iJournals: International Journal of Software & Hardware Research in Engineering
ISSN:2347-4890, ijournals.in/ijshre
Volume 12 Issue 10, October 2024

What are the vulnerabilities of critical US infrastructure, and how could it be protected from cyber-attacks?

Authors: Prof. Richmond Ikechukwu Ibe (PhD)[1]; Dr. Marshal Wenong (PhD)[2]

Affiliation: Western Governors University, UT, U.S.A School of Technology College of IT(Cybersecurity)[1]; Laerdal Medical R&D-Gatesville, TX[2]

DOI: 10.26821/IJSHRE.12.10.2024.121003

Abstract

This study explored six areas of US critical infrastructure and their vulnerabilities. In addition, the type of incidents where these infrastructures could be most vulnerable to attack. These incidents include Cyber-attacks, Natural disasters, and Physical attacks. The problem researched was to understand the critical infrastructure vulnerabilities in the United States. The purpose is to review factors that created these vulnerabilities and find ways to mitigate them. The digitalization of systems appears to have created vulnerabilities to the U.S. critical infrastructure. This study elucidated why critical infrastructure should be protected. In this study, we used a quantitative method approach with a non-parametric test specifically the Kruskal-Walli's test to analyze various critical infrastructure areas highly vulnerable to an attack. This research is grounded in Evolutionary Theory. The Evolutionary theory argues that cyber threats constantly evolve; thus, cybersecurity mechanisms must continuously adapt to keep pace. The NIST Risk Management Framework "RMF" (NIST SP 800-53) was used to mitigate the risk. The possible impact of cyber-attacks on critical systems cannot be ignored. This study explored key cyber vulnerabilities facing U.S. critical infrastructure, as well as mitigation and remediation strategies. The rapid integration of Internet of Things (IoT) devices into critical infrastructure systems has exacerbated the attack surface. These devices often lack adequate security measures, making them easy targets for cybercriminals looking to infiltrate extensive networks. We compared the vulnerabilities amongst these vital infrastructures based on the nature of the attack. The result showed that the incidence of cyber-attacks was higher than physical and natural disasters. This research could benefit government agencies, critical infrastructure policymakers, and organizations that provide critical services. Also, this research could be adopted in academia to teach students who may have professional initiatives on how to manage critical infrastructure. Further research is needed in this field to understand the gaps in protecting these infrastructures.

Keywords: Cyber-security, Critical Infrastructure, Infrastructure Management, Internet of things, and cybersecurity strategies.

Introduction

This research investigated the vulnerabilities of critical US infrastructure, and how it could be protected from cyber-attacks. This study explored six critical areas of US Infrastructure: Water Utility, Energy, Transportation, Healthcare, Financial, and government. In this research, we looked at different incidents such as cyberattacks, Natural disasters, and Physical attacks on these critical infrastructures to determine which of those

has the highest vulnerability to attack. We used Kruskal-Walli's test to analyze various critical infrastructure areas highly vulnerable to an attack. We reviewed different literature that dealt with US critical infrastructure vulnerability to understand the current events and to contribute to the body of knowledge. In this study, we reviewed the problem statement, Purpose statement, Background of the study, Theoretical framework, Literature review, Methodology, Integrated analysis, discussion, and conclusion.

Problem Statement

The digitalization of infrastructural systems appears to have created vulnerabilities to the U.S. critical infrastructure. Many organizations seem not to have paid much attention to addressing the vulnerability issues imposed by the digitalization of these critical Assets. According to Allianz Commercial (2016), "Critical infrastructure, like power generation and distribution, is becoming more complex and reliant on networks of connected devices. Just decades ago, power grids and other critical infrastructure operated in isolation. Now they are far more geographically interconnected and across sectors." Further, the vulnerability of critical infrastructure to cyber-attacks and technical failures has become a big concern (para.7).

Purpose statement

The study aims to understand the critical infrastructure vulnerabilities in the United States and find ways to mitigate risks of possible inadequate care within these infrastructures across sectors. The digitalization of infrastructures has made them more connected than ever before, quite unlike when it was isolated—as a result, it has made them vulnerable to attack. The purpose is to review factors that created these vulnerabilities and find ways to mitigate them.

Background information

America's critical infrastructure is the foundation of modern life and includes systems and assets vital to national security, economic prosperity, sanitation, and public safety. However, they face more cybersecurity threats since these infrastructures are more connected and based on digital technologies. These connections stem from electrical projects to water systems, networks in transportation, and healthcare facilities. The potential impact of cyber-attacks on critical systems cannot be ignored. This study explores key cyber vulnerabilities facing U.S. critical infrastructure, as well as mitigation and remediation strategies.

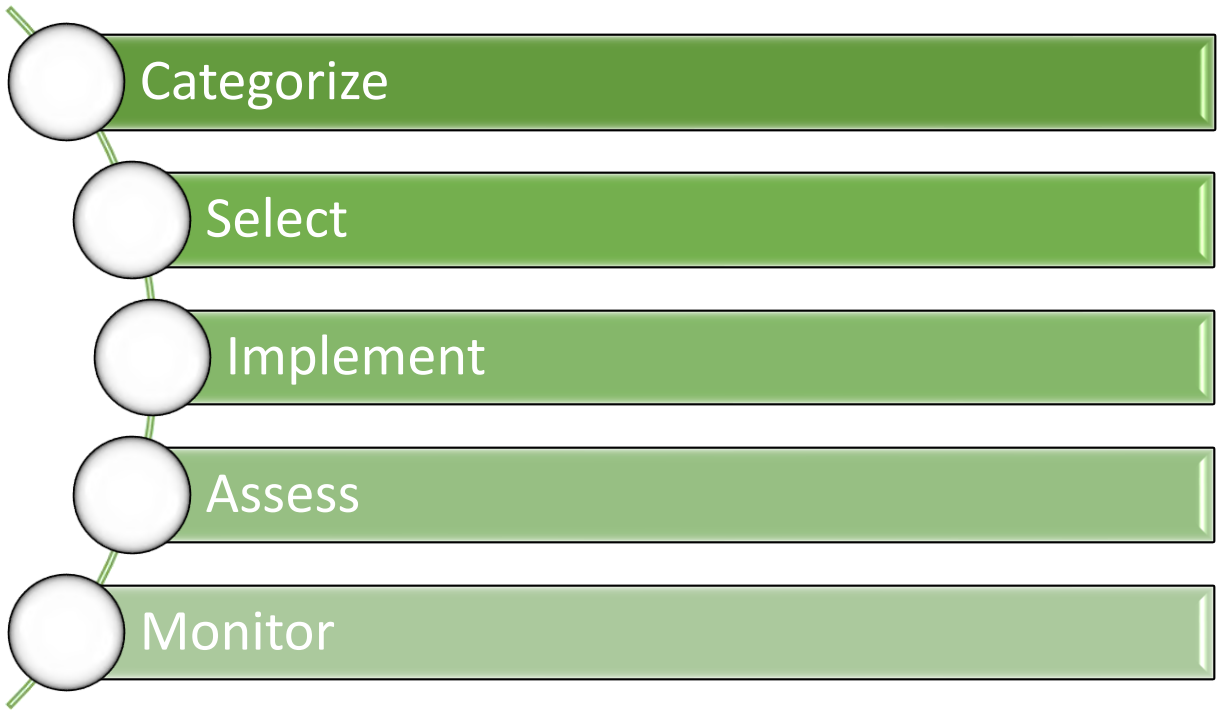
The rapid integration of Internet of Things (IoT) devices into critical infrastructure systems has expanded the attack surface. These devices often lack sufficient security measures, making them easy targets for cybercriminals looking to infiltrate wider networks. Butsianto, Nugraha, Anwar, Anwar, & Judijanto (2024) asserted that "As society becomes increasingly reliant on interconnected devices, ensuring the security of IoT ecosystems is imperative for fostering a trustworthy and resilient digital environment."

