LogicLink: Journal of Artificial Intelligence and Multimedia in Informatics
E-ISSN: 3062-9098 | P-ISSN: 3063-4504 | Vol. 2 No. 2, December 2025, pp. 198 – 206

A Comprehensive Study of Information Security Principles, Threats, and Organizational Protection Measures

M.A. Paiman[1], Serajulhaq Afghan[2], Abdul Karim Himmat[3]
[1]*Universitas Islam Negeri K.H. Abdurrahman Wahid Pekalongan, Pekalongan, Indonesia*
[2]*Benawa University, Kandahar, Afghanistan*
[3]*University of Haripur, Haripur, Pakistan*
*E-mail : mukhtar.ahmad.paiman25118@mhs.uingusdur.ac.id**
**Corresponding author*

Received 20 November 2025; Revised 13 December 2025; Accepted 23 December 2025

Abstract - Information security has become a vital specification and element in modern digital and electronic environments as organizations, governments, and individuals at an accelerating rate rely on information systems to fulfill indispensable operations. The rapid growth of digital communication, cloud computing, mobile technologies, and the Internet of Things (IoT) has augmented the volume of data generated and transmitted, making it more susceptible to cyber threats. Information security underscores on protecting data confidentiality, integrity, and availability through a synthesis of technical, organizational, and human-centered measures. This abstract provides summary of key elements of information security, examines major emerging threats, and highlights the importance of embracing comprehensive security frameworks. Cyberattacks such as ransomware, phishing, Distributed Denial of Service (DDoS), and social engineering have become more advanced, addressing system susceptibilities and human behavior. These attacks can result in financial loss, data breaches, reputational damage, and operational disruption. As a result, organizations must carry out robust security frameworks, including encryption, access control mechanisms, multi-factor authentication, intrusion detection and prevention systems, firewalls, and progressive system tracking. In addition, the integration of artificial intelligence and machine learning has enhanced cybersecurity capabilities by enabling automated threat detection and predictive analysis. However, besides technological advancements, human factors remain a major cause of security breaches. Employee negligence, weak passwords, lack of awareness, and susceptibility to social engineering attacks continue to undermine security efforts. Therefore, effective information security needs not only advanced tools but also strong organizational policies, regular training programs, and a special way of security awareness. Overall, information security is a flexible and evolving field that requires a nonstop adaptation to new threats and technologies. A holistic approach that brings togethar technical solutions, human-centered techniques, and regulatory compliance is essential for safeguarding digital assets and ensuring the resilience of information systems in an increasingly interconnected world.
Keywords – Information security, Risk management, CIA triad, Data protection, Security policies, IT security professionals, Cyberattacks, Digital operations, Network and application security, Digital forensics

1. INTRODUCTION

Information security (infosec) refers to the process of protecting and safeguarding information by controlling and reducing the risks associated with it. As a core part of information

risk management, it focuses on preventing unauthorized access, misuse, disclosure, disruption, deletion, alteration, or damage to data, as well as minimizing the negative effects when such incidents occur. The information being protected can exist in any form—digital, physical, tangible like documents, or intangible like knowledge.

The fundamental goal of information security is to keep a balanced protection of confidentiality, integrity, and availability—commonly known as the CIA triad—while ensuring that security policies are implemented effectively without hindering organizational productivity. Achieving this balance typically requires a structured risk-management process.

To ensure consistency across the field, professionals develop guidelines, policies, and standards covering areas such as password practices, antivirus tools, firewalls, encryption, legal responsibilities, and security awareness training. These efforts are supported by laws and regulations that govern how data is accessed, processed, stored, transmitted, and destroyed.

Although some organizations still rely on paper-based systems that require their own protections, digital operations now dominate. As a result, information assurance is largely managed by IT security professionals who apply security principles to technological systems. These specialists play a critical role in protecting valuable organizational data and defending systems against attacks designed to steal sensitive information or compromise internal operations.

The field of information security encompasses multiple specialized roles, including network security, application and database protection, security assessment, IT auditing, business continuity planning, e-discovery, and digital forensics.

2. RESEARCH METHOD

This study concludes a mixed methods research approach, combining qualitative and quantitative techniques to provide a wide understanding of information security principles and practices. The qualitative component focuses on a conceptual and literature-based analysis, drawing from academic publications, industry standards, organizational policies, and professional reports. This part of the method is used to test core concepts such as the CIA triad, risk management processes, security policy frameworks, and specialized roles within the information security field. Through document analysis, the study synthesizes established knowledge to explain how information security functions across digital and physical environments.

