Gurpreet Dhillon and James Backhouse

Information System Security Management in the New Millennium

Future users of information systems must address organizational problems at a time when the organizational form is being revolutionized.

Rapid advances in electronic networks and computer-based information systems have given us enormous capabilities to process, store, and transmit digital data in most business sectors. This has transformed the way we conduct trade, deliver government services, and provide health care. Changes in communication and information technologies and particularly their confluence has raised a number of concerns connected with the protection of organizational information assets. Achieving consensus regarding safeguards for an information system, among different stakeholders in an organization, has become more difficult than solving many technical problems that might arise. This "Technical Opinion" focuses on understanding the nature of information security in the next millennium. Based on this understanding it suggests a set of principles that would help in managing information security in the future.

A Vision of the Future

Against the backdrop of the electronic age, new organizational structures are emerging. Increasingly we are seeing the advent of strong external coalitions that are transforming traditional monolithic, centralized, and hierarchical organizations into loosely coupled organic networks. These organizational forms are characterized by cooperation instead of autonomy and control. Consequently, the structures facilitate intense sharing of information and a high level of interpersonal and inter-organizational connectivity. Organizations are no longer characterized by physical assets but by a network of individuals who create, process, hold, and distribute information. Such organizations are "location and structure-independent" [6, 8] and are constantly influenced by the changing nature of their environment. This pushes them to make collaborations within and beyond the confines of their firm [3, 9]. These collaborations are supported by both electronic and human networks. Increasingly individuals and companies are setting up such "transnational networks that pay absolutely no heed to national boundaries and barriers" [1].

In order to be more efficient, effective, and responsive organizations give prominence to the use of networks and computer-based information systems. Yet the use of information and communication technologies have increased the incidents of computer abuse. A recent Computer Security Institute survey suggested losses of $124 million in the sampled companies. In England the Audit Commission estimated losses to the order if nearly $2 billion. Indeed losses of such magnitude demand serious consideration of the premises on

which information security is designed.

Facing pressures of organizational cost containment and external competition, many companies are rushing headlong into adopting IT without carefully planning and understanding the security concerns. Organizations are still trying to cope with the intricacy and mystique that surrounds computer systems. It appears less security is applied to data held in computer systems than is the case for data held in manual systems. Office workers are familiar with the security requirements of a filing cabinet but not necessarily those of an information system [5]. In the corporate world, information security is generally seen as being of interest to the IT department, and so many professionals do not give adequate importance to the security concerns of an organization. Even if they do, they come up with over-complicated solutions. Indeed the widespread use of IT by businesses today has given rise to "security blindness" on part of the users.

A vision of the future suggests a borderless global economy, enabled by technology and run by the so-called knowledge workers. Such knowledge workers do not have allegiance to companies or even countries. They move to wherever the best opportunities exist. A more realistic view of the future is that of chaos created by economic reorganizations and breakdown of political and social structures. In fact the new winners could be the organized crime organizations, such as the Mafia, the Columbian drug cartels, and the Japanese Yakuza. It is alleged that in 1990 the Yakuza made a profit of nearly $7 billion, far more than the earnings of a major commercial city. Indeed the fear of tomorrow is the highly sophisticated and educated criminal who can wield the state-of-the-art technology to his or her best advantage [7].

In light of the turbulent future and the existing competitive trends faced by the organizations, security managers hold the key to success or failure of a company's well being. The very role of a security manager is evolving. Organizations can no longer be interpreted in terms of technical installations and their functionality. The focus is shifting so as to consider the wholeness and soundness of information systems and the organization [2, 4]. Consequently a security manager will have to take on the role of maintaining integrity of the organizational infrastructure (not just the technical information systems). Such a move would minimize the prospect of plagiarism, fraud, corruption or loss of data, and the improper use of information systems that could affect the privacy and well-being of all concerned.

In such an environment we do not need excessive rules telling us how to behave in particular circumstances. What we need are principles that require observance at all times, and especially when there may not be any relevant rules to follow. Principles are quintessentially human and social attributes and the reason we are introducing them here is because the question of computer security is not, per se, a technical problem. It is a social and organizational problem because the technical systems have to be operated and used by people. Computer science has little to offer us in this regard. We need to look to organizational theory, management science, and the developing field of information systems instead, for aid and succor in combating the threats to security.

