JISSec
Journal of Information Systems Security

THE INTELLECTUAL CORE OF INFORMATION SYSTEMS SECURITY

Gurpreet Dhillon

University of North Texas, USA

The Journal of Information Systems Security is a publication of the Information Institute. The JISSec's mission is to significantly expand the domain of information system security research to a wide and eclectic audience of academics, consultants and executives who are involved in the management of security and generally maintaining the integrity of the business operations.

Print ISSN: 1551-0123
Online ISSN: 1551-0808
Volume 19, Issue 2

www.jissec.org

This editorial note delves into information systems security's intellectual core. At the center of this concept is the crucial understanding of human activities and their significance in ensuring information protection. As we contemplate this matter, it becomes evident that every human activity, whether as humble as crafting a needle or as monumental as launching a space shuttle, relies upon two fundamental requirements: coordination and division of labor. These two elements define the nature of organizations, where the coordination of diverse tasks toward a meaningful outcome plays a central role. Communication, as the backbone of coordination, is the key to ensuring that various participants exchange information to achieve effective coordination. While computers can serve as facilitators in certain cases, in other situations, it may be more appropriate to rely on alternative means. Formal rules, policies, and procedures can establish coordination, while informal communication with other parties might be the preferred approach in specific scenarios. Purposeful communication harmonizes organizational activities and accomplishes shared objectives.

At the core of coordination and communication lies the indispensable role of information. Indeed, information acts as the binding force that keeps an organization intact. Thus, an organization can be defined as a series of activities revolving around the handling of information. In smaller organizations, managing information may be relatively straightforward. However, as organizations grow in size and complexity, the challenge of handling information becomes more cumbersome yet increasingly vital. Relying solely on informal roles and relationships is no longer sufficient to ensure efficient work processes. Instead, formal systems must be meticulously designed to not only promote consistent actions but also safeguard the integrity of information handling. As organizations expand, the systematic storage, retrieval, release, and collection of vast amounts of information become paramount. Mechanisms must be established to retrieve pertinent information and distribute it to the appropriate recipients. Often, networked computer systems serve as the facilitators for effective information handling. Consequently, information handling can be classified into three levels: technical, formal, and informal, with the combination of these levels comprising an organization's information system.

The concept of information systems security, therefore, encompasses safeguarding the technical infrastructure and protecting the formal and informal systems within an organization. It goes beyond ensuring the integrity of data stored in a computer-based system, as it involves upholding a set of values.

When we talk about a person of integrity, we refer to someone who cannot be swayed by corruption and adheres to a comprehensive system of values. While preventing unauthorized data modifications in a computer-based system is important, information systems security goes beyond that. It also focuses on the consistency of decision-making and the alignment of decisions with the organization's overall objectives. This entails considering how members of the organization interpret data and use that interpretation to guide their decision-making process. Thus, information systems security involves maintaining harmony between formally established systems of authority and information usage and the informal practices that exist in practice. Any discrepancies between these aspects can compromise the integrity and security of the entire organizational structure.

Our ability to effectively organize is closely linked to our competence in handling information. Information acts as the glue that holds organizations together and propels them forward. Consequently, organizations can be viewed as communication systems, and any disruption in the communication process can lead to security and integrity issues. The meanings attributed to actions and behavioral patterns within the organization have direct implications for information systems security.

Adverse events occur when inconsistencies arise regarding the expectations and obligations associated with different roles within the organization. This creates opportunities for individuals in certain roles to commit offenses. The occurrence of adverse events is rooted in the organizational culture and the normative structures in place.

Bringing it together, as the organizational landscape continues to evolve, information systems security must adapt to the shifting context in which data is interpreted and utilized. While traditional principles such as Confidentiality, Integrity, and Availability hold inherent value, it is important to recognize their limitations. These principles predominantly address data perceived as "data" stored within computer systems, focusing on preventing unauthorized disclosure, modification, and withholding of information or resources.

