JISSec
Journal of Information Systems Security

REDEFINING INFORMATION SYSTEMS SECURITY: A REFLECTIVE PERSPECTIVE

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 21, Issue 2

www.jissec.org

In this editorial note, I wish to engage with the definition of Information Systems (IS) security. This reflection stems from the vibrant discussions held at the 24th Annual Security Conference – a forum I founded over two decades ago to foster a community of shared inquiry. As I revisit those conversations, I find myself returning to a foundational question: What truly constitutes IS security? Is it merely about safeguarding data through confidentiality, integrity, and availability, as the traditional model suggests? Or does it call for a deeper, more nuanced understanding – one that sees security as an intrinsic element of organizational existence?

This is not a new line of contemplation. While developing my doctoral research in the mid-1990s, I grappled with the same conceptual challenge. My approach then was to first establish the broader context: clarifying what we mean by an organization, understanding the nature of information systems, and examining the role of computer-based information systems. Only by grounding the discussion in these fundamentals could a meaningful definition of IS security emerge.

Organizations: More Than Structures and Rules

Organizations defy simplistic categorization. Early efforts to analyze them through rigid, technical frameworks often produced incomplete or impractical conclusions. A more insightful approach recognizes organizations as dynamic, socially constructed entities where meaning is continually negotiated. They are not static hierarchies, but living systems shaped by interactions, power dynamics, and cultural undercurrents.

Historically, organizations were viewed as formal bureaucracies governed by rules and procedures. Yet this perspective overlooks the informal dimensions – the unspoken norms, relationships, and belief systems that profoundly influence how organizations operate. A true understanding requires acknowledging both the visible structures and the intangible forces that shape behavior.

Information Systems: The Lifeblood of Organizations

Information systems go far beyond hardware and software. They encompass the communication patterns, decision-making processes, and knowledge-sharing practices that define an organization's identity. Managing information effectively is not just a technical task – it is a core organizational competency.

As organizations grow, informal exchanges often give way to more structured systems. Technology facilitates this shift, but it is only part of the picture. The real challenge lies in balancing standardization with flexibility – ensuring that formal systems support, rather than suppress, the human elements that drive innovation and adaptability.

Computer-Based Systems: A Tool, Not a Solution

Computer-based information systems automate specific aspects of an organization's formal processes, but they cannot – and should not – replace the informal systems that foster creativity and sound judgment. Over-reliance on rigid digital frameworks risks creating dissonance, as employees bypass systems that feel disconnected from practical realities. The key is to discern which functions benefit from automation and which require the nuance of human discretion.sharing.

Security as an Organizational Value

If we embrace a broader view of organizations and information systems, then IS security must also extend beyond technical safeguards. It is not merely about firewalls and encryption – it is about cultivating a culture where integrity, accountability, and shared purpose are deeply embedded.

Security failures often stem not from technological weaknesses but from misalignments – between policy and practice, between roles and expectations, and between stated values and everyday behaviors. A rule may prohibit unauthorized data access, but true security depends on people understanding and believing in the principles behind that rule.

Security as a Cultural Imperative

Ultimately, IS security is inseparable from organizational culture. If we view organizations as networks of meaning, then security becomes a matter of preserving coherence – ensuring that communication flows effectively, roles are clearly defined, and values are consistently upheld.

As technology continues to advance, our understanding of security must evolve with it. We need to move beyond a narrow emphasis on technical controls and adopt a more holistic perspective – one in which security is woven into the very fabric of how organizations think, communicate, and function.

The Shift from Hierarchies to Networked Organizations

The traditional view of organizations as rigid, top-down hierarchies is increasingly obsolete. Today, organizations are better understood as dynamic, networked systems where power and decision-making are distributed rather than centralized. Early bureaucratic models, focused on formal rules and structures, failed to account for the informal relationships, cultural norms, and emergent behaviors that truly shape how work gets done.

Modern organizations resist simplistic categorization. They are fluid, socially constructed entities where meaning and authority are continually negotiated. Digital transformation, remote work, and decentralized collaboration tools have accelerated this shift, enabling flatter, more adaptive structures. Power no longer flows strictly from the top down but emerges through influence, expertise, and connectivity.

