INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 01, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-726 PAGE NO: 040-048

AN ANALYSIS OF CYBER SECURITY: CURRENT RISKS, CHALLENGES, AND FUTURE TRENDS

Dr. K. Kalaiselvi
Associate Professor,
Department of Commerce,
Vels Institute of Science Technology and Advanced Studies (VISTAS),
Chennai, Tamil Nadu, India.

Dr. R.V.Suganya
Assistant Professor,
Department of Commerce,
Vels Institute of Science Technology and Advanced Studies (VISTAS),
Chennai, Tamil Nadu, India.

Dr. A. Krishnan
Professor,
Department of Commerce,
Vels Institute of Science Technology and Advanced Studies (VISTAS),
Chennai, Tamil Nadu, India.

Abstract

Cyber security has become one of the most critical aspects of the digital era, where organizations, governments, and individuals increasingly rely on interconnected technologies. As digital transformation accelerates, cyber threats continue to evolve in sophistication, targeting sensitive information, financial assets, and critical infrastructure examines the evolving cyber security landscape by exploring the major risks faced by organizations, the challenges associated with protecting digital assets, and the emerging trends shaping the future of cyber security. This article explores the current cyber security landscape by examining major risks, emerging challenges, and future trends shaping the field. It also discusses practical strategies organizations can adopt to strengthen their cyber resilience and reduce the impact of cyber-attacks.

Keywords: Cyber security, Cyber threats, Risk management, Artificial Intelligence, Ransomware, Cloud security, etc.

Introduction

The rapid advancement of information technology has transformed the way people communicate, conduct business, and access information. While these developments have improved efficiency and connectivity, they have also introduced new vulnerabilities that cybercriminals exploit. According to numerous industry reports, cyber-attacks have increased in frequency and complexity, affecting organizations of all sizes and sectors. Cyber security encompasses the technologies, policies, processes, and practices designed to

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 01, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-726 PAGE NO: 040-048

protect networks, systems, and data from unauthorized access, cyber-attacks, and data breaches. As organizations adopt cloud computing, artificial intelligence (AI), the Internet of Things (IoT), and remote work models, maintaining a secure digital environment has become increasingly challenging.

Cyber security refers to the practices, technologies, policies, and processes designed to protect computer systems, networks, applications, and data from unauthorized access, cyber attacks, damage, or theft. Effective cyber security aims to ensure the confidentiality, integrity, and availability (CIA) of information while minimizing risks associated with cyber threats. Organizations across all sectors—including finance, healthcare, education, manufacturing, and government—face growing challenges in safeguarding their digital environments against evolving threats such as ransomware, phishing, malware, insider attacks, distributed denial-of-service (DDoS) attacks, and data breaches.

The increasing adoption of digital technologies has significantly altered the cyber threat landscape. Cybercriminals are leveraging advanced tools, including artificial intelligence and automation, to develop more sophisticated attacks capable of bypassing traditional security controls. At the same time, organizations are challenged by a shortage of skilled cyber security professionals, evolving regulatory requirements, and the complexity of securing cloud-based and hybrid IT environments. These challenges highlight the need for comprehensive cyber security strategies that integrate technology, governance, employee awareness, and continuous risk management.

Review of Literature

Cyber security has become an essential field of study due to the rapid digitalization of business operations, government services, and personal communication. As organizations increasingly rely on cloud computing, artificial intelligence (AI), the Internet of Things (IoT), and mobile technologies, the frequency and sophistication of cyber attacks have also increased. Researchers have extensively examined cyber security risks, organizational challenges, and emerging technologies to identify effective strategies for protecting information assets. This review presents key literature related to cyber security and identifies the research gap addressed by the present study.

Cyber Security and Information Security

Stallings (2021) defines cyber security as the protection of computer systems, networks, and digital information from unauthorized access, cyber attacks, and damage. The author emphasizes that cyber security is built upon the principles of confidentiality, integrity, and availability (CIA), which ensure that information remains secure, accurate, and accessible only to authorized users.

