Journal of Computer Applications and Information Technology
Vol. 1, Issue. 1, March 2025, pp. 16~23

Cybersecurity in the Context of COVID-19: Analysis of Cyberattacks in the Pandemic

P. Siva Shamala Palaniapan[1], Zubaile Abdullah[2]
[1,2]University Tun Hussein Onn Malaysia, Malaysia

Article Info

Article history:

Received Jan 9, 2025
Revised Feb 20, 2025
Accepted Mar 11, 2025

Keywords:

COVID-19
Cybersecurity
Data analysis
WHO
Healthcare cybersecurity

ABSTRACT

The COVID-19 pandemic was a wonderful, remarkable occasion that adjusted the lives of billions of residents all around the world, bringing about what turned out to be regularly alluded to as the new-ordinary as far as cultural standards and how we live and work. Besides the remarkable sway on society and business overall, the pandemic created a lot of special digital wrongdoing related conditions which additionally influenced society and business. Security in the healthcare sector is essential as it includes patients' data and medical details. Our examination utilized information investigation to evaluate the effect of cybercrime on emergency clinics, distinguish weak medical services, associations, and set up preventive estimates custom-made for the medical services industry. We revealed that emergency clinics altogether lost, in any event, $2 billion during the initial 5 months of COVID-19, medical care suppliers in California are the most powerless against digital assaults.

Corresponding Author:

P. Siva Shamala Palaniapan,
University Tun Hussein Onn Malaysia, Malaysia.

1. INTRODUCTION

The pandemic has made a colossal test for organizations around the world: to keep working notwithstanding huge shutdowns of workplaces and different offices. The data innovation on which they had for a long time ago depended – their server farms, cloud frameworks, departmental workers, and the computerized gadgets their now-far of representatives used to remain associated with one another and to the organization's information – turns out to be significantly progressively essential. Overnight, the requests put in the computerized framework have soared.

Such innovation additionally turns into a lot greater and increasingly rewarding objective for cybercriminals. Cybersecurity endeavors should be moved up to keep a second emergency from rising: on the computerized gadgets and systems that have gotten unendingly increasingly crucial to organizations as of late. At the end of the day, "business progression" has become a command.

Coronavirus phishing stunts started flowing in January, following fears and chaos about the infection, they've quite recently increased since. Seven days back, Brno University Hospital in the Czech Republic, a noteworthy Covid-19 testing community, endured a ransomware assault that upset tasks and caused medical procedure delays. Additionally, even refined nation-state programmers have been using pandemic-related catches to spread their malware. The conditions are prepared for cyberattacks of various types. There is a treacherous symptom of coronavirus.

Programmers of all stripes are finding the conditions impeccable to worm their way into individual and corporate records. Telecommuters getting to their association frameworks from singular gadgets at home make it less difficult for software engineers to break cybersecurity. IT groups are similarly compelled to engage far off work, cutting down security shows.

The World Health Organization declared an increase of cyber attacks a month prior, including an endeavor to reflect its inside email structure to get passwords of staff individuals. Security firm Barracuda Networks moreover observed a colossal overall spike in email phishing identified with the coronavirus, pursuing people's sentiments of fear and interest.

2. RELATED WORK

At the starting stage, the virus has been identified for about nearly 4 months, and yet there is some confusion on what the virus is originally termed. The World Health Organization (WHO) has organized coronavirus (CoV) as a huge group of viruses that can create many disorders like from common cold and up to more serious disorders like (SARS-CoV)- Severe Acute Respiratory Syndrome and Middle East Respiratory Syndrome (MERS-CoV) coronavirus. This has originated two various names spreading around in the media, however, the WHO has confirmed the correct name of the disease is COVID-19. Since the onset of COVID-19, hospitals in the United States has seen an unprecedented increase in data breaches.

