International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 05 May 2025, pp: 222-230 www.ijaem.net ISSN: 2395-5252

The Economic Impact of Cybersecurity Threats on Critical Infrastructure: Evaluating U.S. Policy Effectiveness and Private Sector Readiness

Md Nazmul Hossain Palash
Asian University of Bangladesh Dhaka • Bachelor of Science: Computer Science & Engineering

Date of Submission: 05-05-2025 Date of Acceptance: 15-05-2025

ABSTRACT
National security and economic stability risks associated with the cyber attack on critical infrastructure have increased. This paper suggests the economic impact of cyber incidents in selected U.S. sectors be assessed, the efficacy of the current federal cyber policies be evaluated, and the private sector's readiness is assessed. It does so through the use of government data, industry reports, and case studies to identify gaps that exist in coordination, workforce preparedness, and compliance in cybersecurity. The paper ends with policy recommendations and strategies for enhancing national resilience through a more comprehensive public – private engagement.

Keywords: Cybersecurity; Critical Infrastructure; Economic Disruption; United States Policy; Private Sector Preparedness; Cyber Threats; NIST Framework; CISA; National Cyber Strategy; Public-Private Collaboration

I. INTRODUCTION

For example, an attack based on ransomware on Colonial Pipeline in 2021 resulted in fuel shortages across the U.S. East Coast, and almost 45% of the region's fuel supply was temporarily shut (CISA, 2021). Critical infrastructure as to which in the United States is determined by the Department of Homeland Security (DHS, 2022) and refers to the systems and assets, physical and virtual, so vital to the continued functioning of national critical functions that their incapacitation or destruction would have a debilitating impact on security, economy, public health or safety, or any combination thereof. These infrastructures underpin the U.S. economy, and when infiltrated by cyberattacks, can cascade beyond their original borders and sectors.

The fragility of these systems have been underscored by high-profile cyber incidents. Colonial Pipeline is an example from 2021, when the company faced an attack by ransomware which shut down roughly 45 percent of the area's fuel supply and caused fuel shortages on the U.S East Coast (CISA, 2021). During the COVID-19 pandemic, ransomware attacks shut down multiple healthcare networks, and as such the leaked sensitive patient data, and delayed treatment (Check Point Research, 2021). According to (CSIS & McAfee, 2020, Cybercrimes are reputed to cost the world economy more than $1 trillion a year and are hardest felt in the United States given its extensive digital infrastructure and weight of its economy.

Consequently, the U.S. government has enacted a number of policy frameworks to safeguard the country's digital infrastructure. These include the NIST Cybersecurity Framework, the Cybersecurity and Infrastructure Security Agency's (CISA) directives, and Executive Orders aimed at enhancing cyber defense and incident response capabilities (NIST, 2018; The White House, 2021). However, despite these efforts, significant gaps remain in policy enforcement, inter-agency coordination, and especially private sector adoption, which is often hindered by resource constraints, varying industry standards, and a shortage of cybersecurity professionals (GAO, 2022; Ponemon Institute, 2023).

This paper examines the economic effect of cybersecurity threats against critical infrastructure in the USA, analyzes the effectiveness of the current federal cybersecurity policies, and explores the preparedness of the private sector for the confrontation of such challenges. According to the study, case studies, policy analysis, and sector- based economic data,

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 05 May 2025, pp: 222-230 www.ijaem.net ISSN: 2395-5252

however, better public- private collaboration is needed to build the nation's cyber resilience.

II. LITERATURE REVIEW

2.1 Cybersecurity and Critical Infrastructure

A nation's critical infrastructure is defined as systems and assets whether physical or virtual, that are essential for the maintenance of a society's vital economic, public health, public safety, or national security services. DHS (2022) points out 16 sectors of critical infrastructure; the energy sector, the health sector, the financial sector, and the communications sector, among others. The merging of operational technology (OT) and information technology (IT) has made these systems more efficient, but also it has made these systems more vulnerable to cyberattacks. Studies have shown that nation-state and criminal cyber actors increasingly target these sectors to exploit system weaknesses or extract ransom payments (Kshetri, 2017; Sanger, 2018).