This networked organizational model thrives on flexibility, agility, and trust rather than rigid control. While hierarchies still exist in some contexts, the most resilient organizations today are those that embrace complexity – balancing structure with adaptability, formal policies with cultural cohesion, and centralized strategy with decentralized execution. The future belongs to organizations that operate as living systems, constantly evolving in response to internal and external forces.

Emergent Security Challenges

In today’s hyperconnected business world, speed and flexibility are everything. Hierarchies are dissolving, teams span continents, and innovation moves at a relentless pace. But with every layer of agility comes an undercurrent of risk – an uncomfortable truth that many modern organizations are only beginning to confront. The very traits that empower today’s companies are the same ones that leave them exposed.

The Illusion of Control

There was a time when businesses operated like well-oiled machines – with clear chains of command, uniform policies, and centralized security. That model is now giving way to a dynamic web of remote workers, autonomous teams, and global partnerships. Authority is dispersed. So is accountability. And, most dangerously, so is vulnerability. Without centralized oversight, security becomes a patchwork: one team follows protocols meticulously; another bypasses them under deadline pressure. A third-party vendor, far removed from core operations, leaves a door open. Everything seems to function – until it doesn't.

Shadow IT: Invisible Risks in Plain Sight

Productivity often breeds improvisation. In the quest to move faster, employees adopt tools outside the IT department's purview – unauthorized messaging apps, personal file-sharing platforms, even AI assistants. These tools help them work smarter, but they also create dangerous blind spots. If IT can't see them, it can't secure them – and hackers are quick to exploit what goes unnoticed. With remote work, the issue deepens. A personal laptop used to check work email on an unsecured network might be the weakest link in an otherwise robust chain – and the user may never realize they've handed over the keys.

The High Cost of Trust

Collaboration is the heartbeat of networked organizations. Teams share freely, communicate informally, and move quickly – fueled by mutual trust. But trust, when unchecked, becomes a double-edged sword. An employee clicks a phishing link and compromises the entire team. A departing contractor walks away with confidential data. A hacker impersonates a colleague in a chat and spreads malware with a single click. The more open the system, the more easily threats – whether intentional or accidental – can slip through.

Security That Can't Keep Up

Innovation rarely waits for permission. New platforms, tools, and technologies are rolled out at breakneck speed, while cybersecurity teams scramble to keep pace. A newly deployed app may carry a critical vulnerability. A rushed API integration might expose customer data. Security becomes a game of whack-a-mole – and the moles are multiplying.

Security vs. Productivity: A Culture Clash

To many employees, security feels like a roadblock. Multi-factor authentication slows them down. Encryption complicates collaboration. So, they seek workarounds – weak passwords, unauthorized apps, disabled protections. Not out of carelessness, but necessity. They're trying to do their jobs. And this leaves cybersecurity teams battling not just external threats, but internal resistance.

The Domino Effect of Third-Party Risk

No organization stands alone. Vendors, cloud services, APIs – each is a thread in the fabric of daily operations. But every connection is also a potential breach point. History offers cautionary tales: a major retailer brought down by an HVAC vendor; a global cyberattack seeded through a trusted software update. In today’s networked world, your security is only as strong as your most vulnerable partner.

Rethinking Security for a Networked Age

The fortress model – build walls, keep threats out – is no longer enough. Modern cybersecurity demands a mindset shift:

- **Zero Trust Architecture** means assuming every request is untrustworthy until verified, every time.
- **Behavioral AI** watches for subtle anomalies – odd login patterns, unusual data transfers – that could signal trouble.
- **Security-by-Culture** makes protection seamless. Reward safe behavior. Empower employees to see security as a catalyst, not a constraint.
- **Automated Enforcement** adapts in real-time – revoking unused permissions and enforcing policies before humans can react.
- **Collaborative Defense** ensures that when one organization is attacked, others are alerted instantly. No one should face threats alone.

Striking the Balance

Modern organizations won’t return to the old ways. They shouldn't. Flexibility and speed are too valuable. But with freedom must come responsibility. With autonomy must come accountability. The future of cybersecurity isn’t about slowing things down. It’s about building defenses that move just as fast – and bend without breaking.

Adapt. Or fall behind. The choice is ours.

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 PhD 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.