STM JOURNALS

Journal of
Network Security

ISSN: 2395-6739 (Online)
ISSN: 2321-8517 (Print)
Volume 13, Issue 3, 2025
September–December
DOI (Journal): 10.37591/JoNS

https://journals.stmjournals.com/jons

Review JoNS

Cybersecurity in a Digital World: Risks and Future Perspectives

Aatraiyee Dixit*, Aparna Madaria, Manisha, Rishabh

Abstract

The field of information security offers a wide range of guidance in academic and practitioner literature. While various strategies such as deterrence, deception, detection, and reaction are explored, most research focuses on technological countermeasures to prevent security threats. This study presents the findings of a qualitative study conducted in Korea, examining how businesses utilize security techniques to safeguard their information systems. The results highlight a strong emphasis on preventive measures, driven by the need to ensure the availability of technology and services. However, there is limited awareness of broader enterprise security concerns. While other tactics were observed, they primarily supported the objective of prevention. The study proposes a research agenda for implementing diverse strategies throughout an enterprise, with a focus on integrating, balancing, and optimizing systems. The study explores various aspects of information security and investigates contexts where security strategies are frequently discussed, such as military sources. It identifies nine distinct security strategies. Through a qualitative focus group approach, security managers from eight organizations discussed their organizations' security practices. The findings indicate a predominant reliance on prevention to maintain technology services, with other methods employed as operational support for this overarching strategy.

Keywords: Cyber security, cyber threats, web 3.0, implications, technology

INTRODUCTION

Rapid technological advancements have increased organizational efficiency, but they have also brought serious risks to an organization's data and information. The protection of networks, systems, and data in the cyber world is known as cyber security, and it is a risky matter for all commercial enterprises. As the number of devices connected to the internet grows at a rapid rate, cyber safety will become increasingly important.

To tackle these risks, organizations need to adopt a strong information security strategy as part of a comprehensive framework. This framework should enable the development, institutionalization, assessment, and continuous improvement of an information security program. Importantly, the strategy should align with and support the organization's overall strategic goals, ensuring that its content is directly linked to these broader objectives [1]. Organizations are increasingly recognizing the crucial role that information and related technologies play in driving innovation and gaining a competitive edge. However, in today's ever-changing information landscape, corporate information and technology services face various security risks. These risks include breaches of sensitive data and prolonged disruptions to email and internet access, which can have a significant impact on business continuity [2].

***Author for Correspondence**
Aatraiyee Dixit
E-mail: Aatraiyeedixit.26@gmail.com

Student (M Tech), Department of Computer Science and Engineering, Lakshmi Narain College of Technology, Bhopal, Madhya Pradesh, India

Received Date: February 04, 2025
Accepted Date: July 02, 2025
Published Date: July 24, 2025

Citation: Aatraiyee Dixit, Aparna Madaria, Manisha, Rishabh. Cybersecurity in a Digital World: Risks and Future Perspectives. Journal of Network Security. 2025; 13(3): 44–49p.

It is worth noting that security managers often overlook business security risks, leading to the implementation of security plans in an ad hoc manner rather than as part of a comprehensive and well-thought-out approach to risk management. This lack of strategic planning exposes organizations to emerging threats and undermines the effectiveness of their security measures [3, 4].

Since the majority of cyberattacks are carried out with the least amount of money and resources, they are primarily asymmetric. As a result, cybercrime poses a serious risk in the current Internet working environment [5]. Figure 1 shows the top nations with the highest number of victim complaints, according to the 2023 report from the Internet Crime Complaint Centre.

LITERATURE REVIEW

Strategy encompasses the selection, implementation, and execution of methods tailored to particular contexts, including military operations. According to Beckman and Rosenfield, strategy involves determining a business's intended direction and the means to reach that goal [6]. This principle is applicable to information security strategy, which aims to utilize defensive technologies to safeguard an organization's information infrastructure while ensuring confidentiality, integrity, and availability with minimal expenditure and effort [7]. Essential techniques include deterrence, prevention, surveillance, detection, response, deception, perimeter defence, compartmentalization, and layering.