2.2 Economic Impact of Cyberattacks

In response, many frameworks and strategies have been adopted by the U.S. government to address these risks. According to IBM Security (2023), the U.S. had the highest average cost of a data breach at $9.48 million in 2023. According to an estimate of CSIS and McAfee (2020), losses caused by cybercrime exceed $1 trillion annually, with a large part concentrated in advanced economies, including the USA. In addition, such attacks on critical infrastructure have localised or national effect on ripple effects, meaning the economic burden spills to the rest of the affected entity (Floridi, 2019).

There are several empirical studies including Anderson et al. The second wave of studies (2019) take into account indirect costs such as market reactions, erosion of consumer trust, and long term losses in productivity. Several frameworks and strategies have been launched by U.S. government to address these risks.

2.3 U.S. Cybersecurity Policy Frameworks

These risks are addressed by several frameworks and strategies of the U.S. government. NIST cybersecurity framework (NIST, 2018) is the voluntary guidelines for organizations to manage their cybersecurity risks. Adoption is inconsistent across sectors, but is widely respected. For solidifying actions of executive governance for greater cybersecurity and secure software supply chain in 2021, one may mention executive order 14028 (The White House, 2021).

With Executive Order 14028 in 2021, the moment abided by The White House (2021) to repeal software supplies chain defense, and strengthen cyber governance was a watershed moment. Yet, many policies are aspirational, say experts, without regulatory teeth (Lewis, 2022).

2.4 Private Sector Readiness

Policy gains, however, have been patchy in terms of private sector readiness. Ponemon Institute says many companies — especially small and medium sized enterprises (SMEs) — are lacking in the financial and technical capability to roll out full cybersecurity programs. Additionally, the U.S. continues to face a cybersecurity workforce shortage of over 500,000 professionals, creating further barriers to effective implementation (ISC², 2023).

Research by Yeo et al. (2021) paints a picture of many firms who are mismatched in executive awareness vs. operational capacity. The need for cybersecurity continuously grows as a board issue, but execution happens too slowly because it is typically fragmented within the organization or underfunded.

III. METHODOLOGY

3.1 Research Design

This study is a qualitative descriptive study using a case study analysis, policy evaluation and thematic content analysis of public and private sector cybersecurity data. This thesis attempts to understand how cyber attacks on critical infrastructure are harmful to the U.S. economy and which government and private stakeholders are ready to confront and mitigate these threats.

3.2 Data Sources

Data is collected from a combination of primary and secondary sources, including:

A reading of government documents and reports from the U.S. Government Accountability Office (GAO), the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST).

Academic journals and books on topics related to cybersecurity economics, policy and governance.

- Moreover, white papers and surveys by industry (e.g., the Ponemon Institute, IBM Security, (ISC)²) offer insight into perceived amounts and types of cybersecurity incidents as well as ideas for solving them.
- Cyber incident databases and compendia of attacks on major infrastructure (e.g., Colonial

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 05 May 2025, pp: 222-230 www.ijaem.net ISSN: 2395-5252

Pipeline, SolarWinds, healthcare ransomware attacks).

3.3 Case Selection Criteria

Case studies are selected based on the following criteria:

- U.S. critical infrastructure sectors (e.g., energy, healthcare, financial services) relevance.
- Economic disruption has its significance or National Security impact.
- The existence of reliable data on the part of government or industry sources.

3.4 Analytical Framework

The study uses a triangular analytical framework combining:

- Economic Impact Analysis: They estimate financial losses, costs of recovery and productivity effects based on cost estimates found in published sources.
- Policy Effectiveness Evaluation: Measuring how federal cybersecurity frameworks (e.g., NIST, CISA initiatives) are implemented and perform.
- Private Sector Readiness Assessment: Evaluating the impact of adoption of security practices; levels of investment, and workforce capabilities.