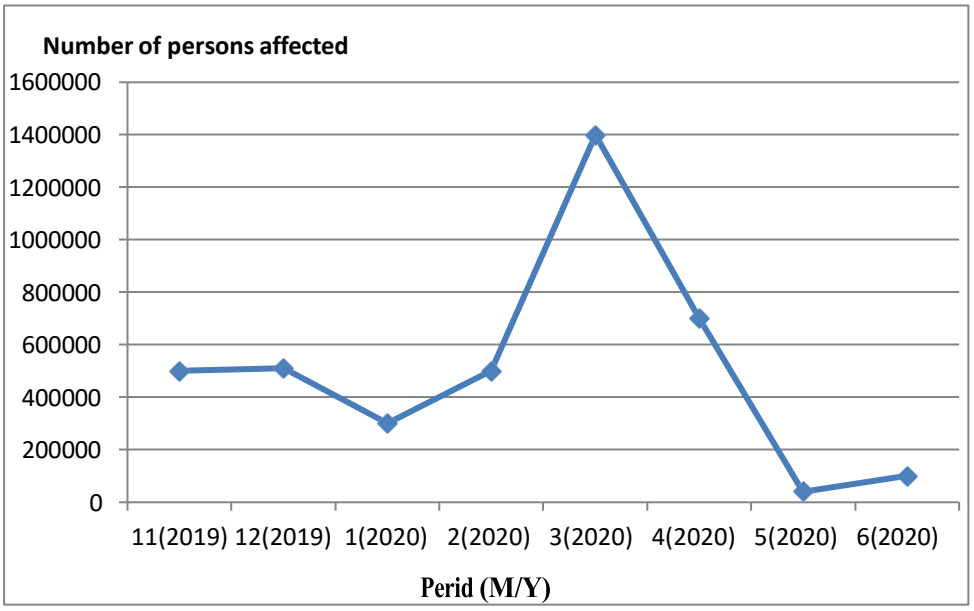

Figure 1. Cyberattacks against hospitals

In February month simply as COVID-19 started to reach the US- the whole number of people affected by health-related cybercrime increased from 500,000 in January to 1.6 million – a 224 percentage rise. There are the reported data breaches; as per the PRC, 60-89 percent of data breaches remain unreported.

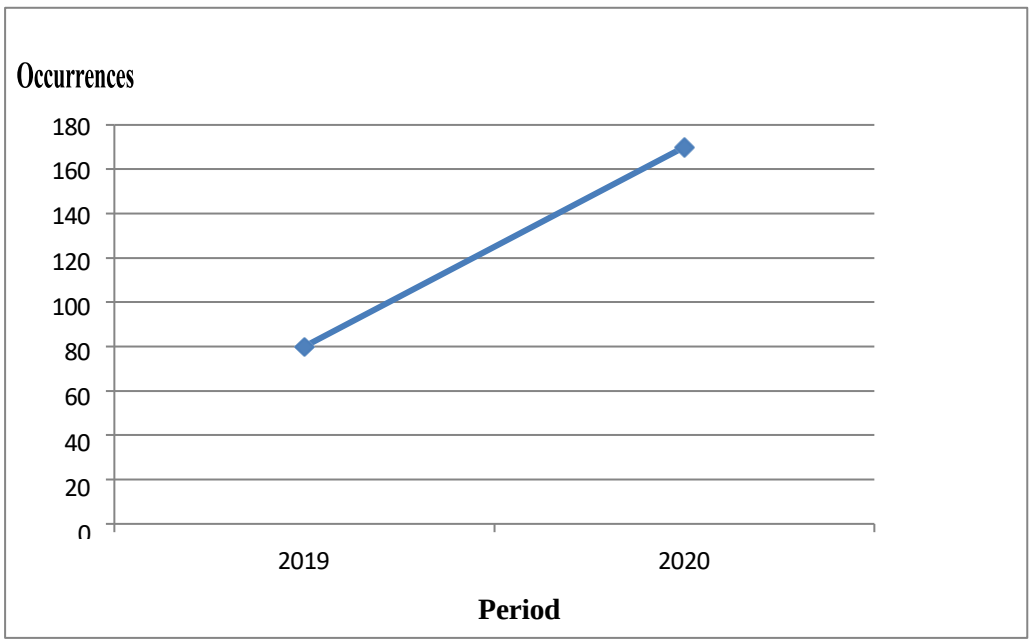

Figure 2. Infringe in the initial stage

Out of the 179 confirmed breaks that occurred between February and June, 57.5% were expected to be hacked, 24.5% were because of unapproved revelation and 8.3% were because of burglary.