Temporal and Spatial Considerations in Strategy

The execution of strategy incorporates time, through either proactive or reactive approaches, and space, by structuring environments into segmented zones that separate trusted systems from untrusted ones [8]. Well-crafted strategies play a crucial role in decision-making and bolster security measures.

Prevention (PREV)

Prevention aims to protect information assets from unauthorized access, loss, or exposure through various policies, including clean desk protocols, encryption, firewalls, and intrusion detection systems [9]. Additional measures such as authentication and vulnerability assessments further enhance security defences.

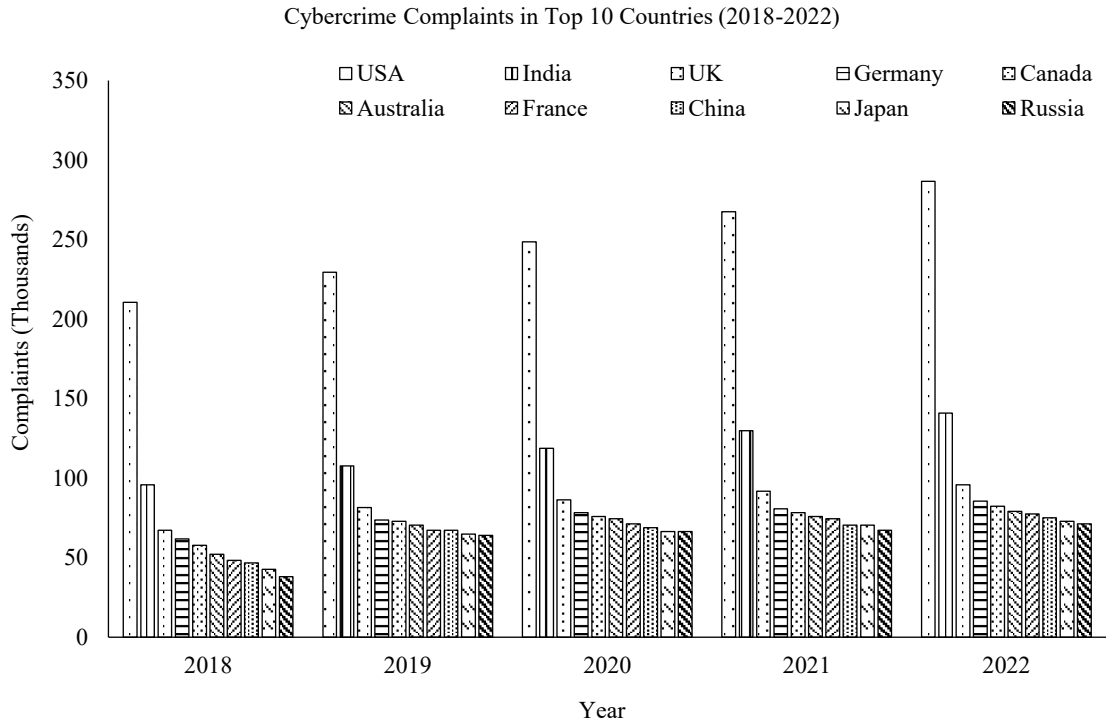

Figure 1. Top 20 Countries by count: Cyber crime complaints.

Deterrence (DETER)

Deterrence is based on the enforcement of discipline and penalties to ensure adherence to security policies. The predictability of consequences and the severity of penalties are critical to its effectiveness [10]. Education and enforcement initiatives improve compliance, thereby reducing instances of misuse and violations.

Surveillance (SURV)

Surveillance entails the monitoring of both physical and digital environments to maintain situational awareness [11]. By employing tools such as intrusion detection systems and sensors, organizations can collect data to gain insights into the security landscape and proactively address potential threats.

Detection (DETECT)

Detection is centred on recognizing specific security incidents, such as intrusions or misuse, enabling organizations to respond effectively.

CYBER SPACE OF INDIA

India's cyberspace is a rapidly growing and evolving ecosystem, encompassing digital infrastructure, government initiatives, private sector involvement, and user engagement. Here is an overview of India's cyberspace.