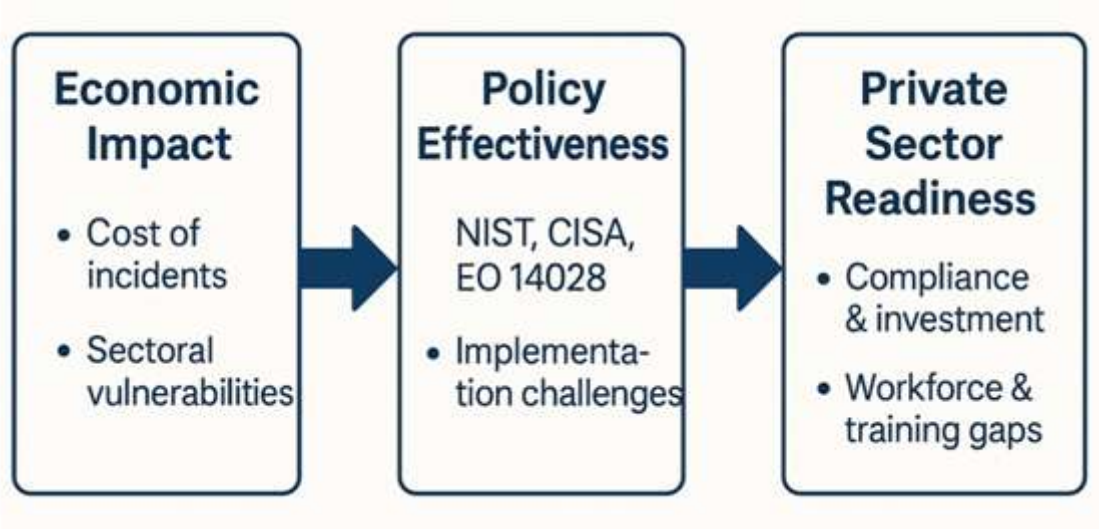

Fig 1: Research Framework

3.5 Limitations

- It is constrained to publicly accessible data, thereby underreporting or perhaps mischaracterizing the totality of cyber incidents.
- In turn, case studies may not fully generalize to the broader population due to industry specific factors.
- Economic estimates are based on secondary sources and use valuation methods that may vary.

IV. CASE STUDIES AND ECONOMIC IMPACT ANALYSIS

4.1 Case Study 1: Colonial Pipeline Ransomware Attack (2021)

In May 2021, Colonial Pipeline, one of the largest fuel pipeline operators in the U.S., was targeted by a ransomware attack. The attack led to the temporary shutdown 4. Case Studies and Economic Impact Assessment

4.1 Case Study 1: Colonial Pipeline Ransomware Attack (2021)

Later, in May 2021, Colonial Pipeline, one of the biggest fuel pipeline operators in the United States, was hit by a ransomware attack. The attack resulted in Colonial Pipeline closing its systems which negatively influenced the fuel supply to 45% of the east coast residents for a brief period. A Russia-based criminal syndicate known as DarkSide ransomware group launched the cyberattack. The disruption had devastating economy effects:

Economic Impact:

- Direct Costs: Colonial Pipeline paid out $4.4 million to resume operations. (U. S. Department of Justice, 2021).
- Indirect Costs: It also led in widespread disruptions in transportation with. The overall economic impact also brought supply chain

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 05 May 2025, pp: 222-230 www.ijaem.net ISSN: 2395-5252

disruptions and logistical expenses from fuel shortages.
- Reputational Damage: It exposed vulnerabilities in the critical infrastructure, hurt to consumers – long-term trust, scrutiny from the federal regulatory zone (CSIS, 2021).

4.2 Case Study 2: SolarWinds Cyberattack (2020)

In 2020, by way of example, SolarWinds, a well-known IT management softwareorganization, was the victim of simply just one of the foremost significant supplychain cyberattacks in history. The Russian-backed hacking group APT29 (Cozy Bear) completed its attack on SolarWinds' Orion software against over 18000 customers with Fortune 500 companies and government departments among those affected.

Economic Impact:
- Direct Costs: The financial losses suffered by SolarWinds in the attack were estimated to be $20 million in terms of incident response, customer compensation, and legal liabilities (SolarWinds, 2021).
- Indirect Costs: The overall impact on affected orgs was data breaches, IP theft and potential Spearfishing activities. Financial services, defense, and healthcare sectors were added regulated place on the compliance expense and scrutiny list (Ponemon Institute, 2021).
- National Security Risks: Beyond the immediate money, the breach laid bare weaknesses in U.S. national cyber defense, prompting more federal spending in cyber defense (CISA, 2021).
- of its systems, affecting nearly 45% of the East Coast's fuel supply. The cyberattack was attributed to the DarkSide ransomware group, a criminal syndicate operating from Russia. The disruption had profound economic consequences:

Economic Impact:
- Direct Costs: Colonial Pipeline paid a $4.4 million ransom to restore operations (U.S. Department of Justice, 2021).
- Indirect Costs: The fuel shortages led to widespread disruptions in transportation, with prices for gasoline and diesel rising by 5-10% in several states. The broader economic impact included supply chain delays and logistical costs due to fuel shortages.
- Reputational Damage: The attack highlighted vulnerabilities in critical infrastructure, leading to long-term consumer trust issues and scrutiny from federal regulators (CSIS, 2021).