Theoretical Framework

This study used the Evolutionary Theory to assess the vulnerabilities of US critical Infrastructure, and how it could be protected from Cyber Attacks. According to Zero Trust Solution (2023) "The Evolutionary theory argues that cyber threats constantly evolve; thus, cybersecurity mechanisms must continuously adapt to keep pace. The theory suggests that cybersecurity measures must be designed to be flexible and capable of changing in

response to the evolving threat landscape" (para.1). This study will adopt the NIST risk management framework to understand how these critical infrastructures are managed and provide the mitigating strategies to protect them.

The NIST Risk Management Framework "RMF" (NIST SP 800-53)



Literature review

According to the US Government Accountability Office "GAO" (2024), "Critical infrastructure has been targeted on several occasions. The best-known incident was in Ukraine in 2015 when hackers successfully infiltrated the electric utility's SCADA system. Key circuit breakers were tripped, and the SCADA system became unusable, causing a system-wide power blackout. It left a quarter of a million people without electricity, in the middle of winter, for up to six hours." (Para.1).

"In October 2019, reports from India confirmed that hackers had infiltrated the country's biggest nuclear power station, at Kudankulam in the southern state of Tamil Nadu. According to the virus scanning website VirusTotal, the hackers had managed to infect at least one computer with malware before the breach was detected." (Para.2)

"In 2020, a series of cyber-attacks targeted Israeli water systems, including pumping stations, sewer systems, and wastewater plants. Cyber terrorists exploited vulnerabilities in outdated ICS to gain access. Fortunately, the attacks failed to disrupt the water supply, but it is believed the hackers were attempting to increase chemicals such as chlorine in the water to harmful levels." (Para.3).

For example, power lines can affect telecommunications, financial services, and healthcare. Additionally, many infrastructure projects rely on third-party suppliers to provide technology and services, introducing supply chain risks. Affected products or software from these vendors may serve as entry points for cyber-attacks. An example of this was the 2020 SolarWinds supply chain attack which highlighted a lack of capacity in third-party equipment, demonstrating that vulnerabilities at vendors can have a significant impact on critical businesses (SolarWinds Cybersecurity Incident, CISA, 2020).

As these systems become increasingly digital and interconnected, they also become more vulnerable to cyberattacks. These attacks can disrupt essential services, cause economic and environmental damage, and undermine public trust in state institutions and security systems. Cyber threats to critical infrastructure are becoming more sophisticated and frequent, as evidenced by several high-profile incidents in recent years. Adversaries ranging from nation-states to cybercriminals to terrorist groups have demonstrated both the ability and intent to exploit vulnerabilities in critical infrastructure for a variety of purposes, including espionage, financial gain, and geopolitical influence (Leandros et al., 2018). The purpose of this article is to examine whether America's critical infrastructure is vulnerable to cyberattacks, using the power grid as an example. This research includes the study of the nature and consequences of these vulnerabilities, existing cybersecurity systems, and the challenges they face. Industry reports and case studies propose a series of solutions designed to improve the resilience and security of the U.S. power grid and other critical infrastructure sectors. These solutions encompass technological innovation, policy reform, and joint public-private sector initiatives. This article aims to contribute to the ongoing discourse on national security and resilience in the face of evolving cyber threats.

Human error and internal threats also pose significant cybersecurity risks to critical systems. Employees in these offices can be attacked by clicking on phishing emails, using weak passwords, or using false information. Additionally, whether intentional or unintentional, insider threats can result in data deletion, vandalism, or other malicious activity that disrupts operations and leads to security disruptions. According to Buenning (2024), “While technological advancements improve security measures, human error remains a threat in cybersecurity vulnerabilities. The relationship of human error to cybersecurity risks covers a range of unintended actions that compromise the integrity of digital systems. This guide explores the complex connection between human error and cybersecurity risks, providing light on unintentional actions that often serve as gateways for security breaches.” (para2).

Verizon, (2021) report found that 85% of data breaches in the healthcare industry are caused by human error, highlighting the importance of people's operational cybersecurity training and awareness. Another major threat is Ransomware attacks and national threats targeting critical systems are becoming more common as attackers attempt to gain access to critical systems and demand payment for their release. These attacks can cause serious disruptions in operations, and financial losses, and even pose a threat to public safety. Additionally, national actors can target critical systems that are part of a criminal or regional conflict and use available cyber resources to gain access and disrupt important processes. A case in point is the Colonial Pipeline ransomware attack that shut down one of the largest pipelines in the United States in 2021. This incident revealed the vulnerability of critical systems to cyber threats and the consequences of such attacks on other critical systems. (Colonial Pipeline Cybersecurity Incident, 2021).

Research Method

This research used a non-parametric test specifically the Kruskal-Walli’s test to analyze various critical infrastructure areas highly vulnerable to an attack. We used the non-parametric test because it would help to test two or more independent samples. In addition, the data collected was secondary data and the researcher could not ascertain if the data is normally distributed. Understanding the vulnerabilities of each critical infrastructure would help to develop a resilience strategy to protect them. The analysis would help to determine which areas of infrastructure are vulnerable to attack, by comparing several types of attacks to each of the critical Infrastructures.

Data Collection Methods

The secondary data collection was used for this research. The data collection sources included the Department of Homeland Security (DHS) data, HIFLD Open Data, Federal Bureau of Investigation (FBI) Data,

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) data, and National Cybersecurity and Communications Integration Center (NCCIC) data. The data was analyzed using SPSS software.

Result

Table 1: Hypothesis Test Summary

Hypothesis Test Summary

	Null Hypothesis	Test	Sig. [a,b]	Decision
1	The distribution of Water and Wastewater Systems is the same across categories of Incidents.	Independent-Samples Kruskal-Wallis Test	.368	Retain the null hypothesis.
2	The distribution of Energy and Utilities is the same across categories of Incidents.	Independent-Samples Kruskal-Wallis Test	.368	Retain the null hypothesis.
3	The distribution of Transportation Systems is the same across categories of Incidents.	Independent-Samples Kruskal-Wallis Test	.368	Retain the null hypothesis.
4	The distribution of Healthcare and Public Health is the same across categories of Incidents.	Independent-Samples Kruskal-Wallis Test	.368	Retain the null hypothesis.
5	The distribution of Financial Services is the same across categories of Incidents.	Independent-Samples Kruskal-Wallis Test	.368	Retain the null hypothesis.
6	The distribution of Government Facilities is the same across categories of Incidents.	Independent-Samples Kruskal-Wallis Test	.368	Retain the null hypothesis.

a. The significance level is .050.

b. Asymptotic significance is displayed.