Infrastructure for Digitalization

India's digital infrastructure is among the biggest and fastest-growing in the world.

Important elements consist of:

- *Broadband Penetration:* With more than 850 million active users as of 2023, India ranks among the top nations in terms of internet users.
- *Mobile Connectivity:* Widespread access to the internet has been made possible by reasonably priced cell phones and mobile data plans.
- *Cloud Services:* Small and medium-sized organizations (SMEs) in particular are changing as a result of the quick uptake of cloud computing.

Difficulties with Cybersecurity

New dangers include ransomware, which is malicious software that encrypts data and requests payment to unlock it [12]. The disastrous effects of ransomware on vital infrastructure have been illustrated by well-known events such as the Colonial Pipeline attack. Phishing is the use of social engineering tactics to deceive someone into divulging private information. The most common way to launch more extensive cyberattacks is still through phishing.

Vulnerabilities of Humans

Human mistake continues to be a major contributor to cybersecurity incidents in spite of technological developments [13]. Common problems include using weak passwords, not updating software, and being vulnerable to social engineering scams.

Restrictions on Resources

Small and medium-sized businesses (SMEs) are susceptible to exploitation because they sometimes lack the funding necessary to implement cutting-edge cybersecurity safeguards. Figure 2 shows the number of cybercrime cases in India (2018–2023).

Government Efforts to Boost Cyberspace

The Program for Digital India

Seek to make India a society empowered by technology. Smart Cities, e-Kranti, and Bharat Net are important initiatives.

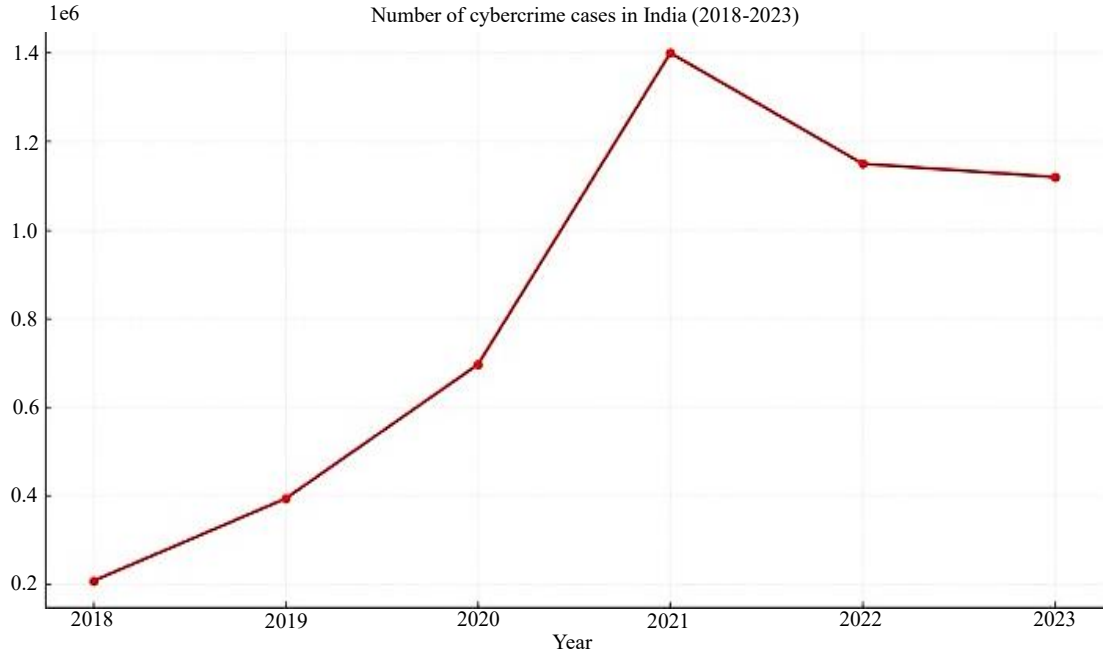

Figure 2: Number of cybercrime cases in India.

