ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 6 / UIF:8.2 / MODERNSCIENCE.UZ

DIFFERENCES BETWEEN INFORMATION SECURITY AND CYBERSECURITY

G‘ofurova Laziza Jasur qizi
+99893-511-74-09. lazizagofurova52@gmail.com
Raxmonberdiyeva Sarvinoz Abdukarim qizi
+99894-002-55-34 sarvinozraxmonberdiyeva2@gmail.com
Students of Tashkent University of Information technologies
named after Muhammad al-Khwarizmi.

https://doi.org/10.5281/zenodo.15625675

Abstract. *Information security and cybersecurity are related but distinct concepts in protecting data. Information security focuses broadly on safeguarding information in any form (digital, physical, or intellectual) by ensuring its confidentiality, integrity, and availability. Cybersecurity specifically concerns the protection of computer systems, networks, and online data from cyber threats. This paper compares these fields in detail, providing definitions, key differences, and practical examples. Diagrams and tables illustrate how each discipline is applied in real-world scenarios. Understanding the difference helps organizations allocate resources appropriately and build effective security strategies.*

Keywords: *information security, cybersecurity, data protection, confidentiality, integrity, availability.*

Introduction

The terms “information security” and “cybersecurity” are often used interchangeably, but they have distinct meanings. Information security is a broad discipline concerned with protecting information assets in all forms and contexts. Cybersecurity is a specialized subset that focuses on protecting digital systems, networks, and data in cyberspace. This article analyzes the key differences between these fields, explains their overlapping concerns, and provides practical examples of each. By comparing their definitions, scopes, and applications, we clarify how organizations approach security in both physical and digital domains.

Information security is generally defined as the practice of protecting information by mitigating risks to its confidentiality, integrity, and availability. In other words, it aims to safeguard data in any form - digital, physical, or intellectual. For example, a company’s data stored on servers, in paper files, or even in an employee’s notes all fall under information security concerns. In particular, information security “is the practice of protecting information by mitigating information risks”, ensuring that unauthorized access, disclosure, or modification of data is prevented.

Cybersecurity is often viewed as a subset of information security focused on the digital realm. It involves protecting computer systems, networks, and electronic data from unauthorized access or damage. As one definition states, cybersecurity is “the practice of protecting systems, networks and programs from digital attacks”. This means guarding against threats like hackers, malware, and network intrusions that target online assets. In practice, cybersecurity deals specifically with securing anything connected to the Internet or cyberspace.

Some experts consider information security the broader “umbrella” because it covers any sensitive data, whereas cybersecurity deals only with data and assets accessible via information

and communication technologies (ICT). In this view, cybersecurity tasks (such as securing routers or cloud servers) fall within the larger mission of information security. However, both fields share common principles. For example, information security's focus on the CIA triad (Confidentiality, Integrity, Availability) applies across all areas, including the digital domain.

The above diagram illustrates the relationship between the two fields. On the left, information security covers protecting information in all forms (analog or digital); on the right, cybersecurity includes anything vulnerable through ICT. Both sets overlap in the digital realm, reflecting that securing online data is a concern shared by both disciplines. In both cases, the goal is to prevent unauthorized access and ensure that information remains confidential, accurate, and available.

Key Differences

Characteristic	Information Security	Cybersecurity
Scope	Protects information in all forms (electronic, physical, intellectual)	Protects systems, networks, and data in cyberspace (digital)
Focus	Overall data protection (CIA principles)	Threats from networked computers and Internet attackers
Typical Threats	Insider theft, physical loss, social engineering	Malware, hacking, denial-of-service, phishing
Controls & Tools	Policies, encryption, locks, access controls	Firewalls, intrusion detection, antivirus, secure coding
Examples	Locked file cabinets, data classification policies	Firewall configuration, patch management, network segmentation

The table above summarizes these contrasts. It highlights that information security spans a wider range of information assets (including printed documents and intellectual property), whereas cybersecurity is centered on digital information and IT infrastructure. Information security often emphasizes policies, training, and physical measures (e.g. locks or guards), while cybersecurity emphasizes technical defenses like firewalls, encryption, and malware detection.

For example, controlling who can access a secure vault or classifying documents is an information security task, whereas configuring a firewall to block hackers is a cybersecurity task. Both domains aim to preserve the confidentiality, integrity, and availability of data, but they apply different techniques given their different scopes.

These distinctions can also be illustrated by scenarios. A cyber attacker who hacks into a network or spreads a virus represents a cybersecurity incident, because the threat originates in the network or Internet. In contrast, if an employee leaks confidential printed records or loses a USB drive with sensitive data, that situation falls under information security, even if no network was directly involved. In practice, organizations must address both aspects: for instance, installing intrusion detection (a cybersecurity control) and enforcing strict file-handling policies (an information security control) to achieve comprehensive protection.

Despite these differences, information security and cybersecurity share many overlapping goals.

Both fields use risk assessment, access control, and incident response processes to protect data. In many organizations the same security team or framework covers both “analog” and “digital” threats, ensuring that policies (like data classification and access rights) extend from paper files to computer systems. Understanding the distinction between these terms helps allocate resources correctly: organizations can ensure they have both network defenses (cybersecurity) and data governance practices (information security) to keep all information safe.

To illustrate these concepts, consider two examples. First, a hospital implementing information security might enforce strict access controls and training for patient records: paper charts are locked in cabinets, and only authorized staff can view electronic health records. These measures protect patient information in all forms, not just online. Second, the same hospital’s cybersecurity efforts would include installing firewalls on its computer network, regularly patching its software, and using antivirus tools to prevent hackers from stealing or altering digital patient data. Both approaches protect medical data, but from different angles.

Another example is a corporate environment. An information security rule might prohibit employees from copying sensitive documents onto personal devices (a policy controlling data handling). A cybersecurity measure might be to monitor network traffic and block connections to suspicious websites (a technical control). Real-world cases emphasize the overlap: a phishing email (cyber threat) can lead to data exposure that is an information security breach. Thus, teams often handle incidents jointly, using both technical analysis and policy reviews to respond to attacks.

The integrated view is that information security sets the overall requirements (like encryption and user education) while cybersecurity implements specific digital solutions (like secure protocols and network segmentation). Policies such as ISO 27001 or NIST standards cover both domains, requiring controls for all types of information. For example, ISO 27001’s requirements for access control and incident response apply to both office documents and server data. In summary, effective security programs coordinate information security and cybersecurity to protect an organization’s data assets from every angle.

Conclusion

Information security and cybersecurity are complementary fields. Information security is concerned with protecting information assets regardless of medium, whereas cybersecurity focuses specifically on the computer and network environment. Both disciplines share the goal of keeping data safe, but they address different threat vectors and use different controls. By understanding their distinct roles, organizations can ensure they implement a full spectrum of defenses—from locking physical archives to securing online systems—so that all sensitive information remains protected under the principles of confidentiality, integrity, and availability.

REFERENCES

1. Amit, **CISO Platform**, “Understanding difference between Cyber Security & Information Security,” Jul. 2016.
2. GeeksforGeeks, “Difference Between Cyber Security and Information Security,” updated Apr. 15, 2025.

3. NIST, *NIST Special Publication 800-12 (Rev. 1): Introduction to Information Security*, 2017 (definitions of CIA).
4. University of San Diego, “Cybersecurity vs. Information Security vs. Network Security,” 6-min read (Michelle Moore, PhD).
5. Wikipedia, “Information security,” (accessed 2025).
6. Wikipedia, “Computer security,” (accessed 2025).