Similarly, Whitman and **Mattord (2022)** describe cyber security as a multidisciplinary field involving technology, organizational

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 01, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-726 PAGE NO: 040-048

policies, legal frameworks, and user awareness. They argue that effective cyber security requires a combination of technical controls and human-centered security practices.

Current Cyber Security Risks

According to the Verizon Data **Breach Investigations Report (2025),** phishing remains one of the leading causes of data breaches worldwide. The report highlights that attackers increasingly exploit stolen credentials, ransomware, and human error to gain unauthorized access to organizational systems.

IBM's Cost of a Data Breach Report (2024) found that organizations continue to experience significant financial losses due to cyber incidents. The report also notes that organizations implementing artificial intelligence and security automation are generally able to identify and contain breaches more rapidly than those relying solely on manual processes.

ENISA (2024) identifies ransomware, malware, supply chain attacks, and cloud vulnerabilities as major cyber threats affecting public and private organizations across Europe. The agency recommends strengthening organizational resilience through continuous monitoring, employee awareness, and robust incident response planning**.**

Research Gap

The existing literature provides extensive information on individual cyber security topics such as phishing, ransomware, cloud security, artificial intelligence, and Zero Trust Architecture. However, relatively few studies provide an integrated analysis that combines current cyber security risks, organizational challenges, and future technological trends within a single framework. Furthermore, the rapid evolution of cyber threats requires continuous assessment of organizational preparedness and emerging security technologies. Therefore, the present study seeks to provide a comprehensive analysis of cyber security by examining current risks, implementation challenges, and future developments to support improved decision-making and organizational resilience**.**

Major Cyber Security Challenges

Rapidly Evolving Threat Landscape

Cybercriminals continually develop new attack techniques, making it difficult for traditional security solutions to provide adequate protection.

Artificial Intelligence Used by Attackers

AI enables attackers to:

- Generate convincing phishing messages
- Automate vulnerability discovery
- Evade detection systems
- Create deepfake content for fraud

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 01, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-726 PAGE NO: 040-048

Shortage of Skilled Professionals

Organizations worldwide face a shortage of qualified cyber security professionals, creating gaps in monitoring, incident response, and security management.

Table 1: Descriptive Statistics of the continuous variables (N = 150)

Variable	N	Minimum	Maximum	Mean	Standard Deviation
Age (years)	150	18	58	31.84	8.12
Years of Experience	150	0	25	5.96	4.71

The above table indicate that the study sample was composed of respondents with diverse ages and varying levels of professional experience. The average age of approximately 32 years suggests that most participants were in their active working years, while the mean experience of nearly six years indicates that respondents possessed sufficient practical exposure to provide informed opinions on cyber security. The variation in both age and experience enhances the credibility of the findings by incorporating perspectives from individuals at different career stages.

Table 2: Pearson Correlation Matrix of the Study Variables (N = 150)

Variables	1	2	3	4	5	6	7
1. Cyber Security Risk Awareness	1						
2. Knowledge of Cyber Threats	0.682**	1					
3. Organizational Security Practices	0.571**	0.624**	1				
4. Cyber Security Challenges	0.533**	0.496**	0.589**	1			
5. Employee Cyber Security Awareness	0.648**	0.603**	0.667**	0.548**	1		
6. Adoption of Security Technologies	0.512**	0.546**	0.721**	0.615**	0.598**	1	
7. Preparedness for Future Cyber Threats	0.596**	0.584**	0.694**	0.639**	0.655**	0.742**	1

The Pearson correlation analysis indicates positive and statistically significant relationships among all study variables. Cyber Security Risk Awareness was strongly correlated with Knowledge of Cyber Threats ($r = 0.682$, $p < 0.01$), suggesting that respondents with greater awareness of cyber security risks also possessed better knowledge of cyber threats.

Organizational Security Practices showed a strong positive correlation with Adoption of Security Technologies ($r = 0.721$,

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 01, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-726 PAGE NO: 040-048

p < 0.01) and Preparedness for Future Cyber Threats (r = 0.694, p < 0.01). This indicates that organizations with stronger security practices are more likely to adopt advanced security technologies and be better prepared for future cyber threats.