The quantitative component complements the qualitative analysis by drawing on secondary numerical data from reputable cybersecurity reports, industry surveys, and global standards published between 2023 and 2024. These sources provide measurable and appropriate indicators related to security awareness levels, incident frequency, threat trends, and the adoption of security controls across organizations. The use of secondary datasets is a well-established approach in information security research, as it enables access to large-scale, validated, and systematically collected evidence (Romanosky, 2016). Key references for this study include NIST cybersecurity publications and standards (including the Cybersecurity Framework 2.0 released in 2024), Verizon's 2024 Data Breach Investigations Report (DBIR), and IBM's 2024 Cost of a Data Breach Report, which provide up-to-date quantitative insights into attack vectors, control failures, human-related vulnerabilities, and organizational risk behaviors.

This externally sourced quantitative finding is integrated with qualitative findings to identify recurring patterns, validate emerging themes, and strengthen the study's overall credibility. The combination of secondary quantitative data with qualitative insights reflects a robust mixed-methods research strategy, as it supports both theoretical explanation and empirically measurable real-world evidence (Creswell & Creswell, 2018; Venkatesh et al., 2013). By incorporating the most recent industry and standards-based data from 2024, this approach

offers a holistic and current understanding of information security, effectively linking conceptual analysis with contemporary organizational outcomes and risk environments.

Table 1. Summary of Key Information Security Principles, Their Operational Definitions, and Relevant Standards

Concept/Principle	Literature-Derived Operational Definition	Key Standards/References (e.g., ISO 27001, NIST)
CIA Triad	A model where Confidentiality, Integrity, and Availability are the central goals of an information security system.	ISO/IEC 27002, *Schneier (1996)*
Risk Management Process	Systematic process for identifying, analyzing, evaluating, and treating information security risks.	NIST SP 800-37, COBIT
Security Policy Framework	A documented set of rules governing how an organization manages, protects, and distributes sensitive information.	Organizational Policy Analysis
Specialized Roles	Defined responsibilities (e.g., CISO, Security Analyst) necessary for policy enforcement and operational security.	Professional Reports, Job Descriptions

Information security standards: Information security standards are techniques generally outlined in published materials that attempt to protect the information of a user or organization. This environment includes users themselves, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. The principal objective is to reduce the risks, including preventing or mitigating attacks. These published materials consist of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies. Information security attributes or qualities, i.e., confidentiality, integrity and availability (CIA). Information systems are composed in three main portions, hardware, software and communications with the purpose to help identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: physical, personal and organizational. Essentially, procedures or policies are implemented to tell administrators, users and operators how to use products to ensure information security within the organizations.

Various definitions of information security are suggested below, summarized from different sources:

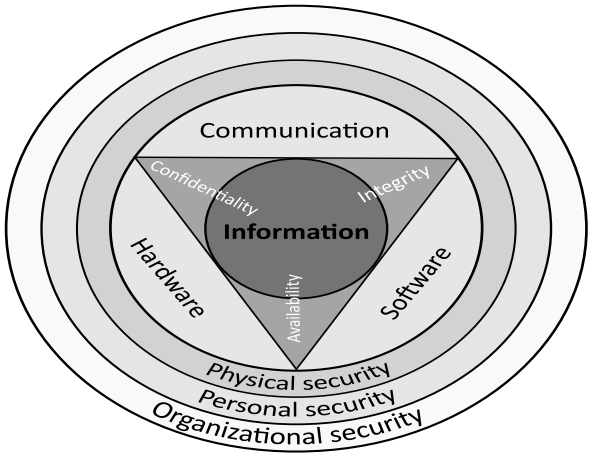

Figure 1. Visual Representation of The CIA Triad and Its Relationship to Information Assets, Security Layers, and Supporting Components.

