I J C R M
International Journal of Contemporary Research In Multidisciplinary

Research Article

Cyber Security as a Necessity for Global Economic

Pooja Rani [1*], Kiran Kumari [2]
[1-2] Research Scholar, Department of Economics, Maharshi Dayanand University, Rohtak, Haryana, India

Corresponding Author: * Pooja Rani

DOI: https://doi.org/10.5281/zenodo.20255908

Abstract

In today's digital world cyber security is extremely important because as technology advances, the need for cybersecurity is increasing at the same peace. Due to rising cybercrimes, not only specific countries but the global economy is also being negatively affected. This impacts the economic stability of the nation and global trade as well. The main objective of this study is to examine the impact of cyber security on the global economy. For this study secondary data resources have been used, including various government publication, articles and internal reports. This study focuses on why investment in cyber security is essential for both develop and developing countries. Additionally, it reveals how effective cyber security regulation and awareness programs help protect the digital economy. The conclusion states that in today's digital era, no country can achieve sustainable global development without cyber security. Therefore, the cybersecurity organisation and team should make cyber risk management their central focus.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 05-04-2026
- **Accepted:** 15-04-2026
- **Published:** 17-05-2026
- **IJCRM:**5(3); 2026: 216-218

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Rani P, Kumari K. Cyber Security as a Necessity for Global Economic. Int J Contemp Res Multidiscip. 2026;5(3): 216-218.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Cyber security, Comprehensive, Global Economy, Investment, risk.

1. INTRODUCTION

In early 2023, countries like the United States, Japan and Australia updated their national cybersecurity plans, agreeing that governments should take more responsibility for protecting businesses and citizens from cyber threats. Cyber security is now considered a shared responsibility, as a system's safety depends on its mightiest point. However because it's hard to measure the financial impact of cyber incidents or the return on investment for protective measures, cyber security is often seen as just an operating cost, specially in developing countries with limited money. Cyber incidents can seriously harm a nation's economy, for a major ransomware attack on costa rica in 2022 caused an estimated loss $30 million every day, this highlights the need for better data on cyber incidents, which very globally based on local social, economic and political factors. High-income countries tend to face financially motivated attacks, while non-high-income countries often experience political motivated disruptions targeting public services.

Today the Internet has become the backbone of the world. Countless online transactions occur every day. In current times, people need the Internet for everything from E commerce to the stock market. It may sound simple, in reality, it has a dark side that everyone should be aware of. In 2023, a cyberattack caused nearly $8 trillion in global losses, and this figure double the following years. Imagine a single Ramson Wear attack like the colonial pipeline hack paralyzed the US fuel supply, causing massive economic damage. This is just one example such cyberattacks rampant world wild. The key question is can the global economy function without cyber security.

Cyber security is no longer limited to the IT sector it has become integral to global economy stability and national security. According to the World Economic Forums, cyber risk now ranks in top five risks. If we look at a developing country like India UPI transaction and bank attacks have led to significant financial losses, eroding people trust. Experts say poor cybersecurity is negative impacting GDP. Upcoming data of company branches, AI drive attacks, and regulatory frameworks will be key discussion points. This study will focus on how cyber security not only reduce risk but also make the global economy resilient. Every country must make it top priority, as the digital revolution would turn into a major disaster at any moment.

OBJECTIVES

1. To comprehensively analyze cyber threats to the Global Economy.
2. To describe the economic benefits derived from of cyber security investment.

METHODOLOGY

This study uses secondary data sources which is collected by various govt. publications, reports, articles, and online sources that are related to the cyber security, its risk and investment.

Comprehensively analyze

Cyber threats impact the global economy in very dangerous way, such as stopping operating system and shutting down supply chains. According to cyble's 2025 Annual "Threat Landscape Report" there has been a significant increase in Ransomware attacks. These attacks target sectors like construction, which severely affects their production and leads to increased financial penalties and downtime cost. In manufacturing and other critical industries, even a single cyberattack can disrupts their supply, which slows down GDP growth. Nowadays, these attacks can be seen in increasing rapidly.