Independent-Samples Kruskal-Wallis Test

Table 2: Water and Wastewater Systems across Incidents

Independent-Samples Kruskal-Wallis Test Summary

Total N	3
Test Statistic	2.000[a]
Degree Of Freedom	2
Asymptotic Sig.(2-sided test)	.368

a. The test statistic is adjusted for ties.

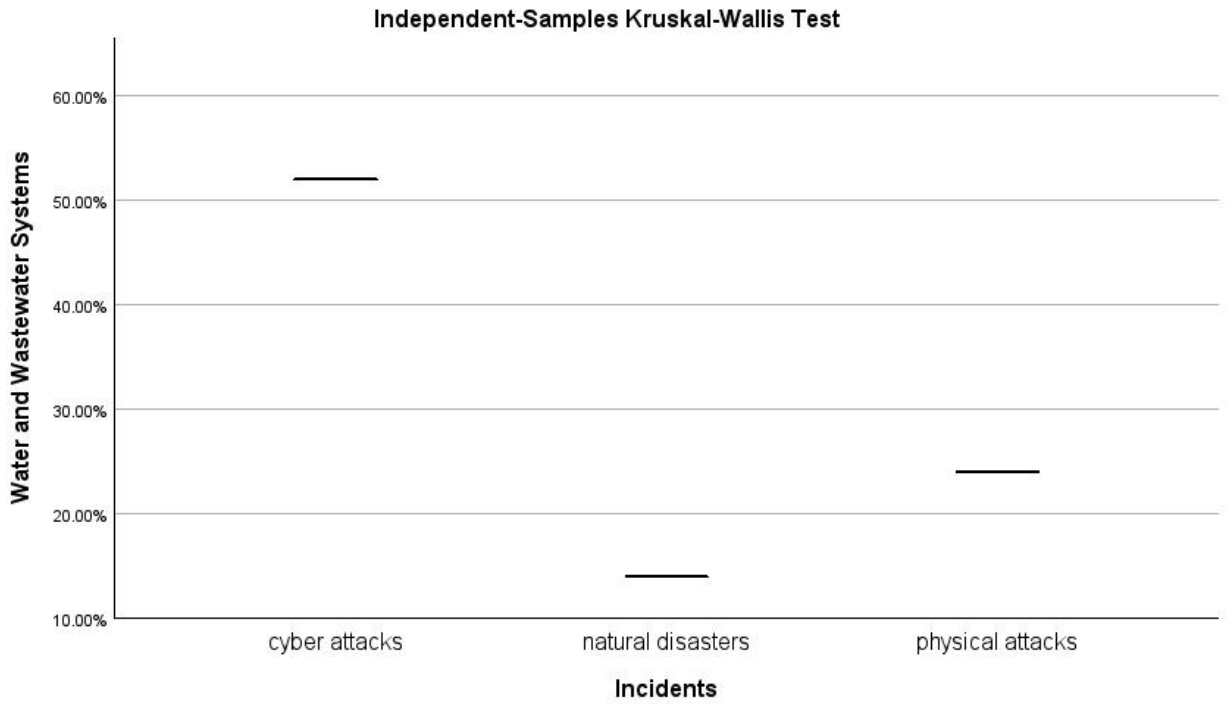


Fig 1: Independent Samples Kruskal-Wallis Test

The Fig 1 was generated based on Table 2 data that represents the Water and wastewater systems. The water and wastewater systems were computed against Incidents that occurred within the infrastructure such as cyber-attacks, natural disasters, and Physical attacks. The result showed that Cyber-attacks incidents were incredibly significant at > = 0.05 and ranked above 50% compared to natural disasters at above 10%, and physical attacks at above 20%, respectively.

Table 3: Pairwise Comparisons of Incidents

Pairwise Comparisons of Incidents

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig. [a]
natural disasters-physical attacks	-1.000	1.414	-.707	.480	1.000
natural disasters-cyber attacks	2.000	1.414	1.414	.157	.472
physical attacks-cyber attacks	1.000	1.414	.707	.480	1.000

Each row tests the null hypothesis that the Sample 1 and Sample 2 distributions were the same.

Asymptotic significances (2-sided tests) are displayed. The significance level is .050.

a. Significance values have been adjusted by the Bonferroni correction for multiple tests.

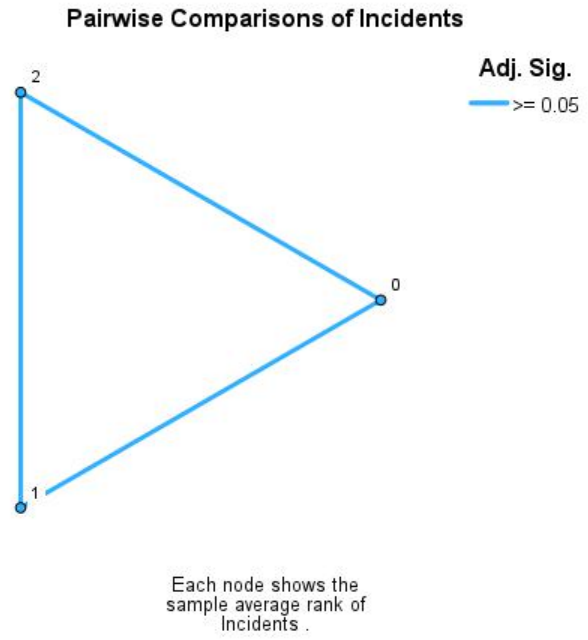


Fig 2: Pairwise Comparisons of Incidents

The above diagram shows the ranking of the three incidences as Cyber-attacks, natural Disasters, and Physical attacks on critical infrastructure. Each node shows the sample average rank of incidents, and the overall result showed a statistically significant > = 0.05.

Table 4: Energy and Utilities across Incidents

Independent-Samples Kruskal-Wallis Test Summary

Total N	3
Test Statistic	2.000[a]
Degree Of Freedom	2
Asymptotic Sig.(2-sided test)	.368

a. The test statistics are adjusted for ties.