a. "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2018)
b. Modern digital environments increasingly depend on cloud services, remote work systems, and mobile technologies, which expand the attack surface that organizations must secure (ENISA, 2023).
c. Organizations face more advanced cyber threats, including ransomware, supply-chain compromises, and AI-driven attacks, requiring adaptive and intelligence-based defense strategies (Verizon DBIR, 2023).
d. Security models are shifting from traditional perimeter defenses to Zero Trust approaches, where no user or device is inherently trusted inside or outside the network (NIST, 2020).
e. Recent trends highlight the need for continuous monitoring and real-time threat detection because modern cyberattacks spread faster and more aggressively than in the past (IBM Security, 2023).
f. Modern information systems must support rapid digital transformation, automation, and cloud integration, which increases the importance and its valuability of strong identity management and secure configurations (ENISA, 2023).
g. Human factors remain one of the largest security risks, as errors, weak passwords, and social engineering continue to be common points of failure (Verizon DBIR, 2023).
h. AI and machine learning are increasingly used to detect anomalies, predict attacks, and automate security incident response in modern organizations (IBM Security, 2023).
i. The financial and operational impact and effect of data breaches has grown worldwide, making cybersecurity a core component of organizational strategy rather than just an IT function (IBM Security, 2023).
j. Modern digital environments require strong privacy and data-protection measures due to increasing regulatory requirements and the growing volume of sensitive information being processed (NIST, 2020).
k. "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (CNSS, 2010)
l. "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (ISACA, 2008)
m. "Information Security is the process of protecting the intellectual property of an organisation." (Pipkin, 2000)
n. "...information security is a risk management discipline, whose job is to manage the cost of information risk to the business." (McDermott and Geer, 2001)
o. "A well-informed sense of assurance that information risks and controls are in balance." (Anderson, J., 2003)
p. "Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties." (Venter and Eloff, 2003)
q. "Information Security is a multidisciplinary area of study and professional activity which is concerned with the progression and augmentation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in

all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.

Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, theft of identity, theft of equipment or information, sabotage, and information extortion. viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses. Identify theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information through social Engineering. Sabotage usually consists of the destruction of an organization's website in an attempt to cause loss of confidence on the part of its customers. Information extortion consists of theft of a company's property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner, as with ransomware. One of the most functional precautions against these attacks is to conduct periodical user awareness.

Governments, military, corporation, financial institutions, hospital, non-profit organizations, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Should confidential information about a business's customers or finances or new product line fall into the hands of a competitor or hacker, a business and its customers could suffer widespread, irreparable financial loss, as well as damage to the company's reputation. From a business perspective, information security must be balanced against cost; the Gordon-Loeb Model provides a mathematical economic approach for addressing this concern. For the individual, information security has a significant effect on privacy, which is viewed very differently in various cultures.

Since the early days of communication, diplomats and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of correspondence and to have some means of detecting tampering. Julious Caesar is credited with the invention of the Caeser Cipher c. 50 B.C., which was created in order to prevent his secret messages from being read should a message fall into the wrong hands. However, for the most part protection was achieved through the application of procedural handling controls. Sensitive information was marked up to indicate that it should be protected and transported by trusted persons, guarded and stored in a secure environment or strong box. As postal services expanded, governments created official organizations to intercept, decipher, read, and reseal letters (e.g., the U.K.'s Secret Office, founded in 1653).

Figure 2. Biometric Eye-Scanning Technology

The purpose of this figure is to illustrate how biometric eye-scanning technology works as part of a secure authentication system.

In the mid-nineteenth century more complex classification system were developed to allow governments to manage their information according to the degree of sensitivity. For example, the British Government codified this, to some extent, with the publication of the Official secrets act in 1889. Section 1 of the law concerned espionage and unlawful disclosures of information, while Section 2 dealt with breaches of official trust. A public interest defense was soon added to defend disclosures in the interest of the state. A similar law was passed in India in 1889, The Indian Official Secrets Act, which was associated with the British colonial era and used to crack down on newspapers that opposed the Raj's policies. A newer version was passed in 1923 that extended to all matters of confidential or secret information for governance. By the time of the First world war, multi-tier classification systems were used to communicate information to and from various fronts, which encouraged greater use of code making and breaking sections in diplomatic and military headquarters.[] Encoding became more sophisticated between the wars as machines were employed to scramble and unscramble information.

