacks. However, the challenge is to identify the fake and malicious content and recognize it as an attack. An IBM (2022) report declared that 25% of security breaches in industrial organizations occurred due to human errors. The lack of effective staff training is the main cause of the success of these attacks [15].

4. Discussion

4.1. Perceptions and Responses to Cyber Threats by Age Groups

This study investigated how people of various ages perceive and respond to cyber threats, revealing significant generational disparities in cybersecurity awareness and practices. Notably, **Figure 2** showed that younger people, while more adept with digital technologies, displayed overconfidence in their cybersecurity awareness. This resulted in their uneven adherence to online safety protocols. On the other hand, older generations took a more careful approach to online contacts despite being less familiar with specific cyber threats.

A particularly remarkable finding was the disparity between perceived and real levels of cybersecurity expertise, especially among younger generations. This inclination toward overconfidence may result in a lack of vigilance in establishing appropriate security measures, increasing vulnerability to cyber threats. Furthermore,

the study found a pervasive lack of formal cybersecurity education across all age groups, indicating a severe gap in knowledge and preparedness.

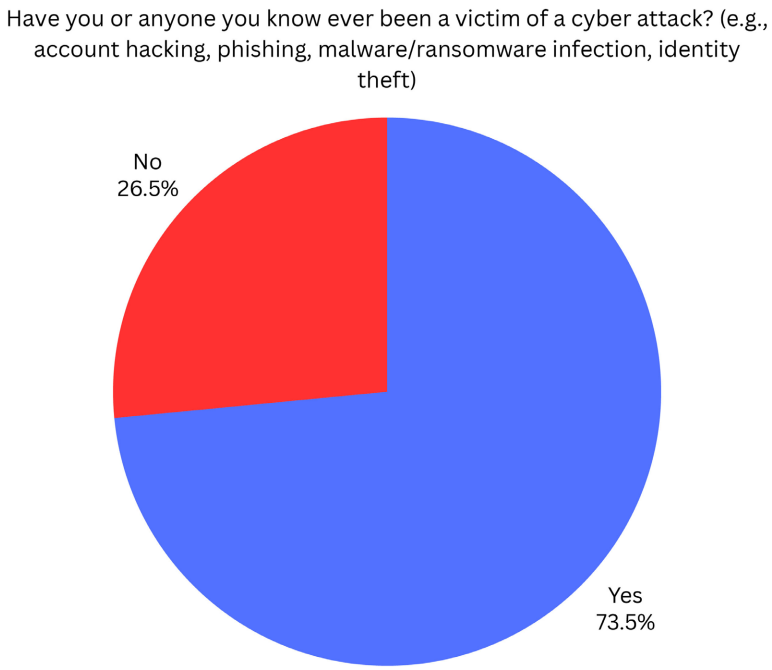

Figure 2. Graphical representation of survey results regarding awareness of cybersecurity issues.

4.2. Impact of Cyber Risks across Age Groups

Through a broad poll of people aged 18 to 65, a valuable insight was gathered into the pervasiveness of cyber threats across generations.

The poll analysis revealed startling results, with 73.5% of the 68 respondents across all age groups either directly experiencing cyber risks or knowing someone who has. While this sample size is limited, it provides valuable preliminary insights that could contribute to the identification of broader trends. These dangers include a wide range of disturbing actions such as account hacking, phishing, malware infections, ransomware assaults, and identity theft, demonstrating the pervasiveness of cybersecurity hazards.

Notably, as shown in **Figure 3**, more than half of the reported cases included compromised or stolen accounts, emphasizing the gravity of potential consequences such as financial loss and the exploitation of personal data. Furthermore, roughly 30% of occurrences were traced to phishing assaults, highlighting the misleading nature of such approaches and their ability to avoid typical security measures.

These findings highlight the importance of universal awareness and preparedness in fighting cyber dangers across all age groups. It is clear that cybersecurity literacy is not limited to experts but is an essential requirement for anyone navigating the digital realm.

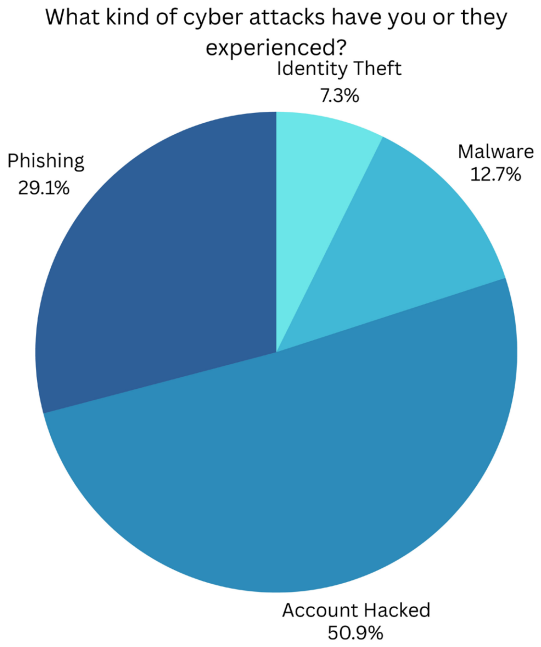

Figure 3. Graphical representation of the various cyber threats identified in the survey results.