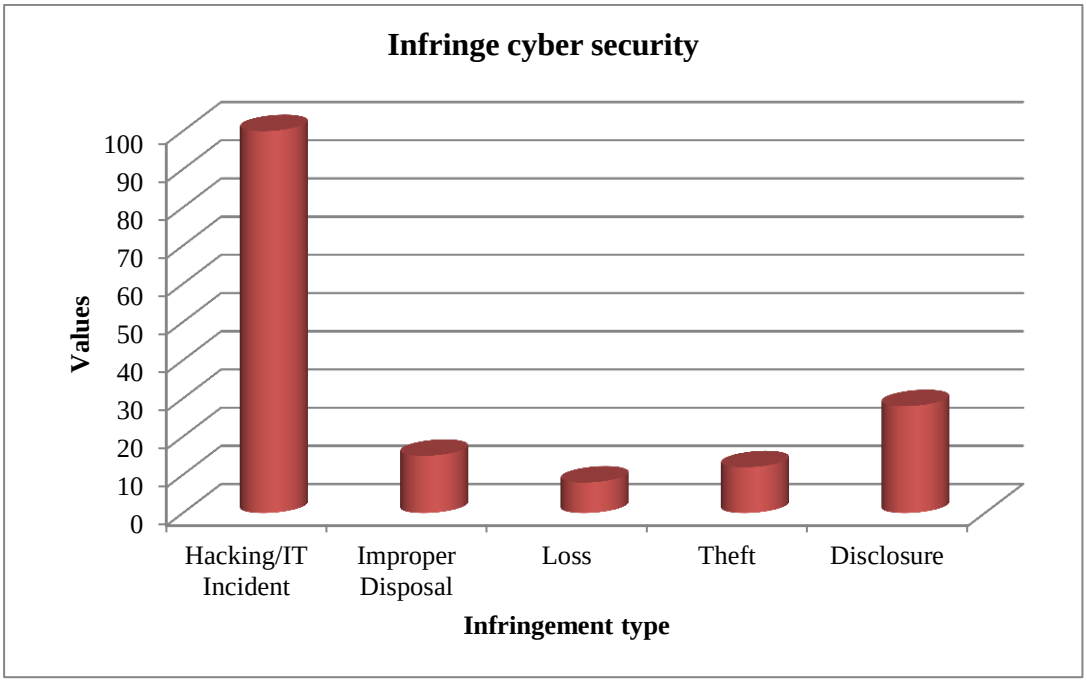

Figure 3. Healthcare cybersecurity Infringement

Unfortunately, these numbers are obvious. As per Corvus, over 75% of the clinics don't utilize measures as basic as email checking and separating tools [3]. A report by IBM recommends that solitary 15% of medicinal services associations have full sent security computerization innovations while 48% have no robotized instruments by any means.

3. IMPACT

Hackers are exploiting a medical services industry zeroed in on COVID-19. Programmers realize that the medical care industry is a wreck right now regarding cybersecurity and this gives them considerably more inspiration to make an ever- increasing number of assaults. After a system has been undermined, the programmer's design is uncovered. The primary rationale in hacking into a medical clinic is monetary profit. Programmers bring in cash by selling patients' ensured wellbeing data out by holding the system for delivering for as much as a large number of dollars.

Cybercrime against medical clinics and social insurance associations has a high human expense. Cyber attacks and information breaks can bolt out an emergency clinic's framework for quite a long time—constraining the medical clinics to dismiss new patients and postpone medical procedures. As indicated by an examination by Vanderbilt University, information breaks cause 36 extra passings for every 10,000 coronary failures every year. In 2019, 83% of human services, associations revealed an expansion in cyber attacks.[5] As COVID-19 cases flood in the United States and medical clinics being flooded, cyber-attacks can prompt considerably more passings.