The establishment of Computer security inaugurated the history of information security. The need for such appeared during World warII. The volume of information shared by the Allied countries during the Second World War necessitated formal alignment of classification systems and procedural controls. An arcane range of markings evolved to indicate who could handle documents (usually officers rather than enlisted troops) and where they should be stored as increasingly complex safes and storage facilities were developed. The Enigma machine, which was employed by the Germans to encrypt the data of warfare and was successfully decrypted by Alan Turing can be regarded as a striking example of creating and using secured information. Procedures evolved to ensure documents were destroyed properly, and it was the failure to follow these procedures which led to some of the greatest intelligence coups of the war (e.g., the capture of U-570.

Numerous mainframe computers were connected online during the Cold War to complete more sophisticated tasks, in a communication process easier than mailing magnetic tapes back and forth by computer centers. As such, the Advanced Research project agency (ARPA), of the United States department of depence, started researching the feasibility of a networked system of communication to trade information within the United States Armed forces. In 1968, the APPANET project was formulated by Larry Robert, which would later evolve into what is known as the internet.

In 1973, important elements of ARPANET security were found by internet pioneer Robert Metcalf to have many flaws such as the: "vulnerability of password structure and formats; lack of safety procedures for a dial of connections; and nonexistent user identification and authorizations", aside from the lack of controls and safeguards to keep data safe from unauthorized access. Hackers had effortless access to ARPANET, as phone numbers were known by the public. Due to these problems, coupled with the constant violation of computer security, as well as the exponential increase in the number of hosts and users of the system, "network security" was often alluded to as "network insecurity".

3. RESULTS AND DISCUSSION

The findings of this mixed-methods study highlight enough key patterns and points related to information security principles, ideas, organizational practices, and emerging threat landscapes. The qualitative analysis of literature, standards, and industry reports confirmed that the CIA triad, risk management processes, and security policy frameworks remain the

foundational pillars of modern information security. Major standards such as ISO/IEC 27001, NIST SP 800-series, and COBIT consistently emphasize structured controls, formalized security policies, and the integration of both technical and human-centered safeguards. Quantitative data collected through assesses and institutional assessments revealed notable gaps between theoretical best practices and their real-world augmentation. The quantitative assessment revealed several gaps between recommended best practices and real-world implementation. Many organizations have standard security measures such as firewalls and antivirus software, but far fewer have adopted advanced safeguards like infiltration detection systems, multi-factor authentication, or data loss prevention tools. Common security weaknesses included password reuse, limited awareness of organizational security policies, and frequent incidents such as phishing, malware infections, and unauthorized access attempts. Organizations with structured security training programs generally demonstrated stronger security practices than those without such initiatives. The findings also identified prevalent security incidents, with phishing, malware infections, and unauthorized access attempts reported as the most common threats. Organizations with structured security training programs experienced fewer incidents compared to those without training initiatives. The results indicate that while awareness of cybersecurity threats is increasing, practical implementation of advanced safeguards and user-centric security practices remains insufficient.

The results demonstrate a clear and insightful discrepancy between established information security standards and their on-ground adoption within organizations. Although frameworks such as ISO 27001 and NIST outline comprehensive control systems, the study found that many institutions rely primarily on basic protective and preventive tools, indicating a limited maturity level in their security posture. This is consistent with existing literature that highlights underinvestment in advanced security technologies despite the rise of sophisticated cyberattacks. The high rates of password reuse, limited awareness of policies, and frequent phishing incidents underscore the central role of human factors in security vulnerabilities. These findings support previous research asserting that human error remains one of the most significant contributors to data breaches. The fact that organizations with consistent training experienced fewer incidents reinforces the importance of ongoing education, behavioral awareness programs, and clear policy communication. Furthermore, the results suggest that despite the adoption of emerging technologies such as AI and machine learning, many organizations have not yet fully integrated these tools into their security frameworks. This may be due to cost constraints, lack of expertise, or resistance to technological change—factors also highlighted in prior studies on barriers to cybersecurity adoption. Overall, the findings emphasize that effective information security requires a holistic, multi-layered approach combining technical controls, strong security governance, trained personnel, and continuous risk assessment. Strengthening human-centered measures, improving policy implementation, and promoting compliance with international standards are essential for enhancing resilience in an increasingly interconnected and threat-prone digital environment.