4.2 Case Study 2: SolarWinds Cyberattack (2020)

In 2020, SolarWinds, a major IT management software company, became the target of one of the most significant supply chain cyberattacks in history. The attack, attributed to Russian state-sponsored group APT29 (Cozy Bear), compromised SolarWinds' Orion software, affecting more than 18,000 customers, including U.S. government agencies, Fortune 500 companies, and critical infrastructure providers.

Economic Impact:
- Direct Costs: The attack's financial impact on SolarWinds alone was estimated at $20 million in terms of incident response, customer compensation, and legal liabilities (SolarWinds, 2021).
- Indirect Costs: The broader impact on affected organizations included data breaches, intellectual property theft, and potential espionage activities. Financial services, defense, and healthcare sectors faced additional regulatory scrutiny and compliance costs (Ponemon Institute, 2021).
- National Security Risks: Beyond the immediate financial impact, the breach exposed vulnerabilities in U.S. cybersecurity defense systems, leading to increased federal investment in national cyber defense (CISA, 2021).

4.3 Case Study 3: Healthcare Ransomware Attacks (2020-2021)

The COVID – 19 pandemic resulted in an influx of ransomware attacks targeting healthcare organizations where several hospitals and healthcare systems were forced to shut down critical systems. One such case was the case of 2020, when Universal Health Services (UHS) system was targeted.

Economic Impact:
- Direct Costs: The attack caused UHS to report $67 million in lost revenue for 'system downtime' and 'reconstruction of infrastructure of IT,' (UHS, 2020).
- Indirect Costs: According to the attack reports, patients experienced large delays in receiving care from the healthcare provider, which was immobilized by the attack with crippled systems that crashed medical records, could

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 05 May 2025, pp: 222-230 www.ijaem.net ISSN: 2395-5252

not schedule appointments or receive test results.

- Reputational and Long-Term Effects: Among the numerous incidents that revealed the vulnerabilities of the healthcare sector, UHS' ransomware attack, among others, propelled increased investments into the cybersecurity and regulatory oversight of the sector (Check Point Research, 2021).

4.4 Economic Impact Synthesis

The following table presents a summary of substantial economic impacts cybersecurity attacks create on United States critical infrastructure systems:

Table 1: Economic Impact of Notable Cyberattacks on U.S. Critical Infrastructure

Incident	Direct Costs	Indirect Costs	Sector Impacted
Colonial Pipeline (2021)	$4.4 million ransom paid	Fuel shortages, price increases, supply chain disruptions	Energy/Transportation
SolarWinds (2020)	$20 million (SolarWinds response)	Data breaches, espionage, compliance costs	IT/Technology, Government
Universal Health Services (2020)	$67 million in lost revenue	Delayed patient care, medical record disruptions	Healthcare

4.5 Analysis of Economic Consequences

Likewise, a cyber attack on critical infrastructure could result in a direct and a long term financial impact. The sooner the cost of the direct cost of the downtime can be quantified, the less the indirect costs—the operational downtime and the reputational damage, for example—can be. An example of such an attack is Colonial Pipeline attack that resulted in the loss of revenues to the wide network but also disrupted the national fuel supply chains and caused the regional economic disruptions. On the other, hand, the cost of the SolarWinds attack was also inflated when the after effect of the government and private sector confidence in cybersecurity systems disorientated confidence at national policy and operational level, too.

Also, this demonstrates that there is a large gap that must be filled in terms of cybersecurity resilience. However, there is clearly a need to close the gap between what the public (CISA, DHS, etc.) sector can do to secure infrastructure. rather than what responsibility the private sector has to secure infrastructure on which it has insufficient regulatory incentives to invest in cybersecurity. These are attacks that we've seen over and over again, and we need to be looking at stricter regulations, better public- private cooperation, and more support of cybersecurity work force.