Key concerns that need consideration:

1. Confidentiality: Confidentiality revolves around restricting data access to authorized individuals. However, with advancements in technology aiming to facilitate broader data accessibility and organizational trends promoting less hierarchical structures, informality, and empowerment, striking a balance between accessibility and security become paramount. Achieving equilibrium between usability and security, convenience and security becomes crucial in this evolving context.
2. Integrity: Maintaining data integrity is of utmost importance, but it is equally critical to consider how data interpretation aligns with organizational norms. Businesses require employees who have the ability to accurately interpret processed and stored information and adhere to company policies and statutory requirements. Safeguarding "interpretation integrity" becomes pivotal in preventing misapplications and errors.
3. Availability: Availability entails ensuring continuous accessibility of systems when needed. While system failures pose security concerns, this principle generally generates fewer controversies within organizations compared to confidentiality and integrity.

However, confidentiality, integrity and availability need to be done RITE, which ensures the effective protection of information assets in the future. Organizations should consider embracing additional guiding principles: Responsibility, Integrity, Trust and Ethicality (RITE). Establishing a subculture that recognizes the indispensability of these principles lays a solid foundation for robust information security.

1. **Responsibility and Knowledge of Roles:** In organizations that are geographically dispersed, comprehending roles and responsibilities assumes paramount importance. As vertical management structures diminish in significance, empowerment takes center stage, necessitating employees to shape their work practices based on clearly defined responsibilities. Responsibility extends beyond being held accountable for past errors; it encompasses proactive management of future developments.

2. **Integrity as a Requirement of Membership:** The integrity of individuals as members of an organization holds great significance. Information has evolved into a critical asset, prompting organizations to carefully evaluate the individuals they admit into their fold. Once within, safeguarding and upholding integrity becomes imperative, as most security breaches originate from existing employees. Maintaining lofty ethical standards is pivotal in deterring fraud and fostering loyalty.
3. **Trust as Distinct from Control:** In contemporary organizations that prioritize self-control.
4. **Ethicality as a Guide, Not Just Rules:** Organizations must cultivate an ethical environment wherein members are expected to align their actions with informal norms and behaviors. While rules cater to formalized procedures and predictable circumstances, situations may arise where rules are absent. In such instances, ethical practices offer valuable guidance. The internet serves as a notable example where formal rules may be lacking, yet a robust set of norms has emerged through academic and research collaboration. Identifying and instilling the requisite ethics among both new and existing members assume critical importance for organizations.

Defining information systems and security has posed a persistent challenge over the years. While some equate information systems solely with computers, others adopt a broader perspective, encompassing organizational structures, business processes, and human involvement within the definition. Regardless of the specific orientation of these definitions, it is indisputable that our society's prosperity is deeply intertwined with our ability to organize, a feat accomplished through the skillful handling of information. The systems we create to manage information are, in many ways, the very fabric of organizations. This perspective resonates throughout the annals of management thinking, with notable figures such as Mary Parker Follett, Herbert Simon, and Peter Drucker emphasizing the pivotal role of information systems in organizations. I have previously discussed some these concepts in my previous writings as well, particularly Dhillon and Backhouse (2000) and Dhillon (1997).

Interestingly, the emerging principles defining information systems and security harken back to an era when there was no technology for close supervision and control of dispersed activities relying rather on individuals' elevated morality, integrity and ethics.

References

Dhillon, G. (1997). *Managing Information Systems Security*. Macmillan Palgrave, Basingstoke, UK.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125-128.

Gurpreet Dhillon holds the G. Brint Ryan Endowed Chair of Artificial Intelligence and Cybersecurity at the University of North Texas, USA. He also holds honorary appointments at the University of KwaZula-Natal, South Africa and Universidade de Lisboa (University of Lisbon], Portugal. Gurpreet earned a Ph.D. from the London School of Economics. He received an Honorary Doctorate from Örebro University, Sweden in 2019. Several of his research papers have been published in FT50 journals. Additionally, he has been featured in the Wall Street Journal, the New York Times, USA Today, Business Week, CNN, NBC News, and NPR.