Policies for Cybersecurity

A framework for protecting cyberspace is offered by the National Cyber Security Policy (NCSP). By providing free antivirus software, Cyber Swachhta Kendra encourages a safe online environment.

Law

The IT Act of 2000 regulates online activity and establishes sanctions for cybercrime. The goal of the proposed Digital Personal Data Protection Bill is to protect privacy and personal information.

NATIONAL CYBER SECURITY POLICY 2013

The National Cyber Security Policy 2013 (NCSP 2013) was introduced by the Government of India to create a secure and resilient cyberspace for citizens, businesses, and the government. It aims to protect critical information infrastructure and promote confidence in the digital ecosystem while addressing the growing challenges posed by cyber threats.

Vision

To create a secure and resilient cyberspace that safeguards citizen data, critical infrastructure, and business operations while fostering trust and economic growth.

Mission

To protect Information and Information cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of Institutional structures, people, processes, technology and cooperation [1].

Department of Electronics and Information Technology, India proposed a law for Cyber Security which is known as National Cyber Security policy and is aimed for prevention from cyberattacks of private and public infrastructure. It also speculates safe information like financial and banking information, sovereign data and personal information of users. It was somewhat relevant to US NSA (National Security Agency) leaks that indicate spying on Indian users by US government, who have no technical or legal safeguards for it.

OBJECTIVES

Ministry of Communications and Information Technology (India) defines Cyber space is a wide and complex environment consisting of communication between people, software services supported by worldwide distribution of information and communication technology. Ministry of Communications and Information Technology (India) define following objectives of the sated policy:

1. To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
2. To create an assurance framework for design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
3. To improve visibility of integrity of ICT products and services by establishing infrastructure for testing and validation of security of such product.
4. To provide fiscal benefit to businesses for adoption of standard security practices and processes.
5. To enable protection of information while in process, handling, storage and transit so as to safeguard privacy of citizen's data and reducing economic losses due to cybercrime or data theft.
6. To enable effective prevention, investigation and prosecution of cybercrime and enhancement of low enforcement capabilities through appropriate legislative intervention.

Private think-tank Observer Research Foundation & Industry body, FICCI conducted a conference with the collaboration of NSCS by the Government of India. There were many speakers present in the conference including the host of the countries like India, Belgium, Russia, Australia, Estonia, Germany, Russia. The two major outputs have come after this conference: firstly, India has shown its eagerness to initiate cyberspace open discussions globally. And secondly, India has made a NATIONAL CYBER SECURITY POLICY rather than strategy of cyber security. Figure 3 shows the distribution of targets in cyberattacks.

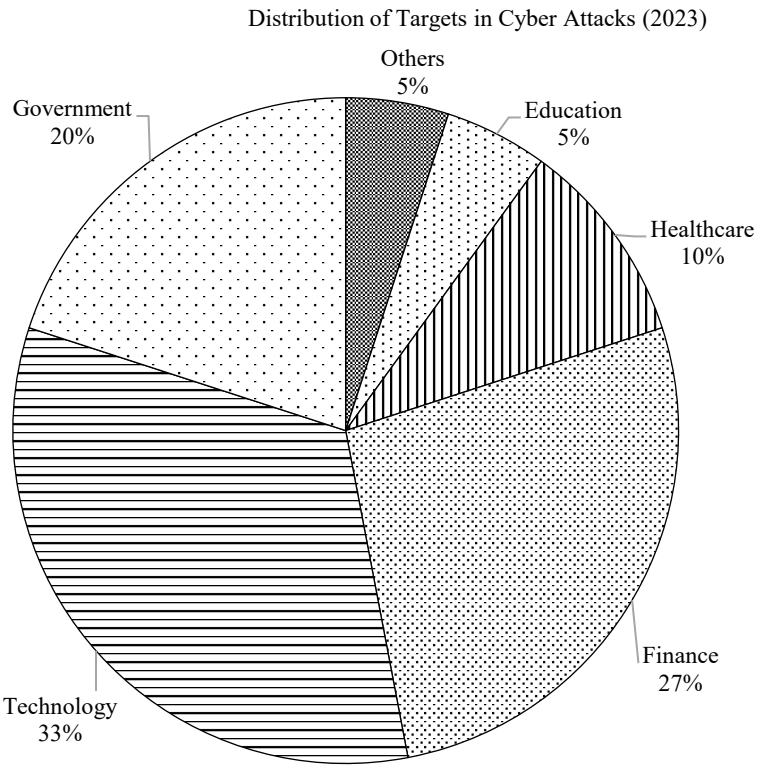

Figure 3. Distribution of targets.