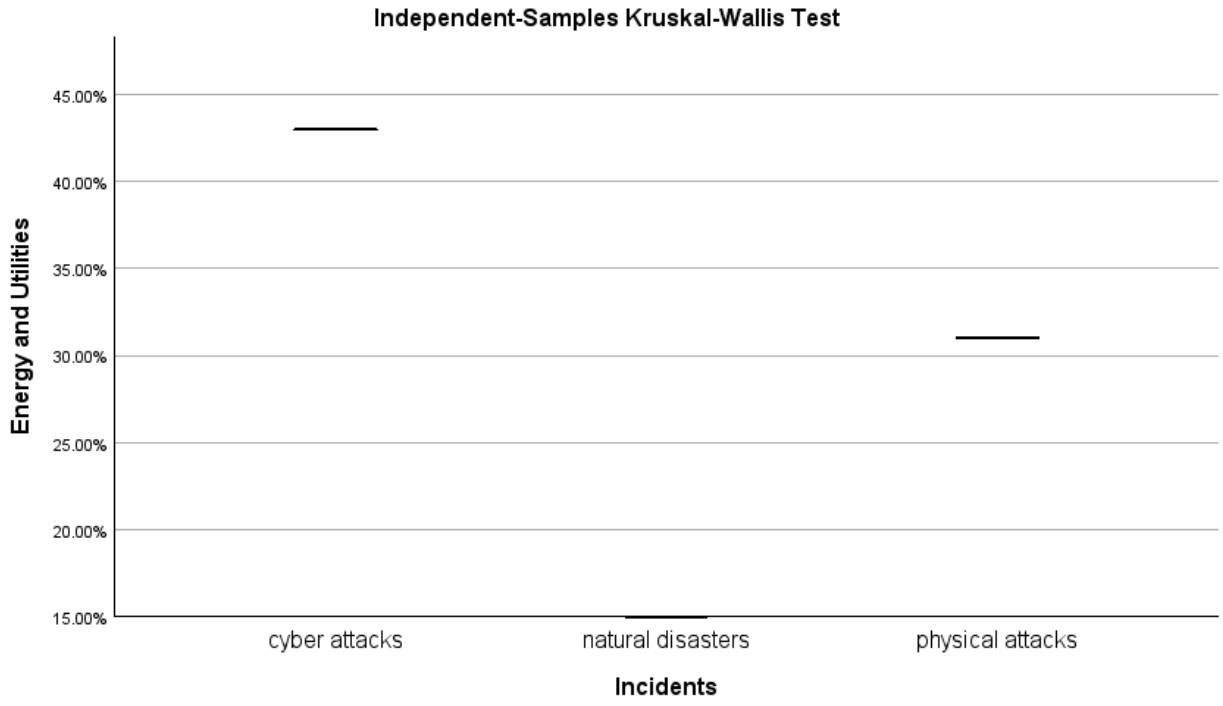


Fig 3: Energy and Utilities across incidents

Fig 3 was generated based on Table 4 data that represents the Energy and Utilities across incidence. The energy and utility were computed against Incidents that occurred within the infrastructure such as cyber-attacks, natural disasters, and Physical attacks. The result showed that Cyber-attacks incidents were ranked at above 40% when compared to natural disasters below 15%, and physical attacks at above 30%, respectively. The overall result showed a statistically significant of > = 0.05

Table 5: Pairwise Comparisons of Incidents

Pairwise Comparisons of Incident

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
natural disasters-physical attacks	-1.000	1.414	-.707	.480	1.000
natural disasters-cyber attacks	2.000	1.414	1.414	.157	.472
physical attacks-cyber attacks	1.000	1.414	.707	.480	1.000

In Table 5 above, each row tests the null hypothesis that the Sample 1 and Sample 2 distributions are the same. Asymptotic significances (2-sided tests) are displayed. The significance level is .050.

a. Significance values have been adjusted by the Bonferroni correction for multiple tests.

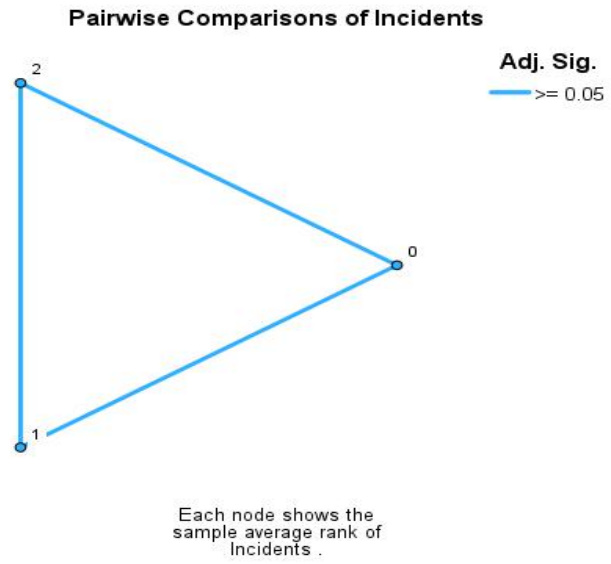


Fig 4: Pairwise Comparison of Incidents

The above diagram shows the ranking of the three incidences as Cyber-attacks, natural Disasters, and Physical attacks on critical infrastructure. Each node shows the sample average rank of incidents, and the overall result showed a statistically significant > = 0.05

Table 6: Transportation Systems across Incidents

Independent-Samples Kruskal-Wallis Test Summary

Total N	3
Test Statistic	2.000[a]
Degree Of Freedom	2
Asymptotic Sig.(2-sided test)	.368

a. The test statistic is adjusted for ties.

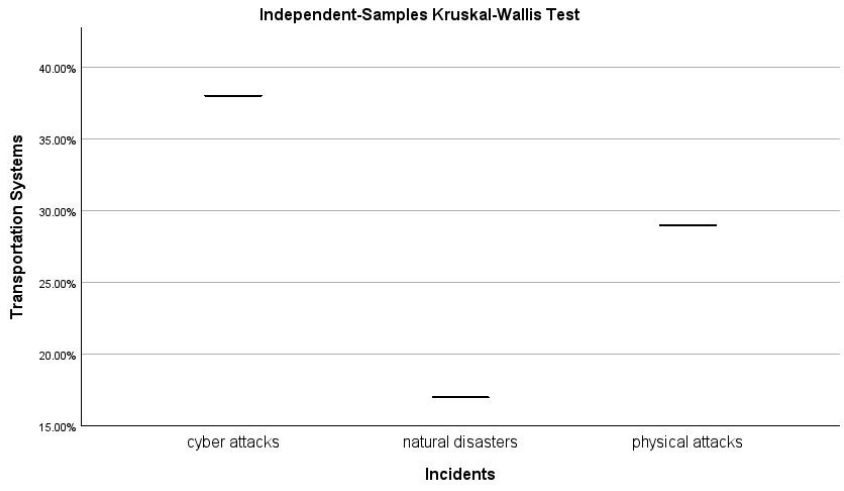


Fig 5: Independent Samples Kruskal-Wallis Test Transportation System.

Fig 5 above represents the output data from the Kruskal-Wallis Test. The data showed that cyberattack on transportation Infrastructure was above 35% compared to Physical attacks at above 25% and Natural disasters at above 15%, respectively.

Table 7: Pairwise Comparisons of Incidents

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
natural disasters-physical attacks	-1.000	1.414	-.707	.480	1.000
natural disasters-cyber attacks	2.000	1.414	1.414	.157	.472

physical attacks-cyber attacks	1.000	1.414	.707	.480	1.000

Each row tests the null hypothesis that the Sample 1 and Sample 2 distributions are the same.

Asymptotic significances (2-sided tests) are displayed. The significance level is .050.

a. Significance values have been adjusted by the Bonferroni correction for multiple tests.

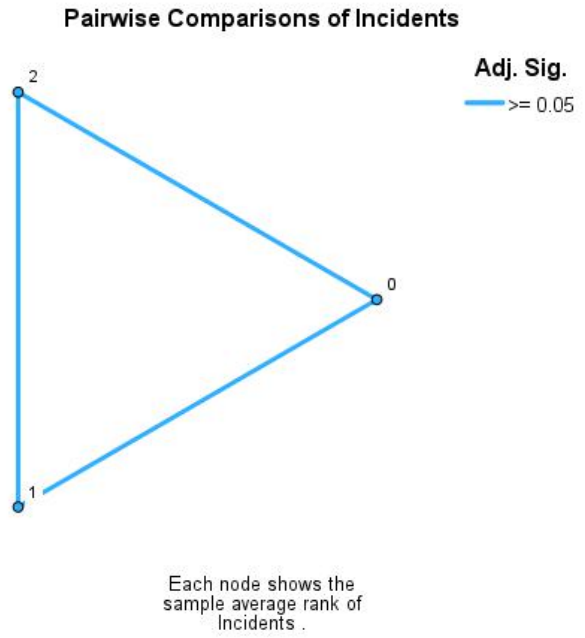


Fig 6: Pairwise Comparisons of Incidents Average Rank

The above diagram shows the ranking of the three incidences on Transportation systems as Cyber-attacks, natural Disasters, and Physical attacks on critical infrastructure. Each node shows the sample average rank of incidents, and the overall result showed a statistically significant > = 0.05

Table 8: Healthcare and Public Health across Incidents

Independent-Samples Kruskal-Wallis Test Summary

Total N	3
Test Statistic	2.000[a]
Degree Of Freedom	2

Asymptotic Sig.(2-sided test)	.368

a. The test statistic is adjusted for ties.