4. CONCLUSION

This study talks about that information security maintains an essential and continuously evolving discipline that needs a balanced combination of technical solutions, organizational policies, and human-centered practices. The mixed-methods approach provided a broad fundamental understanding of how foundational principles such as the CIA triad, risk management processes, and structured security frameworks are recognized and shown across literature, standards, and professional guidelines, it is not yet uniformly augmented in organizational settings. A significant gap is revealed from results between theoretical best

practices and practical application. When many institutions have adopted basic protective measures, the augmentation of advanced security controls, such as security violation detection systems, multi-factor authentication, and automated threat analysis tools, remains limited. This gap increases exposure to common threats such as phishing, malware infections, and unauthorized access attempts. The findings further highlight that human factors including password misuse, lack of awareness, and insufficient training continue to be among the most persistent vulnerabilities. The study reinforces that technological advancements alone cannot sufficiently safeguard information assets. Effective information security requires strong organizational governance, continuous employee training, adherence to established international standards, and a proactive risk management culture. Organizations that integrate both human and technical defenses consistently experience fewer security incidents, demonstrating the need for a holistic approach to cybersecurity. In conclusion, powering information security requires a coordinated effort that brings people into agreement, processes, and technologies within a comprehensive security framework. As digital systems continue to expand and cyber threats grow more sophisticated, organizations must continually adjust to, invest in advanced security practices, and cultivate a security-aware culture. Doing so will enhance resilience, protect critical assets, and ensure the integrity and reliability of information systems in an increasingly interconnected world.

REFERENCES

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *Journal of Cybersecurity, 5*(1), tyz005. https://doi.org/10.1093/cybsec/tyz005

Hadlington, L., Ilett, R., Jach, H. K., & Curtis, N. (2023). Human factors in cybersecurity: The role of personality and digital-era risks. *Cyberpsychology, Behavior, and Social Networking, 26*(4), 280–287. https://doi.org/10.1089/cyber.2022.0120

Hsu, C.-L., Lin, J. C.-C., & Wang, Y.-H. (2022). Understanding information security policy compliance: A unified model integrating threat appraisal and organizational climate. *Information & Management, 59*(3), 103595. https://doi.org/10.1016/j.im.2021.103595

Lundgren, B., & Möller, N. (2017). Defining information security. *Science and Engineering Ethics, 25*(2), 419–441. https://doi.org/10.1007/s11948-017-9992-1

Meitarice, S., Febyana, L., Fitriansyah, A., Kurniawan, R., & Nugroho, R. A. (2024). Risk management analysis of information security in an academic information system at a public university in Indonesia. *Journal of Information Technology and Cyber Security, 2*(2), 58–75. https://doi.org/10.30996/jitcs.12099

Nugroho, F. R., Afiana, F. N., & Kuncoro, A. P. (2024). NIST Cyber Security Framework development for website information collection. *Jurnal Teknologi Sistem Informasi dan Aplikasi, 7*(3), 1335–1342. https://doi.org/10.32493/jtsi.v7i3.41541

O'Reilly, P., Rigopoulos, K., Feldman, L., & Witte, G. (2023). *2022 Cybersecurity & Privacy Annual Report (NIST SP 800-225).* National Institute of Standards and Technology. *(No DOI or public URL currently available — NIST has not published an official link for SP 800-225).* Cybersecurity Framework Review

O'Reilly, P., Rigopoulos, K., Witte, G., & Feldman, L. (2022). *2021 Cybersecurity & Privacy Annual Report (NIST SP 800-220).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-220

Schmidt, M. (2023). Information security risk management terminology and key concepts. *Risk Management, 25*(2). https://doi.org/10.1057/s41283-022-00108-8

Sharma, P., & Hespanha, J. (2020). Secure estimation subject to cyber stochastic attacks. In *Cloud Control Systems: Emerging Methodologies and Applications in Modelling* (pp. 373–404). Elsevier. https://doi.org/10.1016/b978-0-12-818701-2.00021-4

Somepalli, S. H., Mohammed, A. H., & Shaik, F. (2020). Information security management. *HOLISTICA – Journal of Business and Public Administration, 11*(2), 1–16. https://doi.org/10.2478/hjbpa-2020-0015

Taherdoost, H. (2022). Review of cybersecurity frameworks. *Electronics, 11*(14), 2181. https://doi.org/10.3390/electronics11142181

Torten, R., Reaiche, C., & Boyle, S. (2021). The impact of employee compliance with information security policies on cybersecurity effectiveness. *Information & Computer Security, 29*(3), 471–487. https://doi.org/10.1108/ICS-04-2020-0057