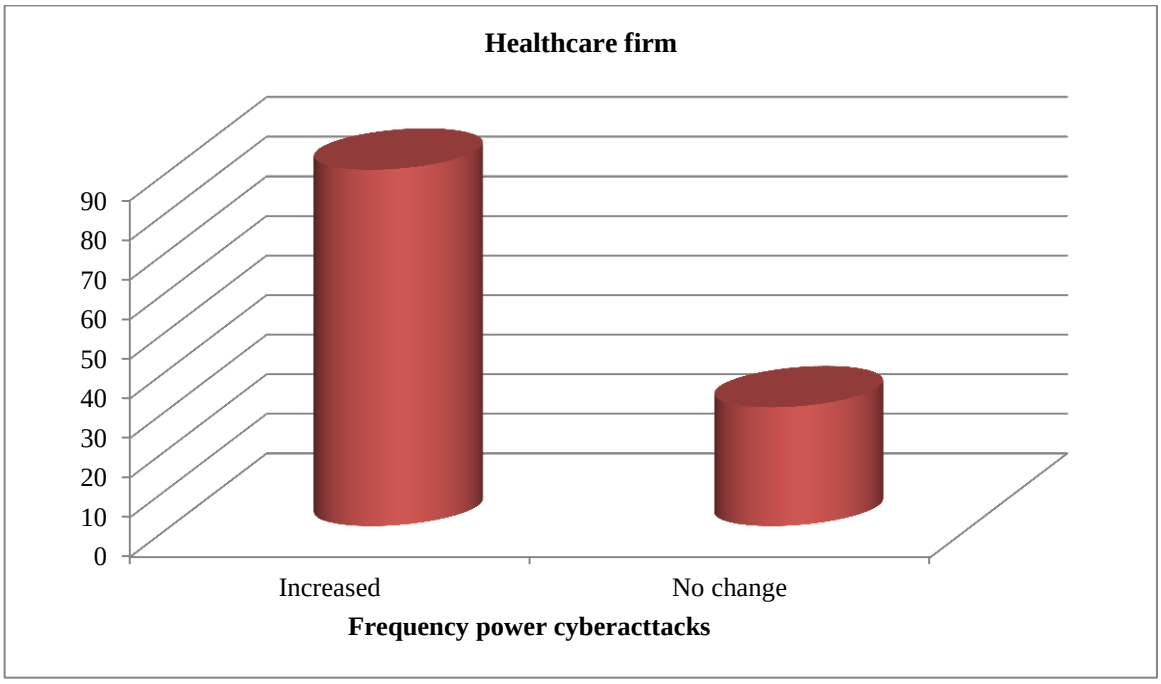

Figure 4. Cyberattacks

Aside from the human cost, information penetrates additionally have a robust dollar-cost related to them. As indicated by an IBM report, emergency clinic information breaks cost $429 per record in 2019. This implies the American medicinal services industry lost over $700 million just in February and nearly $2 billion since the beginning of COVID-19. Providing health care services access is the foundation of a triumphant health reaction. Each physical act of assault, obstacle, or hazard that obstructs the accessibility, approach, and liberation of such works is described as an intervention in health care by the WHO. As mentioned in figure 5, the nature of the offensive on healthcare-associated to COID-19 differs significantly across situations and can series from the utilization of serious weapons aiming health amenities to the accusation of health care workers.

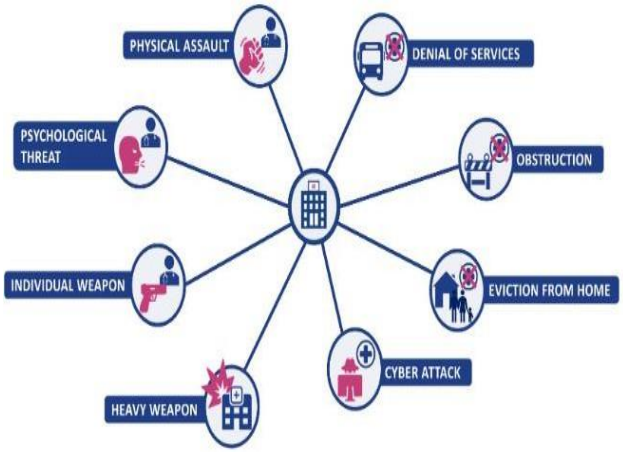

Figure 5. Various types of attacks related to COVID-19

Vulnerabilities

Human services, suppliers took the brunt of these assaults—representing an astonishing 71% of the breaks. They were trailed by Business Associates and Health Plan associations that represented 16.8% and 11.7% of the penetrates separately.