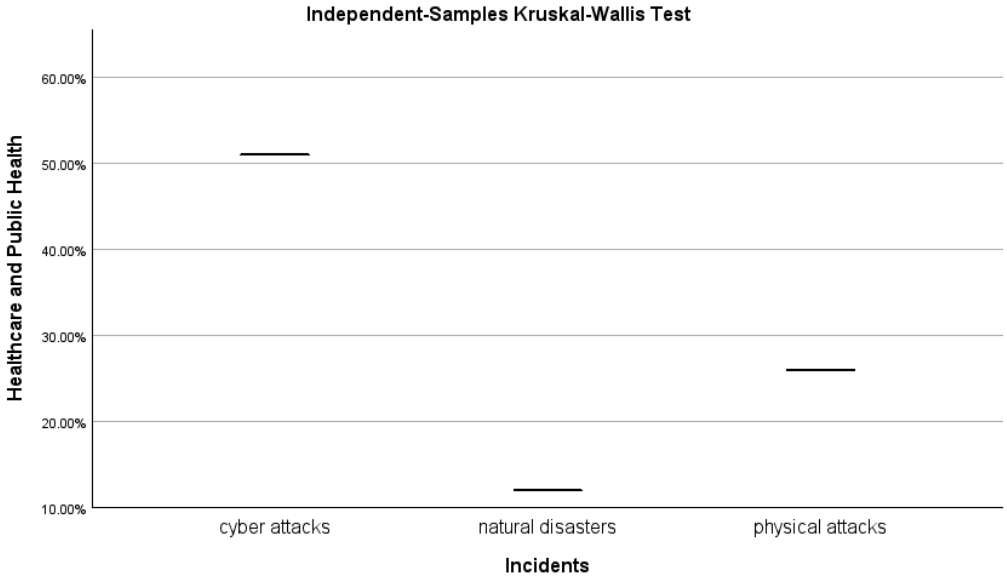


Fig 7: Independent Samples Kruskal-Wallis Test Healthcare

Fig 7 above represents the output data from the Kruskal-Wallis Test. The data showed that cyberattacks on the Healthcare Infrastructure across incidents were above 50% compared to Physical attacks at above 20% and Natural disasters at above 10%, respectively.

Table 9: Pairwise Comparisons of Incidents

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
natural disasters-physical attacks	-1.000	1.414	-.707	.480	1.000
natural disasters-cyber attacks	2.000	1.414	1.414	.157	.472
physical attacks-cyber attacks	1.000	1.414	.707	.480	1.000

Each row tests the null hypothesis that the Sample 1 and Sample 2 distributions are the same.

Asymptotic significances (2-sided tests) are displayed. The significance level is .050.

a. Significance values have been adjusted by the Bonferroni correction for multiple tests.

The below diagram shows the ranking of the three incidences of healthcare infrastructure across incidents such as cyber-attacks, natural disasters, and physical attacks on critical infrastructure. Each node shows the sample average rank of incidents, and the overall result showed a statistically significant > = 0.05

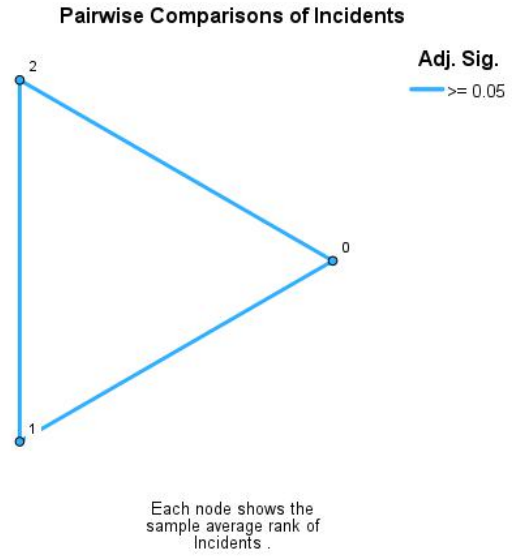


Fig 8: Pairwise Comparisons of Incidents Average rank of incidents

Table 10: Financial Services across Incidents

Independent-Samples Kruskal-Wallis Test Summary

Total N	3
Test Statistic	2.000[a]
Degree Of Freedom	2
Asymptotic Sig.(2-sided test)	.368

a. The test statistics are adjusted for ties.

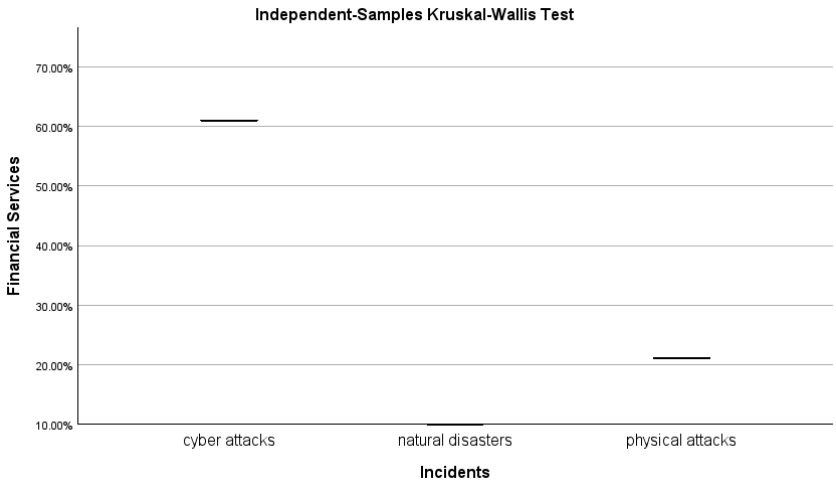


Fig 9: Independent-sample Kruskal-Wallis Test

Fig 9 above represents the output data from the Kruskal-Wallis Test. The data showed that cyberattack on Financial services Infrastructure was above 60% compared to Physical attacks at above 20% and Natural disasters at 10%, respectively.

Table 11: Pairwise Comparisons of Incidents

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
natural disasters-physical attacks	-1.000	1.414	-.707	.480	1.000
natural disasters-cyber attacks	2.000	1.414	1.414	.157	.472
physical attacks-cyber attacks	1.000	1.414	.707	.480	1.000

Each row tests the null hypothesis that the Sample 1 and Sample 2 distributions are the same.

Asymptotic significances (2-sided tests) are displayed. The significance level is .050.

a. Significance values have been adjusted by the Bonferroni correction for multiple tests.

