JISSec
Journal of Information Systems Security

# COORDINATING IN THREES: UNRAVELING COMPLEXITY IN INFORMATION SYSTEMS SECURITY MANAGEMENT

**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 20, Issue 1

www.jissec.org

## Abstract

Defining an information system poses a multifaceted challenge, ranging from a technology-centric view to a broader perspective involving organizational structures, processes, and human dynamics. This editorial note explores the technical, formal, and informal components of organizations. It highlights the vital importance of safeguarding information systems for the organization's resilience. Delving into coordination within organizations, it centers on the tripartite formal, informal, and technical systems. Successful coordination hinges on the harmonious interaction of these subsystems, supporting organizational integrity and resilience.

**Keywords**: Information Systems Security Definition, Integrity, Coordination in threes, Technical controls, Formal controls, Informal controls, TFI model.

**What is information systems security?**

In the intricate and diverse landscape of human activities, from the most basic task of crafting a needle to the complexity of orchestrating a space shuttle launch, two fundamental principles reign supreme: coordination and the division of labor. These principles form the bedrock upon which organizations are built, shaping their essence, and delineating their operational fabric. At the center of effective coordination resides communication—a vital thread that interweaves organization elements and harmonizes collaborative efforts. Communication takes on various forms, sometimes involving computers to facilitate coordination. However, the coordination method is malleable, adapting to the specific context. It may manifest itself through the establishment of formal rules and procedures, or informal exchanges among participants. Regardless of the specific approach, the ultimate goal remains unwavering: to synchronize organizational endeavors in pursuit of shared objectives.

The crux of successful coordination and communication is encapsulated within information—an influential force that binds organizations together. Information serves as the lifeblood of an organization, propelling its actions, shaping its decisions, and underpinning its very existence. As organizations grow and become more complex, the management of information assumes paramount importance. While smaller entities may navigate the realm of information with relative ease, their larger counterparts grapple with data handling complexities. The transition from informal communication structures to formal systems becomes imperative, necessitating efficient systems design and implementation. These systems enforce consistent actions and safeguard information management integrity. Organizations need strategic mechanisms for storing, retrieving, and disseminating vast quantities of information. Networked computer systems play a pivotal role in this orchestration, heralding the advent of the organizational information system.

The definition of information systems security faces a range of interpretations. Some narrowly perceive it as a technology-driven entity, while others embrace a broader perspective that encompasses organizational structures, operational processes, and human dynamics. However, an undeniable truth remains – the prosperity of society rests upon our ability to organize effectively, a feat facilitated through adept information handling. This principle is championed by eminent management scholars such as Mary Parker Follett, Herbert Simon, and Peter Drucker. They emphasize the pivotal role of information in shaping organizations' landscapes. Communication and coordination, therefore, are central to information systems security

JISSec
Journal of Information Systems Security

### The TFI model

Despite being integral to the tapestry of organizations, communication and coordination need to be dissected, particularly for the constituent components – technical, formal, and informal (aka TFI). Communication and coordination navigate the intricate pathways of information management across these three tiers, revealing the nuanced dynamics that shape their functioning. At the heart of this exploration is a resounding premise: safeguarding information systems across all strata is an imperative step in fortifying an organization's resilience and longevity.

Therefore, organizations adopt a tripartite focus – centered on three coordinating systems: formal, informal, and technical. The formal system, anchored in consistency, propels organizations' operational machinery. It draws strength from external messages, often originating from suppliers, customers, or regulatory bodies. These messages are meticulously transcribed into the organization's internal formal systems, setting in motion a cascade of interconnected activities. This formal framework materializes tangible outputs – ranging from inventory reports to carefully crafted marketing strategies, all meticulously documented.

Simultaneously, the informal system functions in parallel – an arena where expanding organizations foster cohesion among diverse groups through informal channels. However, the coexistence of formal and informal systems can sometimes give rise to tensions, reflecting disparities in attitudes, objectives, and aspirations. This juncture marks the initiation of the concept of "coordination in threes." The metaphor of a fried egg – a yolk representing the technical system, the albumin layer symbolizing the formal system, and the egg white embodying the informal system – illustrates the delicate balance required for harmonious organizational functioning (see Figure 1).

In essence, successful coordination in an organizational context hinge upon the harmonious interaction of these three subsystems. They must work in tandem, underpinning organization integrity, cohesion, and resilience. Through this holistic lens, we peer into the intricate mechanics that drive organizations. We unveil the essence of coordination's multifaceted nature and its pivotal role in securing the intricate dance of information and action.