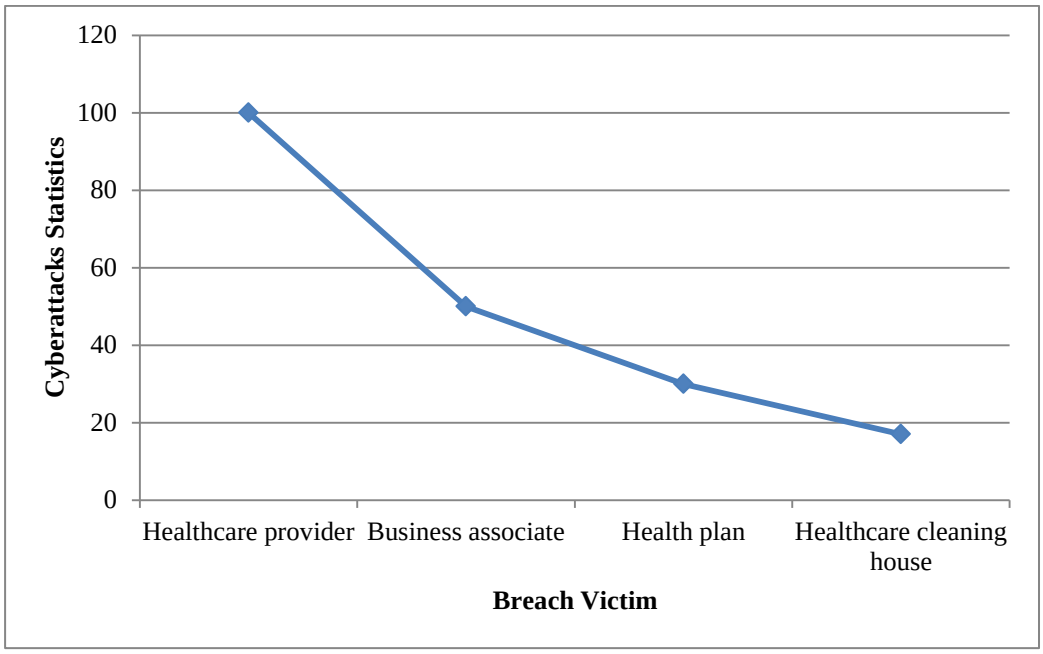

Figure 6. Breach Entity

The messages were the greatest method of danger transmission—causing 44% of the breaks. System Server and Paper/Films were the following basic section focuses.

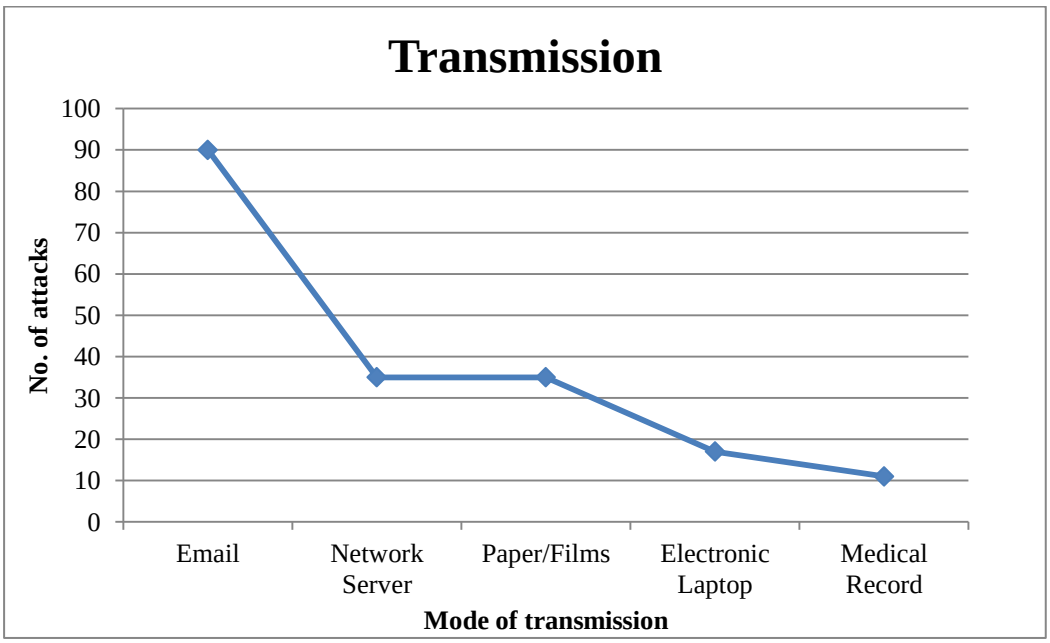

Figure 7. Mode of transmission

Electronic Medical Records and Laptops were other normal passage focuses. Strikingly, 4% of the breaks were accounted for as being brought about by a blend of email and system worker. California's medical clinics were focused on the most as they represented 11% of the complete cases. Be that as it may, after California, a large portion of the 38 states that announced information penetrates were stuffed intently.