Information Security Principles for the Next Decade

Information systems security will have to address not just the data but the changing organizational context in which it is interpreted and used. The traditional information security principles of confidentiality, integrity and availability are fine as far as they go, but they are very restricted. They apply most obviously to information seen as "data" held on computer systems where confidentiality is the prevention of unauthorized disclosure, integrity the prevention of the unauthorized modification, and availability the prevention of unauthorized withholding of data or resources.

Issues of concern. Confidentiality refers mostly to restricting data access to those who are authorized. The technology is pulling very hard in the opposite direction with developments aimed at making data accessible to the many, not the few. Trends in organizational structure equally tug against this idea—less authoritarian structures, more informality, fewer rules, empowerment.

Integrity refers to maintaining the values of the data stored and manipulated, such as maintaining the correct signs and symbols. But what about how these figures are interpreted for use. Businesses need employees who can interpret the symbols processed and

Facing pressures of organizational cost containment and external competition, many companies are rushing headlong into adopting IT without carefully planning and understanding the security concerns.

stored. We refer not only to the numerical and language skills, but also to the ability to use the data in a way that accords with the prevailing norms of the organization. A typical example is checking the creditworthiness of a prospective loan applicant. We need both data on the applicant and correct interpretation according to company rules and for that matter statutory requirements. A secure organization not only needs to secure the data but also its interpretation.

In June 1994, London police arrested a gang of fraudsters who managed to defraud the Department of Social Security of more than $3 million by assuming 2,000 different identities, supported by a welter of stolen and forged documents, including passports, driving licenses, and birth certificates. There was nothing wrong with the integrity of the data. But the benefit rules were misapplied so that rightful claimants did not receive their due payments, or they went to the wrong ones. It was entirely a problem of interpretation. In such situations what's needed is the maintenance of "interpretation integrity."

Availability refers to the fact that the systems used by an organization remain available when they are needed. System failure is an organizational security issue. This issue, although not trivial, is perhaps less controversial for organizations than the previous two principles.

Some Additional Principles: RITE

What we suggest for consideration are some further principles without which future organizations are doomed. Inculcating a subculture where *r*esponsibility, *i*ntegrity, *t*rust and *e*thicality (RITE) are considered important and are the first steps in securing the information assets of the organization in the future.

Responsibility (and knowledge of roles). In a physically diffuse organization it is ever more important for members to understand what their respective roles and responsibilities should be. Today vertical management structures are disappearing as empowerment gains in stature as a more effective concept for running organizations well. Furthermore, members are expected to develop their own work practices on a basis of a clear understanding of their responsibilities.

So being responsible means not just carrying the can for when something has gone wrong in the past (accountability—for attributing blame) but refers also to handling the development of events in the future in a particular sphere. This is especially important for dealing with new developments that call for ad hoc responsibilities not catered for in the company hierarchy or organizational chart. If some new circumstance has arisen and someone has to take charge of it, who should it be? The modern organization needs the right person to take up the burden unsolicited.

Integrity (as requirement of membership). Integrity of a person as a member of an organization is very important. Information has become the most important asset/resource of organizations. It has properties that are peculiar—you can divulge information to a third party without removing it from where it came, and without necessarily revealing you have done so. Business-sensitive information has great value, and organizations need to consider whom they allow to enter the fraternity. But cases still abound where new employees are given access to sensitive information without their references being properly checked.

Once members are inside, the organization needs to consider how to maintain and uphold integrity. A person of integrity does not always remain so. The vast majority of breaches of systems security come from existing employees. Pressures can change individuals; marital, financial, medical problems can all play their part, sometimes in combination. Office romances are common backdrops for internal computer frauds; money is useful to impress or to keep two households going.

There has been a lowering of ethical standards generally in recent years eliminated perhaps in part by the loss of middle management job tenure, resulting

in an increase in fraud. Unswerving loyalty to the employer can no longer be assumed or taken for granted, and yet remains a prize for those fortunate organizations who can claim it. Elaborate systems of control are much more expensive; informally secure arrangements come free.