V. POLICY EFFECTIVENESS EVALUATION

5.1 Overview of U.S. Cybersecurity Policies

To deal with the growing threats against critical infrastructure, the U.S. government has employed a number of key policy and frameworks. They include the Cybersecurity Framework promulgated by the National Institute of Standards and Technology (NIST), the initiatives with Cybersecurity and Infrastructure Security Agency (CISA), and Executive Order 14028, issued around improving the nation's cybersecurity (The White House, 2021).

NIST Cybersecurity Framework (2018)

In order to assist the private sector organizations in managing their cybersecurity risk, the NIST Cybersecurity Framework was created to guide them. Five key functions are stressed in the framework: At the heart of cybersecurity, there are the five words, Identify, Protect, Detect, Respond, Recover. The standard is very highly regarded for its expansive, adaptive application, and has recently been fast adopted by many of the industries in critical infrastructure.

Strengths:

- Provides a risk-based scalable approach for the industry.
- Possible common language for public–private sector collaboration.
- Allows organizations to prioritize cybersecurity spend on resources that steps in importance (NIST, 2018).

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 05 May 2025, pp: 222-230 www.ijaem.net ISSN: 2395-5252

Weaknesses:

- The framework is voluntary, so it does not help ensure that all sectors carry out the framework as comprehensive as it is (GAO, 2022).
- A few sectors, for example, healthcare and transportation, have had trouble making in full an adoption of the National Institute of Standards and Technology (NIST) controls directives because of resource issues and compliance issues as indicated by the Ponemon Institute (2023).

The Cybersecurity and Infrastructure Security Agency (CISA) Initiatives

CISA is the operating arm of the U.S. Department of Homeland Security for cybersecurity and works with the private sector and federal agencies to coordinate its efforts. C3 consists of the Critical Infrastructure Cyber Community (C3) Voluntary Program, the National Risk Management Center, and Cybersecurity Incident Response Teams (CIRT).

Strengths:

- Provides real-time information sharing between the public and private sector entities.
- Offers resources to improve threat detection, vulnerability management, and threat response(CISA 2021).
- Implements collaboration in programs such as the CISA Shields Up program which offers tools and resources for companies to address elevated cyber threats.

Weaknesses:

However, private sector participation has been inconsistent, with many private companies not integrating all of CISA's resources, and has not incorporated the guidance provided by CISA (GAO, 2022).

On the other side, information sharing among the federal agencies and private companies is retarded by fears of leaking information and then regulatory compliance (Ponemon Institute, 2020).

The NIST Framework consists of five continuous functions (Identify, Protect, Detect, Respond, and Recover) as illustrated in the Diagram 1.

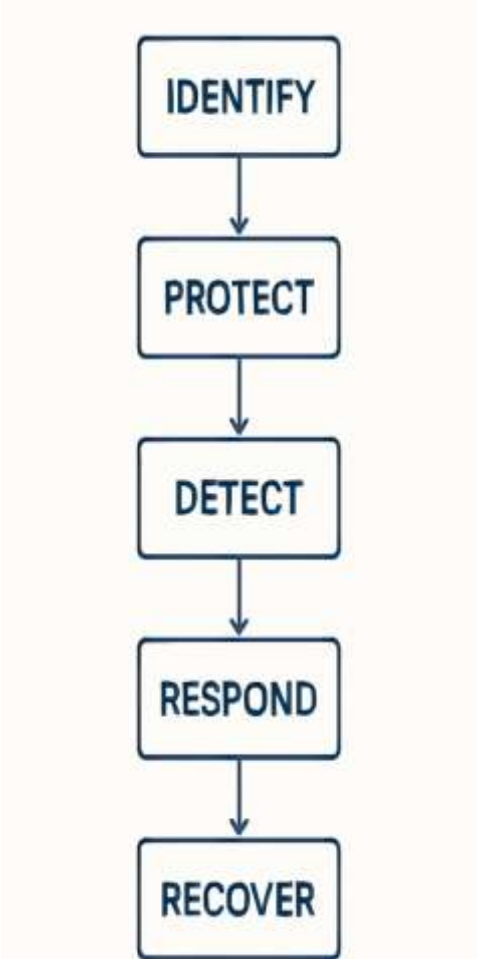

Fig 2:NIST Cybersecurity Framework

5.2 Executive Order 14028: Improving Cybersecurity

In response to increasing high-profile cyberattacks The U.S. Government implemented Executive Order 14028 during May 2021. The executive order compels many federal agencies to build better cybersecurity systems while demanding better software supply chain protection and public-private partnership enhancement.