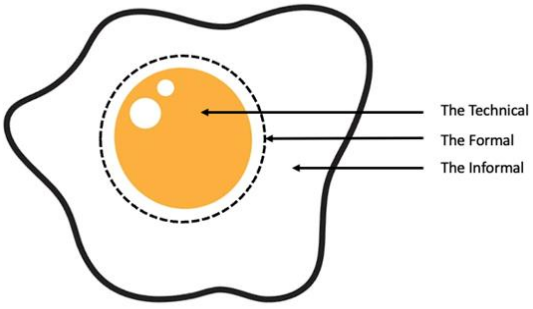


**Figure 1, Coordinating in threes**

***The "T" in the model***

So, what are technical controls? Today, businesses are actively embracing the concept of employing intricate technological measures to safeguard data stored in computer systems. Many of these measures revolve around access control and authentication. One particularly noteworthy advancement is the widespread adoption of smart card technology, especially in the financial sector. The authentication techniques have made significant strides. It is now widely acknowledged that relying solely on simple password protection falls short, prompting the necessity to verify an individual's identity (i.e., confirming if the user is who they claim to be). This requirement has been partially met through the utilization of sophisticated 'challenge-response box' technology. Other noteworthy developments include block ciphers for safeguarding sensitive data. Notably, message authentication has garnered considerable interest due to its practical applicability to the financial services and banking industry. Furthermore, the integration of methods like voice analysis and digital signatures has further enhanced security controls driven by technology. ICICI Bank in India, for example, incorporates a video of the individual when opening an account rather than static images. A random snapshot helps prevent fraud. Technological solutions nevertheless hinge on their ability to justify costs.

While technological controls play a pivotal role in establishing protective measures for sensitive information, skepticism exists regarding their overall effectiveness. Perpetrators often opt for the simplest, safest, and most straightforward means to achieve their objectives, rather than resorting to exotic and sophisticated methods. For instance, it is significantly easier for a criminal to gather information by eavesdropping on conversations or accessing written documents on paper. This is rather than electronic eavesdropping. In fact, there have been very few documented cases of radio frequency eavesdropping in the past four decades. Therefore, prior to implementing technological controls, business enterprises should carefully consider the establishment of well-designed baseline organizational safeguards, including processes such as vetting, responsibility allocation, and awareness initiatives.

***The "F" in the model***

Technological controls need adequate organizational support. Consequently, rule-based structures need to be implemented. These determine the consequences of misinterpretation of data and misapplication of rules in an organization and help in allocating specific responsibilities. At an organizational level, the development of a 'taskforce' helps in security management and gives strategic direction to various initiatives. Ideally the task force should have representatives from a wide range of departments such as audit, personnel, legal and insurance. Computer security professionals should provide ongoing support. Besides these, significant importance should be given to personnel issues. Failing to consider these adequately could have

disastrous consequences. Formal controls should not only address hiring procedures but also responsibility structures during employment. A clear understanding of responsibility structures helps in the attribution of blame, responsibility, accountability, and authority. It is undoubtedly without saying that employees' honest behavior is influenced by their motivation. Therefore, it is imperative to inculcate a sub-culture that promotes fair practices and moral leadership. However, the greatest care should be taken of employees' termination practices. It is a well-documented fact that most cases of information systems security occur shortly before the employee leaves the organization.

Finally, the key principle in assessing how much resources to allocate to security (technical or formal controls) is that the amount spent should be in proportion to the criticality of the system, the cost of remedy and the likelihood of a breach of security occurring. It is necessary for organizations to adopt appropriate controls to protect themselves from negligent duty claims and to comply with data protection legislation.

***The "I" in the model***

Enhancing awareness of security issues stands out as the most cost-effective measure an organization can implement. Frequently, information systems security is presented to users in a manner that exceeds their comprehension, serving as a deterrent to the adoption of adequate controls. Awareness elevation should be accompanied by an ongoing educational and training initiative. These training and awareness programs play a pivotal role in nurturing a 'trusted' core group within the organization. The primary focus should be on cultivating an organizational subculture that enables a clear understanding of management's intentions. This environment should also foster the development of a shared belief system, fostering commitment among organization members. This can be accomplished through sound management practices. Such practices hold particular significance in today's organizations, which increasingly outsource key services, leading to increased reliance on third parties for infrastructure support. This shift has implications for heightened dependency and vulnerability, elevating risks likelihood.

The initial step in establishing sound management practices and mitigating the risk of a security breach involves the adoption of baseline standards, as previously emphasized. Currently, the international community has taken concrete strides in this direction by formulating security standards. While compliance and monitoring issues may require further attention, these represent crucial steps in our pursuit of creating high-integrity, dependable organizations. However, compliance with a rule or a standard is not the *sine qua non* of a well-managed security program. Developing and sustaining a security culture is crucial.

**Putting it together**

In our ongoing discussion, we've delved into the intricate inner workings of organizations. We perceive them as complex entities comprised of technical, formal, and informal systems. Within this organizational framework, we've emphasized the pivotal role played by security controls operating at these three levels. This underscores the critical imperative of preserving the overall integrity of these systems and controls.