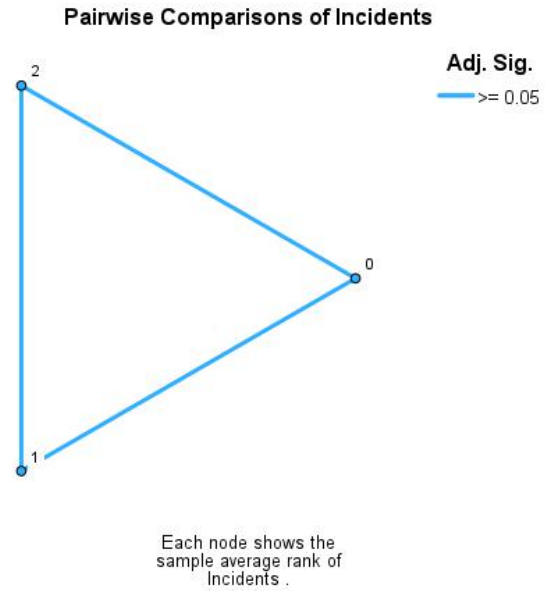


Fig 10: Pairwise Comparison of incidents Average rank of incidents.

Fig 10 shows the ranking of the three incidences on Financial Services infrastructure across incidents such as Cyber-attacks, natural Disasters, and Physical attacks on critical infrastructure. Each node shows the sample average rank of incidents, and the overall result showed a statistically significant > = 0.05

Table 12: Government Facilities Across Incidents

Independent-Samples Kruskal-Wallis Test Summary

Total N	3
Test Statistic	2.000[a]
Degree Of Freedom	2
Asymptotic Sig.(2-sided test)	.368

a. The test statistic is adjusted for ties.

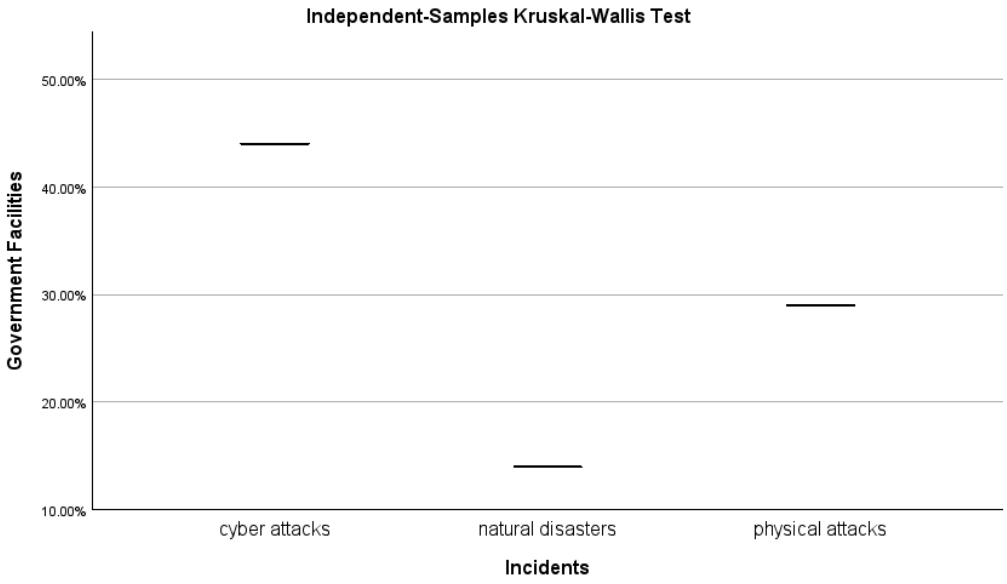


Fig 11: Independent sample Kruskal-Wallis Test Government facilities.

Fig 11 above represents the output data from the Kruskal-Wallis Test. The data showed that cyberattack on Government facilities Infrastructure was above 40% compared to Physical attacks at above 27% and Natural disasters at above 13%, respectively.

Pairwise Comparisons of Incidents

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
natural disasters-physical attacks	-1.000	1.414	-.707	.480	1.000
natural disasters-cyber attacks	2.000	1.414	1.414	.157	.472
physical attacks-cyber attacks	1.000	1.414	.707	.480	1.000

Each row tests the null hypothesis that the Sample 1 and Sample 2 distributions are the same.

Asymptotic significances (2-sided tests) are displayed. The significance level is .050.

a. Significance values have been adjusted by the Bonferroni correction for multiple tests.

Fig12 shows the ranking of the three incidences on Government facilities' infrastructure across incidents such as Cyber-attacks, natural Disasters, and Physical attacks on critical infrastructure. Each node shows the sample average rank of incidents, and the overall result showed a statistically significant > = 0.05

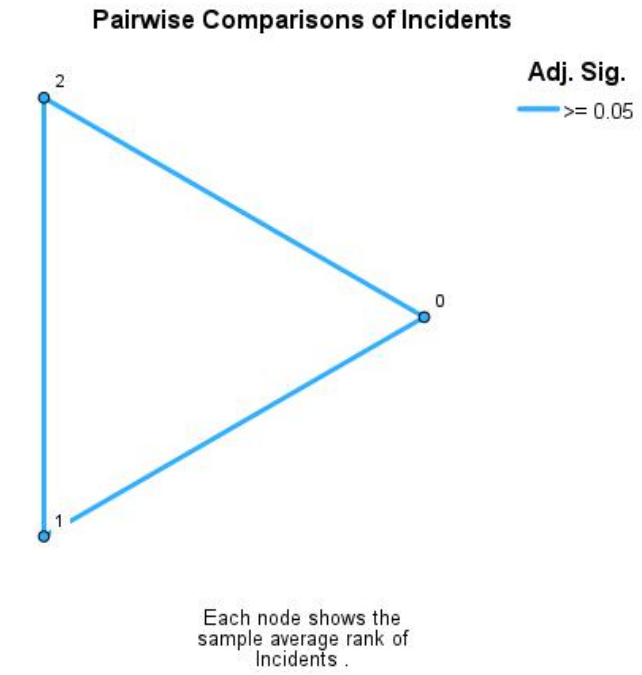


Fig 12: Pairwise Comparisons of incidents sample average ranking

Integrated Data Analysis

In this study, we looked at six critical areas of U.S. infrastructure. These were computed and compared against all incidences such as cyber-attacks, natural disasters, and Physical attacks. The result showed that Cyber-attacks incidents were significant at > = 0.05. The independent-sample Kruskal Wallis test was used to compare all incidences across all critical infrastructures. The result showed that the Null Hypothesis was retained based on the statistically significant result of >=0.05. When we compared the frequency of the Occurrence of water and waterways systems attacks, the result showed N=3, Min = 14.00%, Max = 52.00%, Mean =30.00%, and Standard deviation (std Dev) = 19.6977%. See Fig 13 below.

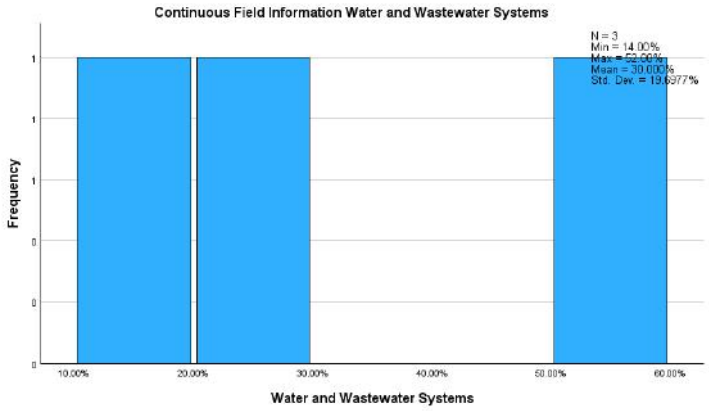


Fig 13: Continuous Field information water and Wastewater System.