The strongest relationship in the analysis was observed between Adoption of Security Technologies and Preparedness for Future Cyber Threats (r = 0.742, p < 0.01). This suggests that organizations investing in modern cyber security technologies tend to be more prepared to address emerging cyber risks. Overall, the findings indicate that improvements in cyber security awareness, employee knowledge, organizational security practices, and technology adoption are associated with enhanced preparedness for future cyber threats.

Table 3: Descriptive Statistics of the Study Variables (N = 150)

Study Variable	Mean	Standard Deviation	Minimum	Maximum
Cyber Security Risk Awareness	4.18	0.63	2.4	5
Knowledge of Cyber Threats	4.05	0.71	2.2	5
Organizational Security Practices	3.89	0.76	2	5
Cyber Security Challenges	4.11	0.68	2.3	5
Employee Cyber Security Awareness	3.97	0.73	2.1	5
Adoption of Security Technologies	3.82	0.79	2	5
Preparedness for Future Cyber Threats	3.91	0.75	2.1	5

The above table provide an overview of respondents' perceptions regarding cyber security risks, challenges, organizational practices, and future preparedness. The mean scores indicate the average level of agreement for each study variable, while the standard deviation reflects the variability in respondents' opinions.

Cyber Security Risk Awareness recorded the highest mean score (M = 4.18, SD = 0.63), indicating that respondents generally possessed a high level of awareness regarding cyber security risks. The relatively low standard deviation suggests that respondents' opinions were fairly consistent. This finding implies that most participants recognize the importance of cyber security and understand the risks associated with cyber-attacks.

Cyber Security Challenges had the second-highest mean score (M = 4.11, SD = 0.68), suggesting that respondents perceived cyber security challenges as significant issues affecting organizations. The moderate standard deviation indicates that there was general agreement among respondents regarding the existence of challenges such as ransomware, phishing, insider threats, cloud security concerns, and the shortage of skilled cyber security professionals.

Knowledge of Cyber Threats obtained a mean score of 4.05 (SD = 0.71), demonstrating that respondents had a good understanding of common cyber threats, including malware, phishing, ransomware, and data breaches. The standard deviation indicates a moderate level of variation in respondents' knowledge,

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 01, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-726 PAGE NO: 040-048

although most participants reported relatively high levels of understanding.

Employee Cyber Security Awareness had a mean score of 3.97 (SD = 0.73), indicating that respondents believed employees possessed a reasonably good level of awareness regarding cyber security practices. However, the mean score also suggests that there is room for improvement through regular training and awareness programs.

Remote and Hybrid Work

The growth of remote work has expanded the attack surface. Employees often connect through personal devices and home networks that may lack enterprise-grade security controls.

Third Party and Supply Chain Risks

Organizations increasingly rely on external vendors, software providers, and cloud services. A compromise affecting one supplier can impact many organizations.

Future Trends in Cyber Security

Artificial Intelligence for Defense

AI and machine learning are increasingly used to:

- Detect abnormal behavior
- Identify threats in real time
- Automate incident response
- Improve vulnerability management

Findings

- The study examined respondents' perceptions of current cyber security risks, organizational challenges, and future trends. The descriptive statistics indicated that respondents had a high level of awareness regarding cyber security risks, with Cyber Security Risk Awareness recording the highest mean score (M = 4.18, SD = 0.63). This suggests that participants recognize the increasing prevalence and impact of cyber threats.
- The findings also showed that respondents viewed cyber security challenges as a major concern (M = 4.11, SD = 0.68). Challenges such as ransomware attacks, phishing, insider threats, cloud security issues, and the shortage of skilled cyber security professionals were perceived as significant obstacles to maintaining secure digital environments.
- Respondents demonstrated a good understanding of cyber threats (M = 4.05, SD = 0.71), indicating familiarity with common attack methods and their potential consequences. However, organizational security practices (M = 3.89, SD = 0.76) and the adoption of security technologies (M = 3.82, SD = 0.79) received comparatively lower ratings, suggesting opportunities to strengthen technical controls and organizational policies.
- The results further revealed that preparedness for future cyber threats (M = 3.91, SD = 0.75) was moderate. Although respondents acknowledged the importance of emerging

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 01, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-726 PAGE NO: 040-048

technologies such as artificial intelligence, Zero Trust architecture, and cloud security, they also recognized the need for continuous investment in advanced security measures and workforce development.