Now a days it is being observed that cyber based supply chain attacks are increasing rapidly. By injecting malicious code into any company's software updates, attackers can negatively impact more than 100 companies at the same time. It has mostly been seen that these attacks target SAAS cloud, third party vendors. BFSI retail the government sector data branches are clearly increasing, and in 2025 there were more than 6000+ ransomware incident. In the global economy these attacks create cascading effect and negatively impact it, such as when one vendor is affected, and company's downstream business stop functioning, causing damage to trade and investment.

We are seeing that artificial intelligence (AI) is becoming a source of security, power, and political influence in all countries. It is no longer just an advanced technology but has turned into a dangerous proliferation. This is increasing geopolitical risks across the world. Through this, every country is developing its own autonomous weapons, which do not require any human intervention to operate. They independently select and attack their targets. For example, China and the United State are producing AI based military drones on a large scale. Using these, future wars can become even more dangerous. Additionally, deepfake videos or information can be created with this technology so easily influence the public. Those countries using AI based technology will lead in global competition, economy and political power. Most of countries are investing billions of dollars in such technologies.

Over all from the cyble analysis we have understood that these cyberattacks cause heavy damage to the global economy. Some cases are direct and other indirect. For a country like India the risk remain quite high. We can also see a negative effect on global GDP. Only through proactive system can the global economy be kept secure.

Benefits of cyber security investment

Cyber security investment means expending the money strategies to safe the data from cyberattacks. There are many benefits that we can achieve by investing in cyber security. Cyber security investment helps us to protect our sensitive data such us financial record, customer information, reduces the risk of hacking and research-based data. It helps prevent fraud. It gives strong security system and to ensure that organization continue their activities smoothly and reduce operational downtime. At a broader level, cyber security investments contribute to protecting essential national system such as banking network, energy grids, and defense infrastructure from cyber threats.

CONCLUSION

Online attacks have the power to wipe out entire companies and damage national economics badly. They cause billions in losses

every year through stolen data, stopped operational and broken trust. The solution lies in investing wisely in security measures right from the start. This proactive approach blocks attacks before they cause harm saves massive clean-up costs, and keeps daily business running smoothly. Nations and firms that prioritize defense spending now will avoid future disaster. Without this preparation, even the strongest organization remain at risk. Forward thinking protection is not just smart-it's essential for survival and success in today's digital world. Only through advanced planning can we turn potential catastrophe into continued progress and stability. Cyber threats can destroy business and economy completely. Smart expanding own protection be forehead is the only way to stop big losses. Companies should be plan ahead with strong defense to stay safe and keep growing.

REFERENCES

1. Akey P, Lewellen S, Liskovich I, Schiller C. Hacking corporate reputations. Rotman School of Management Working Paper. 2021;(3143740).
2. Apau R, Koranteng FN. Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior. Int J Cyber Criminol. 2019;13(2).
3. Aidasoro I, Gambacorta L, Giudici P, Leach T. Operational and cyber risks in the financial sector. 2020.
4. Biener C, Eling M, Wirfs JH. Insurability of cyber risk: An empirical analysis. Geneva Pap Risk Insur Issues Pract. 2015;40:131-158.
5. Caven P, Camp LJ. Towards a more secure ecosystem: Implications for cybersecurity labels and SBOMs. SSRN Electron J. 2023;4527526.
6. Nir Kshetri. Cybercrime and cybersecurity in Africa. J Glob Inf Technol Manag. 2019;22(2):77-81.

About the Corresponding Author

Pooja Rani is a Research Scholar in the Department of Economics at Maharshi Dayanand University. Her academic interests include economic development, public policy, social issues, and contemporary economic challenges in India. She is actively engaged in research work contributing to the field of economics through analytical and interdisciplinary approaches.