CONCLUSION

This study looked at cybersecurity challenges in the context of Industry 4.0, employing a systematic approach to the literature review and a qualitative examination of the contents of the articles that were chosen. The evaluation of the articles concentrated on four areas of examination. These areas include: (1) an examination of cybersecurity and Industry 4.0/IIoT definitions; (2) an examination of industry types and industrial assets most affected by cybersecurity issues; (3) a definition of system vulnerabilities, cyber threats, risks, and countermeasures to be taken in Industry 4.0 scenarios; and (4) the identification of guidelines and more structured solutions to deal with cybersecurity issues. As a consequence, each area's major elements were outlined in a reference framework. The framework gathers and summarizes the most referenced evidence for each area of investigation in order to provide an immediate possibility of synthesis that can be used to guide future research as well as management activities. Although various solutions for cybersecurity challenges in Industry 4.0 have been created, none of them take into account the three exposure layers of Cyber-Physical Systems (physical, network, and compute) that cyberattacks might exploit simultaneously. Furthermore, the papers examined do not approach cybersecurity from a solely management standpoint, but rather from an IT standpoint. A management viewpoint should aid businesses in the proper adoption of new organizational practices and change management activities.

REFERENCES

1. Mosteanu NR. Artificial intelligence and cyber security–face to face with cyber attack–a Maltese case of risk management approach. Ecoforum. 2020 May 9; 9(2): 1–8.
2. Soni VD. Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. Available at SSRN 3624487. 2020 Jun 10.
3. Patil P. Artificial intelligence in cybersecurity. International Journal of Research in Computer Applications and Robotics (IJRCAR). 2016 May; 4(5): 1–5.
4. Sagar BS, Niranjan S, Sachin DN. Providing cyber security using artificial intelligence–a survey. In 2019 IEEE 3rd international conference on computing methodologies and communication (ICCMC). 2019 Mar 27; 717–720.
5. Sedjelmaci H, Guenab F, Senouci SM, Moustafa H, Liu J, Han S. Cyber security based on artificial intelligence for cyber-physical systems. IEEE Netw. 2020 Jun 2; 34(3): 6–7.
6. Beckman SL, Rosenfield DB. Operations strategy: competing in the 21st century. McGraw-Hill/Irwin; 2008.
7. Wiafe I, Koranteng FN, Obeng EN, Assyne N, Wiafe A, Gulliver SR. Artificial intelligence for cybersecurity: a systematic mapping of literature. IEEE Access. 2020 Jul 31; 8: 146598–612.
8. Yampolskiy RV, Spellchecker MS. Artificial intelligence safety and cybersecurity: A timeline of AI failures. arXiv preprint arXiv:1610.07997. 2016 Oct 25.
9. Morel B. Artificial intelligence and the future of cybersecurity. In Proceedings of the 4th ACM workshop on Security and artificial intelligence. 2011 Oct 21; 93–98.
10. Wirkuttis N, Klein H. Artificial intelligence in cybersecurity. Cyber, Intelligence, and Security. 2017 Jan; 1(1): 103–19.
11. Zarina IK, Ildar RB, Elina LS. Artificial Intelligence and Problems of Ensuring Cyber Security. Int J Cyber Criminol. 2019 Jul 1; 13(2): 564–577.
12. Li JH. Cyber security meets artificial intelligence: a survey. Front Inf Technol Electron Eng. 2018 Dec; 19(12): 1462–74.
13. Taddeo M, McCutcheon T, Floridi L. Trusting artificial intelligence in cybersecurity is a double-edged sword. Nat Mach Intell. 2019 Dec; 1(12): 557–60.