Strengths:

- The order requires federal agencies to use zero trust models while also requiring them to replace their outmoded IT infrastructure.

* Has provisions for better cybersecurity standards for software vendors to which will minimize vulnerabilities caused by third party applications (The White House, 2021).

- Through this initiative the U.S. government increases CISA's power to serve as primary coordinator of cybersecurity activities across the nation.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 05 May 2025, pp: 222-230 www.ijaem.net ISSN: 2395-5252

Weaknesses:

The implementation process moved slowly and different industries face challenges while ensuring compliance with regulations.
Private organizations have taken part voluntarily yet the order reaches very few companies (Lewis, 2022).

5.3 Challenges in Policy Implementation

Numerous obstacles have restricted the successful execution of federal policies and frameworks despite their intended effectiveness.

1. Voluntary Participation: Multiple self-initiated programs from the private sector operate under NIST and CISA's guidelines. Appropriate cybersecurity measures to be taken are most likely just on the part of private companies if there are mandatory cybersecurity standards, and there are penalties for not complying (Lewis, 2022).
2. Resource Constraints: Small and medium-sized enterprises (SMEs) face difficulties in developing secure programs because they don't have the proper funds or cyber expertise. Many sectors including healthcare and education demonstrate significant cybersecurity gaps according to Ponemon Institute's 2023 research.
3. Lack of Information Sharing: Despite facilitating the flow of information between the public and private sectors, CISA, data confidentiality, legal boundaries as well as competitive issues have continued to prevent the unencumbered sharing of critical threat intelligence (GAO, 2022).
4. Cybersecurity Workforce Shortage: A recent study by (ISC²) reveals that the failure to find enough cybersecurity professionals reaches 500,000 unfilled positions this year in the United States. The shortage makes it more difficult to implement effective cybersecurity practices since industries require specialists in their fields.

Diagram 2 confirms the continuous legal and organizational obstacles which slow down the effective transmission of public–private threat intelligence.

Fig 3: Public-Private Collaboration Challenges

5.4 Policy Effectiveness Assessment

An analysis of U.S. cybersecurity policies ultimately demonstrates that there are several very strong aspects regarding development of a framework, government cohesion, and support for sector engagement. The private sector fails to adopt cybersecurity measures at widespread levels despite the existing policy weaknesses. The combination of voluntary policies and insufficient funding for implementation with insufficient cybersecurity professionals greatly diminishes the success rate of these policy frameworks.

The fact that Executive Order 14028 is progress from a step forward on specifically requiring federal agencies to modernize their cybersecurity practices, it still fails to impose such regulations on the private sector actors and does not have any immediate impact.

VI. RECOMMENDATIONS AND CONCLUSION

6.1 Summary of Key Findings

Also, this research looked into the economic impact of cybersecurity threats to U.S. critical infrastructure and their review of the current government method of protecting U.S. critical infrastructure. Several key findings in this research are:

1. Economic Consequences of Cyberattacks: Economic impact of cyberattacks on critical

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 05 May 2025, pp: 222-230 www.ijaem.net ISSN: 2395-5252

infrastructures, direct and indirect, such as Colonial Pipeline, SolarWinds, and healthcare organization's. There's the cost of the ransom, cost of downtime, and market disruption, and your cost of reputational damage.

2. Policy Strengths and Limitations: Due to the voluntary nature, and inconsistent implementation, among various sectors U.S. cybersecurity policies such as NIST Cybersecurity Framework, CISA initiatives and Executive Order 14028, their effectiveness is somewhat limited.
3. Private Sector Readiness: Indeed, the effort taken to enhance cybersecurity amongst the private sector has not had the desired impact amongst many private sector organization, especially small and medium enterprises (SMEs) that lacked the ability to implement strong cybersecurity standards due to resource constrains.
4. Cybersecurity Workforce Shortage: The public and private sector really haven't made the progress they need to make when it comes to cybersecurity preparedness, and it's still a deep shortage of qualified cybersecurity professionals to be a roadblock to that.

6.2 Recommendations

Recommendations for strengthening the U.S. cybersecurity posture for critical infrastructure, based on the analysis are proposed as follows.