Our next logical step involves harnessing this understanding of the three organizational levels and their associated controls to unveil the vulnerabilities that can compromise an organization's security.

Organizational information handling is often encapsulated within an organizational structure, typically depicted through organizational charts. Although organizational charts serve as a common means to illustrate organizational hierarchies and functions, opinions regarding their usefulness vary. This variance stems from the difficulty of adequately representing informal information handling facets. In eras when computers were not central to the organization's operations, we heavily relied on formal bureaucratic procedures to manage information. Historical examples, such as the British Empire's governance of vast territories and the thriving cotton trade between 18th-century England and the US without technical systems, exemplify the necessity of intricate structures to comprehend their functions. Security measures at this level primarily revolved around associating access rights with hierarchical positions—an approach that thrived as organizational structures remained relatively stable over extended periods, with security primarily entailing physical locks and keys.

Efficiency stands as a paramount concern in organizational operations. Initially, certain formal activities received technological enhancements, like email and short message systems for communication. More recently, computers have played a central role, evolving from isolated entities within individual companies to interconnected systems spanning entire organizations. As technology has advanced, so too have the corresponding trust mechanisms, progressing from passwords to biometrics, with potential future developments on the horizon.

However, as our exploration delves deeper, we encounter the growing complexity of various social groups within organizations that engage in communication and share memberships. It becomes imperative to distinguish between formal and informal aspects, while contextualizing technical elements within this broader landscape. Security in this context hinges on maintaining consistent communication and accurate interpretation of information. Ethical considerations and trust-related issues gain significance.

Added another layer of complexity, organizations establish relationships with one another. Yet, at the core of all information handling, a pattern of coordination in threes remains prevalent, serving as a distinctive facet of security management. Armed with this foundational understanding and guided by our argument that information systems security revolves primarily around the management of integrity across these three levels, we embark on our exploration of issues and concerns related to information systems security management.

## Final words

When we conceptualize information systems security in terms of technical, formal, and informal systems, several significant aspects come to light. First and foremost, it highlights that security management extends beyond the confines of technical infrastructure. Secondly, it emphasizes the need to maintain the integrity of all three subsystems rather than showing favoritism towards one at the expense of the others. Thirdly, effective security management entails the proper integration of technical controls within formal controls. These controls fall within informal controls. Neglecting this integration can result in overly complex or insufficient solutions. Lastly, in today's era, where artificial intelligence plays a significant role, security management must accord equal importance to both technology actors and human agents. This underscores the socio-technical nature of the security challenge and the corresponding solution.

## Acknowledgements

Many of the concepts and ideas presented in this editorial note have previously been discussed by the author in various publications, including but not limited to: (Dhillon, 1995), (Backhouse & Dhillon, 1995), (Backhouse & Dhillon, 1996), (Dhillon & Backhouse, 1996), (Dhillon, 1997a), (Dhillon, 1997b), (Dhillon, 1999), (Dhillon, 2001), (Dhillon, 2004), (Dhillon, 2007), (Thomas & Dhillon, 2012), (Dhillon & Chowdhuri, 2014), (Dhillon, 2023), among others.

## References

Backhouse, J., & Dhillon, G. (1995). Managing computer crime: a research outlook. *Computers & Security*, *14*(7), 645-651.

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems*, *5*(1), 2-9.

Dhillon, G. (1995). *Interpreting the management of information systems security* [PhD, London School of Economics and Political Science, University of London]. London.

Dhillon, G. (1997a). The Clinical Information System: a case of misleading design decisions. In J. Liebowitz & M. Khosrowpour (Eds.), *Cases in information technology management in modern organizations* (pp. 275-287). Idea Group Publishing.

Dhillon, G. (1997b). *Managing information system security*. Macmillan.

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security*, *7*(5).

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security*, *20*(2), 165-172.

Dhillon, G. (2004). The Challenge of Managing Information Security. *International Journal of Information Management*, *24*(1), 3-4.

Dhillon, G. (2007). *Principles of information systems security: text and cases*. John Wiley & Sons.

Dhillon, G. (2023). The Intellectual Core of Information Systems Security. *Journal of Information Systems Security*, *10*(2), 91-95.

Dhillon, G., & Backhouse, J. (1996). Risks in the use of information technology within organizations. *International Journal of Information Management*, *16*(1), 65-74.

Dhillon, G., & Chowdhuri, R. (2014). Organizational Transformation and Information Security Culture: A Telecom Case Study. In S. Jajodia, F. Cuppens, & N. Cuppens-Boulahia (Eds.), *ICT Systems Security and Privacy Protection*. Springer.

Thomas, M., & Dhillon, G. (2012). Interpreting Deep Structures of Information Systems Security. *The Computer Journal*, *55*(10), 1148-1156.

**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.