4.3. Limitations

The study's limitations include its dependence on self-reported data, which could add bias to the conclusions. The limited sample size and the lack of analysis of the statistical significance may also prevent generalizability of these findings. Future studies could supplement the study by employing objective methods of measuring cybersecurity knowledge, increasing sample size and diversity, and conducting a significance analysis.

5. Conclusions

This research on cybersecurity risks provides a comprehensive overview of the present digital threat landscape and the readiness of varied groups to face these problems. It measured understanding and preparedness against cyber dangers across age groups, occupations, and geographical locations using a series of surveys.

The investigation into cybersecurity risks in the United States revealed that the most common cybercrimes include phishing, malware attacks, and identity theft. Notably, there has been an alarming increase in the frequency of ransomware attacks in recent years. While the findings indicate that the public is generally aware of cyber threats, there is still a need for a better understanding of specific types of assaults and effective security strategies.

Furthermore, this study looked into generational differences in cybersecurity awareness, finding that younger generations are more comfortable with digital technologies and frequently underestimate the severity of cyber hazards. Older generations, while more cautious, may lack the expertise required to identify and

manage advanced cyber threats successfully.

To strengthen the resilience of all generations, the paper proposes that educational institutions, workplaces, and government institutions implement targeted cybersecurity programs that emphasize practical security practices.

Moreover, implementing a holistic strategy for cybersecurity, which includes technical measures such as robust security software and encryption and strategic tactics such as employee training and awareness initiatives, is critical in mitigating and avoiding cybercrimes. Government laws and regulations are essential in improving national cybersecurity, while international coordination is required to combat cybercrime globally.

Finally, this study thoroughly reviewed cybersecurity risks and proposed a multidimensional approach to effectively tackling these difficulties. Understanding the nature of cyber risks and applying strategic solutions will help create a more secure and resilient digital environment in the future.

This study serves as a wake-up call for increased cybersecurity attention and education among people of all ages. As technology becomes more integrated into our daily lives, understanding and mitigating cyber dangers becomes increasingly essential, mandating concerted efforts to provide persons of all ages with the knowledge and skills they need to protect themselves online.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Bhagwani, V. (2023) Cybersecurity. *International Journal of Scientific Research in Science and Technology*, **7**, 1-9.

[2] (2023) Glendale School District Recovering from Cyber Attack. Government Technology. https://www.govtech.com/education/k-12/glendale-school-district-recovering-from-cyber-attack

[3] Zak, K. and Zak, K. (2023) GUSD Cyber Access Restored; Assistant Superintendent Named—Glendale News-Press. Glendale News-Press—Building Strong Communities, One Smile at a Time. https://outlooknewspapers.com/glendalenewspress/archives/gusd-cyber-access-restored-assistant-superintendent-named/article_ea3d2a4a-fd6a-5b8d-b34d-203e70693da4.html

[4] Pandey, P.K. (2021) Overview of Cybersecurity. *International Journal for Research in Applied Science and Technology*, **9**, 608-611.

[5] Kumar, R. (2023) A Review Article on Cybersecurity. *International Journal of Scientific Research in Engineering and Management*, **7**, 1-5.

[6] Burt, A. (2023) The Digital World Is Changing Rapidly. Your Cybersecurity Needs to Keep Up. Harvard Business Review. https://hbr.org/2023/05/the-digital-world-is-changing-rapidly-your-cybersecurity-needs-to-keep-up

[7] Yadav, B. (2022) Overview of Cybersecurity. *International Journal of Advanced Re-*

search in Science, *Communication and Technology*, **2**, 489-492.

[8] Ajankar, S.S. (2021) Cyber Security: Techniques and Perspectives on Transforming—A Review. *International Journal of Scientific Research in Science and Technology*, **8**, 473-480.

[9] Gulhane, P.N. (2021) Introduction to Cybersecurity—A Review. *International Journal of Scientific Research in Science and Technology*, **8**, 484-487.

[10] Madhumitha, V. (2023) Cyber Security. *International Scientific Journal of Engineering and Management*, **2**, 1-7. https://doi.org/10.55041/ISJEM00267

[11] USAFacts (2023) How Many Cyber-Attacks Occur in the US? https://usafacts.org/articles/how-many-cyber-attacks-occur-in-the-us

[12] Bischoff, P. (2021) Cybercrime Victims Lose an Estimated $318 Billion Annually. Comparitech. https://www.comparitech.com/blog/vpn-privacy/cybercrime-cost/

[13] Internet Crime Complaint Center (IC3). https://www.ic3.gov/

[14] Internet Crime Complaint Center (IC3) (2022) Annual Report 2022. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[15] Alnajim, A.M., Habib, S.J., Islam, M., AlRawashdeh, H.S. and Waseem, M. (2023) Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches. *Symmetry*, **15**, Article 2175. https://doi.org/10.3390/sym15122175