1. Establish mandatory cybersecurity standards for the Critical Infrastructure Sectors.

Although employing a framework, such as NIST, offers useful guidance, it provides voluntary information and smaller entities tend to neglect them. Bans on telecom equipment from firms such as Huawei would help remove loopholes for potentially cyberespionage firms that exist out of concern for being cut off from the major Western suppliers they need for their own customers. Such standards should be sectoral and consider the unique risks of each sector (e.g. energy. health care, finance).

2. Enhance Public-Private Sector Collaboration

Sharing information continues to be a main challenge in cybersecurity. Asking private sector companies to work with government agencies like CISA would help to improve exchanges in threat intelligence and responding to incidents. Overcoming these concerns would require a more formal, legally protected information sharing framework that would alleviate the concerns about confidentiality and the loss of competitive advantage, and inspire more pro active collaboration.

3. Invest in Cybersecurity Workforce Development

The gap of cybersecurity professionals is so severe that it is halting the security of critical infrastructure. Government and private sectors should invest in workforce development initiatives to train and recruit the skilled cybersecurity workforce. To widen the talent pool, programs should focus on the promotion of diversity and inclusion in the cybersecurity workforce to mitigate the gap in the skills available.

4. To Strengthen Healthcare Cybersecurity Resilience and in Other Vulnerable Sectors

While the healthcare sector is generally reliant on legacy systems and sensitive data, it remains especially vulnerable to cyberattacks. Reducing the exposure of cybersecurity for healthcare providers, especially SMEs, as well as other vulnerable sectors (education, transportation) necessitates investments that are targeted to those areas. Oversight by regulatory bodies should also be increased to assure minimum security standards are in place.

5. Goals 3, 4: Foster Public Awareness and Executive Accountability

At the highest levels, cybersecurity should not be considered a business ask, it should be seen as a business imperative. There must be accountability of corporate boards and C-suite executives for cybersecurity decisions and investments. The publicity [1] of the financial or reputational risks (described later in the report) from cyberattacks stored might encourage private businesses to dedicate sources towards better cybersecurity positioning.

6.3 Conclusion

There is a significant risk of economic consequences as well as cybersecurity threats to critical infrastructure in the U.S. While there have been policy framework as well as federal initiatives, the inherent vulnerabilities in public and private sector preparedness remain unresolved. Steps required to cut back the economic impact of cyberattacks contain strengthening cybersecurity policies, increasing coordination among various sectors, and fixing the cybersecurity workforce shortage.

The government must make sure that government policy and regulation evolve to reflect threats becoming evermore sophisticated cyber adversaries engage in increasingly, and businesses have more responsibility for defending critical infrastructure. Through nurturing a culture of resilience, innovation, and cooperation, and in response to limitations facing the U.S. government and organizations, the U.S. can enhance the protection of critical infrastructure from cybercrime economic and national security threat.

REFERENCES

[1]. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., ... & Savage, S. (2019). Measuring the cost of cybercrime. Journal of Cybersecurity, 2(2), 121–135.
[2]. CISA. (2021). Shields Up: CISA's Response to Cyber Threats. Retrieved from https://www.cisa.gov/shields-up
[3]. GAO. (2022). Cybersecurity: Federal Efforts Need to Address Shortcomings in Critical Infrastructure Protection. Retrieved from https://www.gao.gov
[4]. IBM Security. (2023). Cost of a Data Breach Report. Retrieved from https://www.ibm.com/security/data-breach
[5]. ISC². (2023). Cybersecurity Workforce Study. Retrieved from https://www.isc2.org
[6]. Lewis, J. A. (2022). Rethinking Cybersecurity Regulation in the U.S. Center for Strategic and International Studies. Retrieved from https://www.csis.org
[7]. NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). National Institute of Standards and Technology. Retrieved from https://www.nist.gov/cyberframework
[8]. Ponemon Institute. (2023). Cybersecurity in the C-Suite and Boardroom. Retrieved from https://www.ponemon.org
[9]. The White House. (2021). Executive Order on Improving the Nation's Cybersecurity. Retrieved from https://www.whitehouse.gov
[10]. U.S. Department of Justice. (2021). Colonial Pipeline Cyberattack: A Case Study. Retrieved from https://www.justice.gov
[11]. UHS. (2020). Universal Health Services: Cyberattack Impact and Recovery. Retrieved from https://www.uhs.com