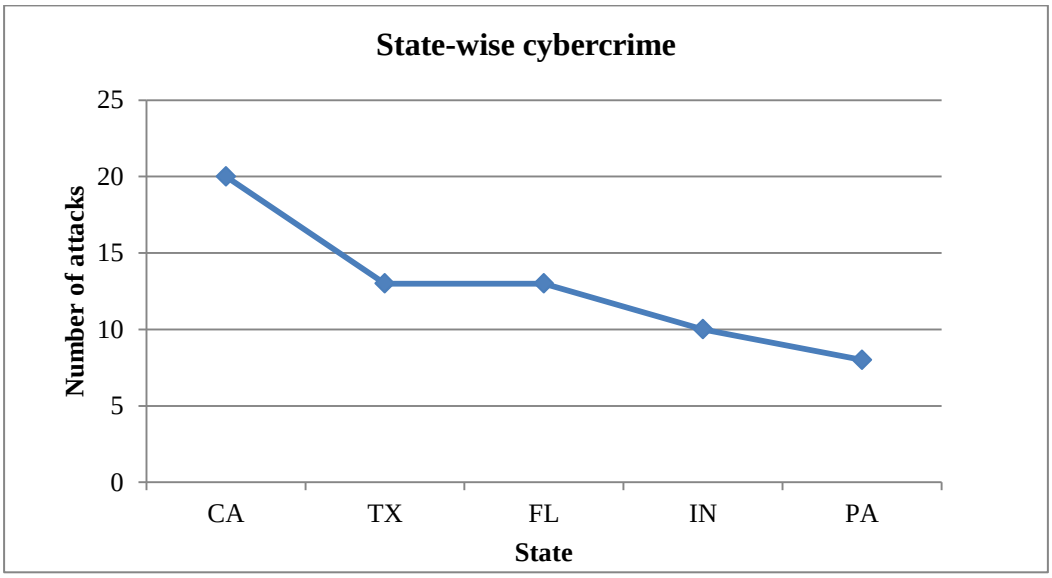

Figure 8. State-wise cybercrime against healthcare

69% of such infringements were performed in the absence of a business partner. The state-wise cybercrime against healthcare is depicted in Figure 8.