Trust (as distinct from control). In modern organizations where the emphasis is less on external control and supervision and more on self control and responsibility, there have to be mutual systems of trust. Division of labor demands that your colleagues should be trusted to act in accordance with company norms and accepted and agreed patterns of behavior. Appropriate levels of confidentiality as well as ethical practice must be expected of the bona-fide member.

Close supervision is less viable so trust must act as the cohesive element in a geographically diffuse organization. Although the notion of trust has been used to describe the security architecture of computer systems (for instance, the Trusted Computer System Evaluation Criteria), we need to inject this notion into organizational theory surrounding secure information systems.

One interesting concept has emerged in this regard—the half-life of trust. Just as radiated objects retain a half-life of radiation for some time after the initial event, so too exists a half-life of trust that lasts for some time after the physical face-to-face encounter that generated it has occurred. Members of a project group discuss how to tackle a task and allocate responsibilities before going off to their various locations to communicate later at a distance. At a certain point the trust established among them will evaporate and a further face-to-face encounter is required. This is typical of a virtual organization of the future—only up to a point.

Ethicality (as opposed to rules). We presuppose (or want to be able to) that fellow members will act in accordance with some ethical practices. These are not the company rules that can be applied to all formalized procedures. What we're referring to is the ethical content of informal norms and behavior. Rules apply in foreseen and predictable circumstances and cannot be invoked in new and dynamic situations. In many contexts there simply are no rules. An interesting example of this is the Internet itself. There are no rules governing how the Internet is used. There is no governing body. The U.S. as chief subsidizer pulled out in 1991 and left an organization ungoverned. And the Internet has positively thrived. However, there is a very strong set of working norms that has emerged through the years of academic and research collaboration, and those norms have developed a syntax for Internet communications and also restraints on the kind of permissible communications. The problem is where do new and existing members get the ethics organizations need now more than ever?

Conclusion

In addition to confidentiality, integrity, and availability (CIA), the responsibility, integrity, trust and ethicality (RITE) principles hold the key for successfully managing information security in the next millennium. However, users will have to be wary of the manner in which these principles are implemented. While technical controls are vital, especially with regard to who accesses computer systems and to what they are allowed to do once admitted, sophisticated future users of information systems will have to address the organizational problems at a time when the form the organization takes is being revolutionized. Ironically, the principles that seem to be emerging harken back to earlier times when the technology for close supervision and control of dispersed activities was nonexistent, an era when people had high morality, integrity, and ethics. ■

GURPREET DHILLON (dhillon@nevada.edu) is an assistant professor in the College of Business at University of Nevada Las Vegas, NV.

JAMES BACKHOUSE (j.p.backhouse@lse.ac.uk) is a senior lecturer in the Information Systems Department at the London School of Economics.

REFERENCES

1. Angell, I.O. Winners and losers in the information age. *LSE 7*, 1, (1995), 10–12.
2. Angell, IO. Computer security in these uncertain times: the need for a new approach. In *Proceedings of The Tenth World Conference on Computer Security, Audit and Control, COMPSEC*, London, UK (1993), Elsevier Advanced Technology, pp. 382–388.
3. Brynjolfsson, E. and Mendelson, H. Information systems and the organization of modern enterprise. *J. Org. Compu. 3*, 3 (1993), 245–255.
4. Dhillon, G. and Backhouse, J. Risks in the use of information technology within organizations. *Int. J. Info. Manag. 16*, 1, (1996), pp. 65–74.
5. Dunn, R. Data integrity and executive information systems. *Comput. Cont. Q. 8*, (1990), pp. 23–25.
6. Keen, G.W. *Shaping the Future: Business Design Through Information Technology*. Harvard Business School Press, Boston, Mass., 1991.
7. Moore, Jr., R.H. Wiseguys: Smarter criminals and smarter crime in the 21st century. *Futurist 28*, 5, (1994), 33–37.
8. Negroponte, N.P. Products and services for computer networks. *Scientific American* (Sept. 1991).
9. Reich, R.B. *The Work of Nations*. Vintage Books, New York, 1992.