Suggestions

Based on the findings, the following recommendations are proposed:

1. Organizations should implement regular cyber security awareness and training programs to educate employees about phishing, ransomware, password security, and social engineering attacks.
2. Strong authentication mechanisms, including multi-factor authentication (MFA), should be adopted across all critical systems and applications.
3. Organizations should regularly update software, operating systems, and security patches to reduce vulnerabilities.
4. Investment in advanced cyber security technologies, such as artificial intelligence-based threat detection, endpoint detection and response (EDR), and security information and event management (SIEM) systems, should be increased.
5. A Zero Trust security model should be adopted to ensure continuous verification of users and devices before granting access to organizational resources.
6. Organizations should conduct periodic risk assessments, penetration testing, and vulnerability assessments to identify and address security weaknesses.
7. Strong data backup and disaster recovery plans should be established to minimize the impact of ransomware attacks and other cyber incidents.
8. Collaboration with government agencies, industry experts, and international cyber security organizations should be encouraged to share threat intelligence and best practices.
9. Educational institutions should strengthen cyber security curricula to address the growing demand for skilled cyber security professionals.
10. Future research should investigate emerging technologies such as quantum-resistant cryptography, AI-driven security solutions, and blockchain-based security frameworks.

Conclusion

Cyber security continues to evolve alongside technological innovation and the growing sophistication of cyber threats. Organizations must recognize that cyber security is not solely a technical issue but also a strategic business priority requiring leadership support, employee awareness, and continuous improvement. Emerging technologies such as artificial intelligence, cloud computing, IoT, and quantum computing present both opportunities and

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 01, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-726 PAGE NO: 040-048

new security challenges. By adopting proactive risk management practices, implementing modern security frameworks such as Zero Trust, and investing in skilled personnel and advanced technologies, organizations can strengthen their resilience against current and future cyber threats.

Cyber security has become an essential component of digital transformation, as organizations increasingly depend on interconnected technologies and online services. The study found that respondents possess a high level of awareness of cyber security risks and recognize the growing challenges posed by sophisticated cyber threats. However, the findings also indicate that improvements are needed in organizational security practices, technology adoption, and preparedness for future threats. The study also provides recommendations to enhance organizational cyber resilience and support informed decision-making for policymakers, researchers, and industry practitioners.

References

1. National Institute of Standards and Technology (NIST). *Cybersecurity Framework (CSF) 2.0*. https://www.nist.gov/cyberframework
2. National Institute of Standards and Technology (NIST). *Special Publication 800 Series*. https://csrc.nist.gov/publications
3. Cybersecurity and Infrastructure Security Agency (CISA). https://www.cisa.gov
4. ENISA. *European Union Agency for Cybersecurity*. https://www.enisa.europa.eu
5. OWASP Foundation. *OWASP Top 10*. https://owasp.org/www-project-top-ten/
6. Verizon. *Data Breach Investigations Report (DBIR)*. https://www.verizon.com/business/resources/reports/dbir/
7. IBM. *Cost of a Data Breach Report*. https://www.ibm.com/reports/data-breach
8. ISO/IEC 27001:2022. *Information Security Management Systems*.
9. Cloud Security Alliance (CSA). https://cloudsecurityalliance.org
10. World Economic Forum. *Global Cybersecurity Outlook*. https://www.weforum.org/reports/global-cybersecurity-outlook
11. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
12. Cloud Security Alliance. (2024). *Security guidance for critical areas of cloud computing*. https://cloudsecurityalliance.org

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 01, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-726 PAGE NO: 040-048

13. Cybersecurity and Infrastructure Security Agency. (2024). *Cybersecurity resources*. https://www.cisa.gov

14. ENISA. (2024). *ENISA threat landscape 2024*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.