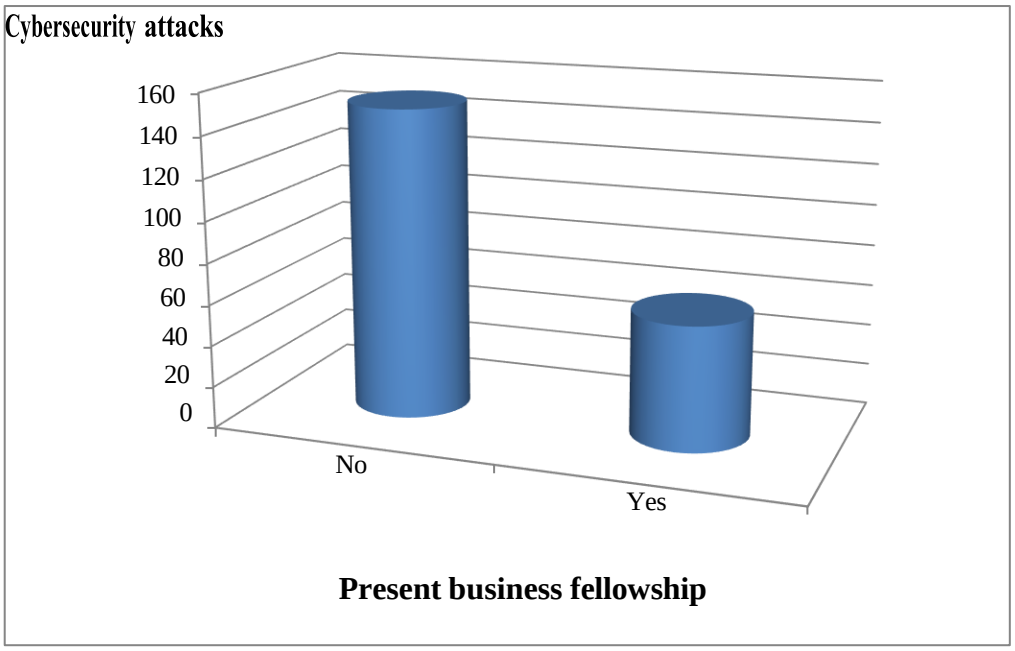

Figure 9. Risk assessment: business associate

4. RESULT

Preventive Measurement

With hacking being by along the most basic cybersecurity break—clinics need to embrace fundamental procedures to protect their information. Medicinal services associations will in general utilize obsolete renditions of programming projects, internet browsers, and working frameworks. These give programmers simple access to their data [8].

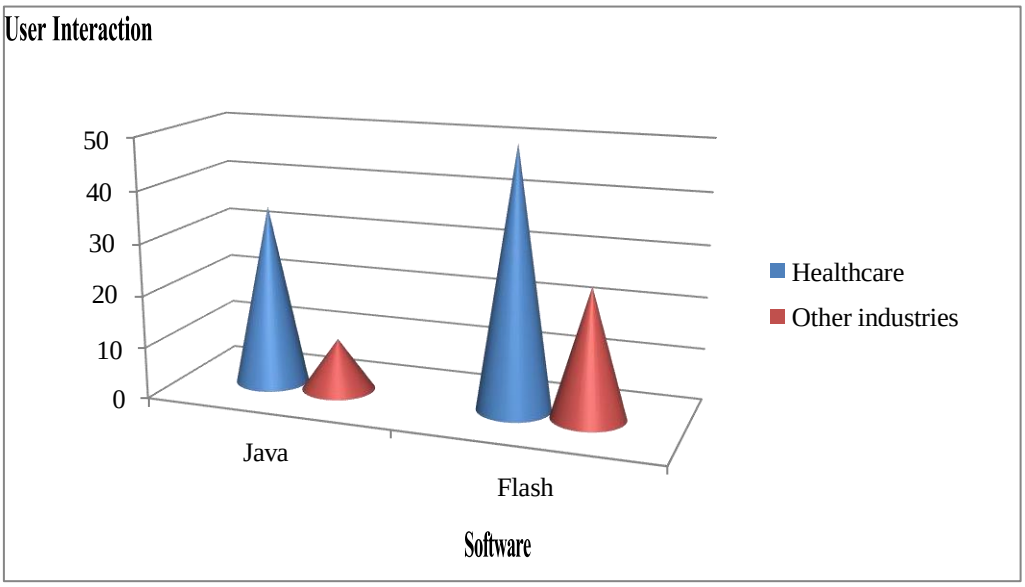

Figure 10. Prevention Strategy

As a matter of first importance, human services suppliers should ensure all their products and equipment is exceptional. Besides, they should take normal reinforcements to guarantee that a duplicate of information exists on either the cloud or outer drives. Persistent information ought to likewise be scrambled and never communicated over open systems. Thirdly, antivirus virtual products ought not exclusively to be introduced yet in addition to consistently refreshed and kept up.

IT groups need to have

a) Professional level email bolsters that squares explicit connections dependent on Hash and record expansion

b) Anti-malware programs that filter all connections before opening them

All connections ought to be gone through either transparency report, checkphish.ai, or urlscan.io before being opened. COVID-19 spaces are half bound to be malicious9 thus emergency clinics should utilize checked blocklists like cyberthreatcoalition.org/blocklist on their system foundation.

Additionally, solid passwords ought to be utilized and 2-factor validation ought to be placed in place.

These fundamental advances can forestall the greater part of the phishing and information penetrates at medical clinics. Wellbeing associations with IT groups ought to normally screen the emergency clinic system to distinguish any anomalies and unordinary action. In conclusion, clinics need to critically build consumption on safety efforts and virtual products.