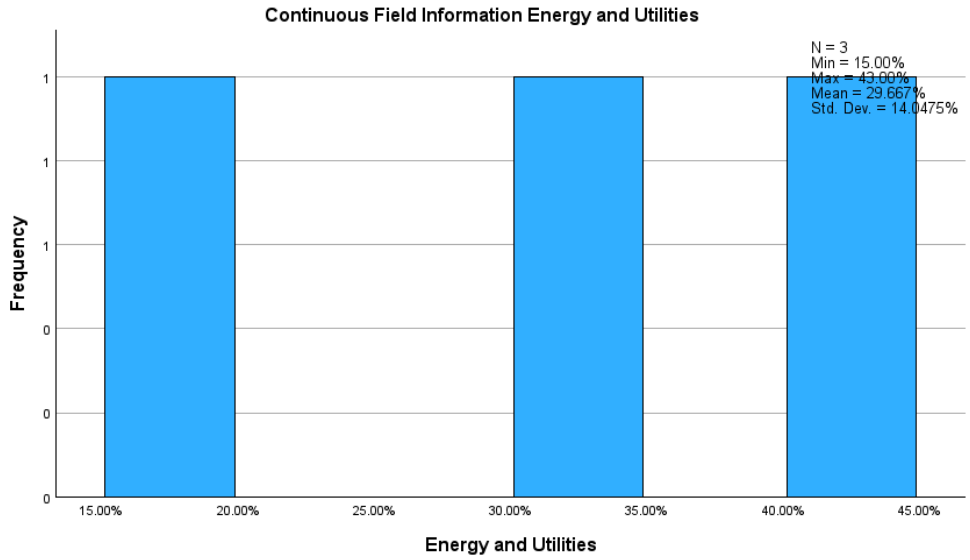


Fig 14. Continuous Field Information Energy and Utilities

Further, when we compared the frequency of the attack occurrence of the Energy and Utility infrastructure across infrastructure domains, the result showed N =3, Min =43.00%, Mean = 29.667%, std Dev = 14.0475%. See Fig 14 below.

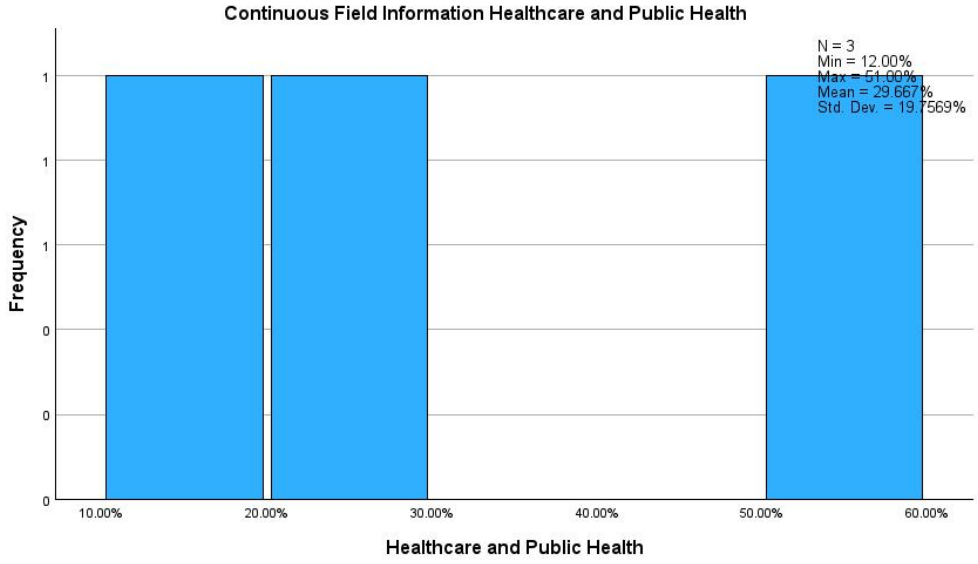


Fig 15: Continuous Field Information Healthcare and Public Health.

When comparing the frequency of attacks within Healthcare and Public Healthcare infrastructure across the three domains the result showed N= 3, Min =12.0%, Max = 51.00%, Mean = 29.667%, and Std Dev = 19.7569%. When you compare the standard deviation of healthcare infrastructure cyber-attacks to water and waterways attacks, they tend to have a commonality in how dispersed the data is in relation to the Mean as represented in Fig 15 below.

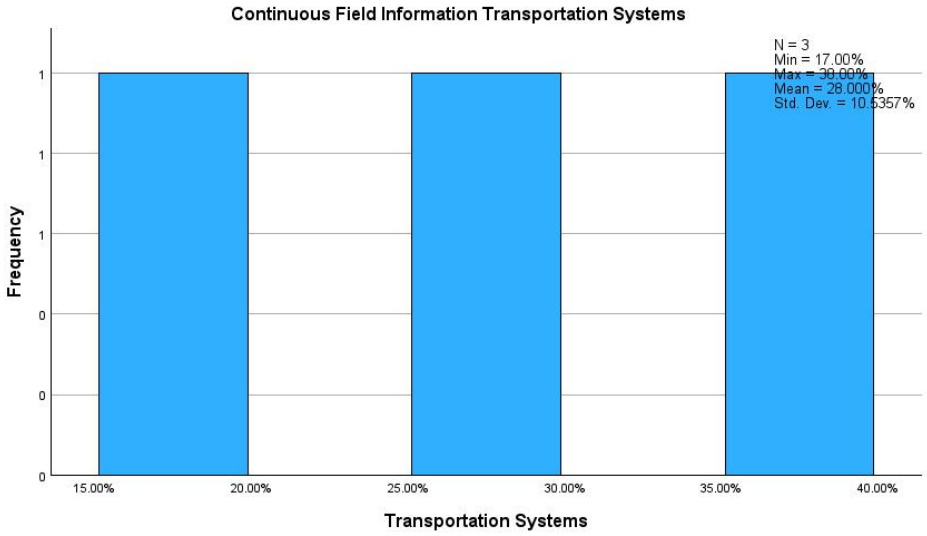
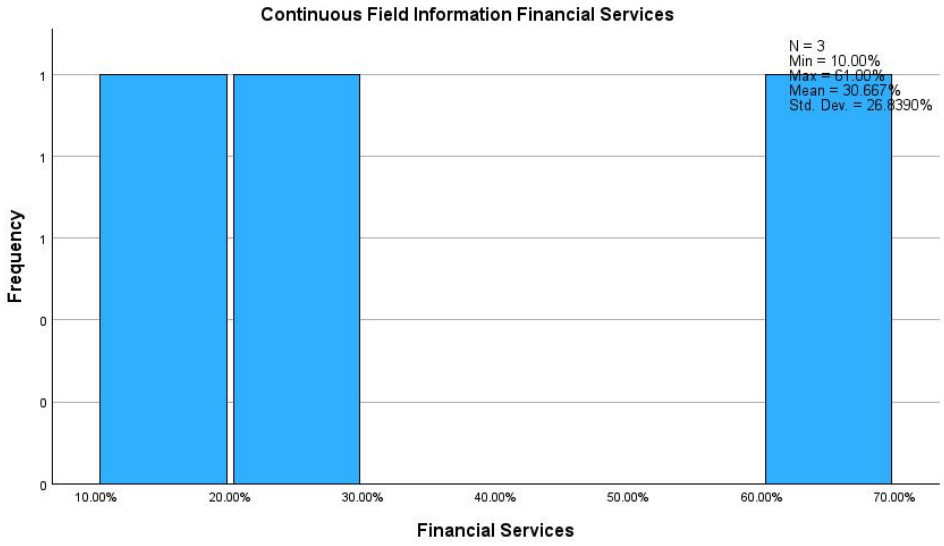