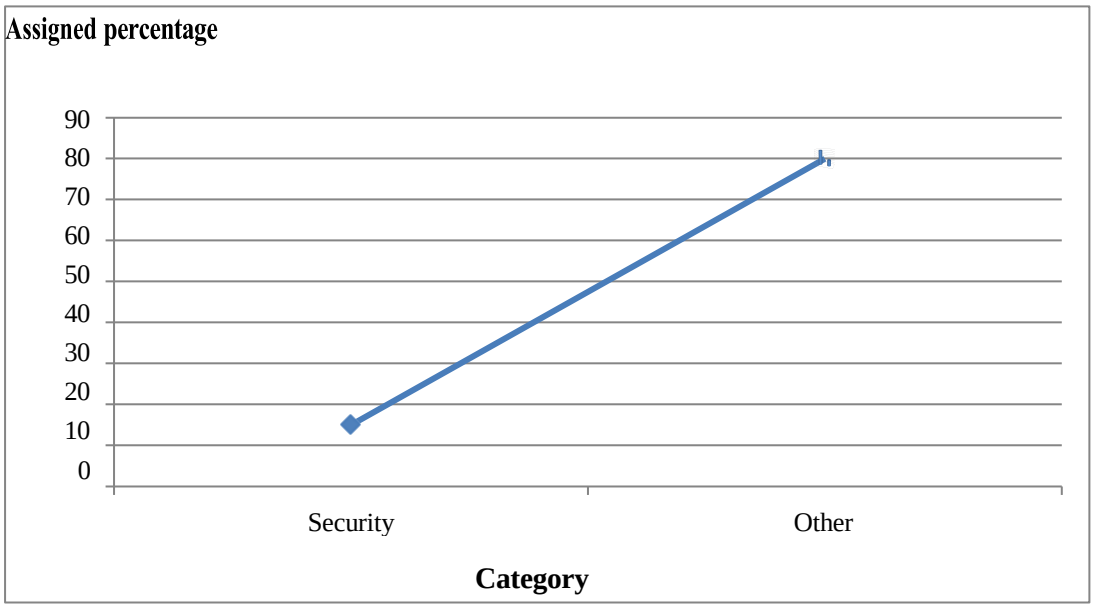

Figure 11. Assigning of the technology budget

5. CONCLUSION

The medicinal services industry is helpless against digital assaults simply like each other industry, even though the expenses – both human and fiscal – can be wrecking. The rising cybersecurity dangers of this industry can be diminished altogether by taking defensive measures.

REFERENCES

[1] Francois Mouton, Arno de Coning, “COVID-19: Impact on the Cyber Security Threat Landscape”, 1-18.
[2] "Breach Report - US Department of Health & Human Services ttps://ocrportal.hhs.gov/ocr/breach/breach_report. jsf
[3] "A closer look at data breaches – Oxford Academic. "https://academic.oup.com/cybersecurity/article-pdf/2/1/3/26672851/tyw003.pdf.
[4] "Open Ports, Phishing Key Targets in Healthcare Ransomware" 5 Jun. 2020, https://healthitsecurity.com/news/open-ports-phishing-key-targets-in-healthcare-ransomware-attacks.
[5] "2019 Cost of a Data Breach Report – All About SECURITY." hthttps://www.all-about-security.de/fileadmin/micropages/Fachartikel_2 8/2019_Cost_of_a_Data_Breach_Report_final.pdf.
[6] "New Study: Hospital Breaches Could Be Killing Patients" 8 Nov. 2019, https://www.infosecurity-magazine.com/news/hospital-breaches-could-be-killing/.
[7] "Cost of a Data Breach Study | IBM." https://www.ibm.com/security/data-breach.
[8] "The Current State of Healthcare Endpoint Security | Duo Security." 21 Apr. 2016, https://duo.com/blog/the-current-state-of-healthcare-endpoint-security.
[9] "Coronavirus-themed domains 50% more likely to be malicious" 6 Mar. 2020, https://www.cybertalk.org/2020/03/06/coronavirus-themed-domains-50-more-likely-to-be-malicious-than other-domains/.
[10] "5% of hospital IT budgets go to cybersecurity despite 82% of" https://www.beckershospitalreview.com/cybersecurity/5-of-hospital-it-budgets-go-to-cybersecurity-despite-82-of-hospitals-reporting-breaches.html.
[11] Susan Alexandra, Cybersecurity & Healthcare During COVID-19, April 13, 2020, https://www.globalsign.com/en/blog/cybersecurit y-healthcare-during-covid-19