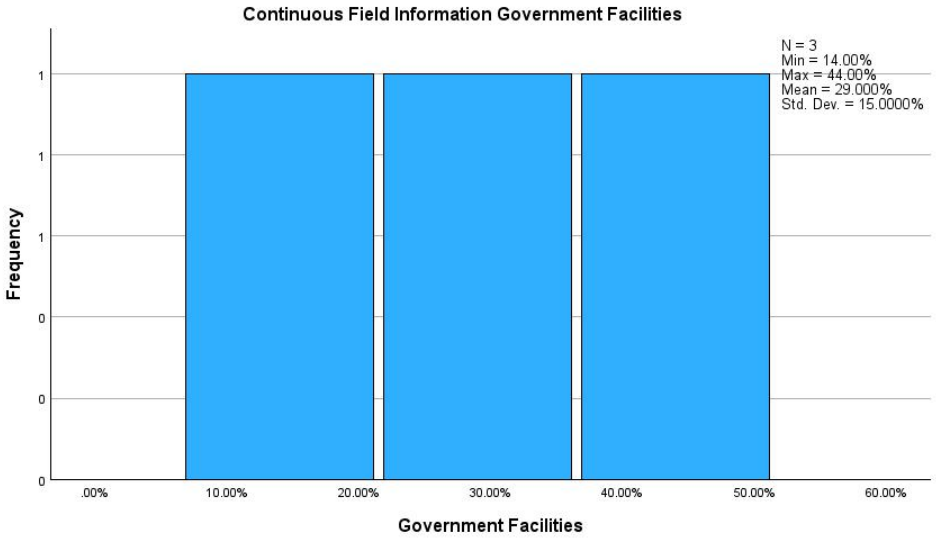
Fig 16: Continuous Field Information Transportation Systems

We compared the nature of Physical, cyber, and natural disasters with other attacks on critical infrastructure systems such as Transportation. The result showed N= 3, min = 17%, Max = 30.00%, Mean = 28%, std Dev = 10.5357%. See Fig 16 above.

This means that the average number of attacks on transportation systems deviated at approximately 10.5% at a minimal rate of 17%, compared to healthcare at a 12% standard deviation.



When we compared the frequency of diverse types of attacks such as Physical, cyber, and natural Disasters on Financial Services. The result showed N = 3, Min = 10.00%, Max =61.00%, Mean 30.667% and Std. Dev = 26.8390%, the data dispersed heavily to the mean. This means that there are a lot of variances in the observed data around the mean.



When we compared the frequency of distinct types of attacks such as Physical, cyber, and Natural disasters on Government facilities, the result showed N= 3, Min = 14%, Max = 44, Mean = 29.00%, and Std. Dev. = 15%.

Discussion

The digitalization of systems appears to have created vulnerabilities to the U.S. critical infrastructure. This study used a non-parametric test specifically the Kruskal-Willis test (pairwise comparison of incidents) to compare different samples of incidents on all critical Infrastructures presented in this study. We identified three types of attacks: Physical, Cyber, and natural disaster. We compared the vulnerabilities amongst these vital infrastructures based on the nature of the attack. The result showed that the incidence of cyber-attacks was higher than physical and natural disasters. Based on the literature reviewed for this study, "the area of concern was the Interconnection and supply chain risks on these Critical systems. A cyber-attack on one critical system could Impact multiple business functions within organizations that the system supports. According to the United States Government Accountability Office "GAO" (2024), "Critical infrastructure has been targeted on several occasions. A case in point is Ukraine's Power infrastructure, Indian Nuclear power station, and Israel's water infrastructure. As you can see in this study, cyber-attacks were higher on the incidence chart when compared to other forms of attack. Another aspect of concern is human error in critical infrastructure. As indicated in the literature reviewed:

Buenning (2024), "While technological advancements improve security measures, human error remains a threat in cybersecurity vulnerabilities. The relationship between human error to cybersecurity risks covers a range of unintended actions that compromise the integrity of digital systems. This guide explores the complex connection between human error and cybersecurity risks, providing light on unintentional actions that often serve as gateways for security breaches." (para2).

The NIST Risk framework adopted for this study was used to mitigate these risks. The NIST Risk framework states that vulnerable organizations should Prepare, categorize, select, implement, assess, and monitor these vulnerabilities.

Conclusion

Based on the data analyzed, the number of cyber-attack incidents on critical infrastructure was higher than that of other forms of attacks such as natural disasters and physical attacks. Therefore, more resources should be allocated to cyber-attack incidents than other attacks. The government should constantly train the employees on the risks of fishing attacks on critical infrastructure. The training will help to mitigate the risk of human error that could aid an attacker from infiltrating the critical infrastructure.

References

Allianz Commercial (2016), Cyber-attacks on critical infrastructure. Expert risk article. Retrieved from https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html. https://statescoop.com/new-york-775-million-cyberattacks-critical-infrastructure/

Butsianto, S., Nugraha, U., Anwar, M., Anwar, S., & Judijanto, L. (2024). Cybersecurity on the Internet of Things (IoT) Era: Safeguarding Connected Systems and Data. *Global International Journal of Innovative Research*, *1*(3), 290–297. https://doi.org/10.59613/global.v1i3.39

Buenning, M. (2024). How Human Error Relates to Cybersecurity Risks [IT Editorial Expert Blog]. Retrieved from https://www.ninjaone.com/blog/how-human-error-relates-to-cybersecurity-risks/#:~:text=In%20the%20digital%20age%2C%20the,contribute%20significantly%20to%20cybersecurity%20risks.

Colonial Pipeline Cybersecurity Incident, (2021). Cyber case study: Colonial Pipeline Ransomware Attack. Retrieved from https://insurica.com/blog/colonial-pipeline-ransomware-attack/

Leandros et al (2018). Cyber security of critical infrastructures, 4(1), pg. 42-45. https://doi.org/10.1016/j.icte.2018.02.001.

SolarWinds Cybersecurity Incident, (2020). SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response. Retrieved from https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

US Government Accountability Office "GAO" (2024). Cybersecurity for Critical Infrastructure. International Electrotechnical Commission [blog]. Retrieved from https://www.iec.ch/blog/cyber-security-critical-infrastructure-0

Verizon DBIR, (2021). Data Breach Investigations Report. Retrieved from https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report

Zero Trust Solutions, (2023). Cybersecurity Theory Review. Retrieved from https://www.linkedin.com/pulse/cybersecurity-theory-review-zerotrustsolutions#:~:text=Evolutionary%20Theory%3A%20This%20theory%20argues,to%20the%20evolving%20threat%20landscape.