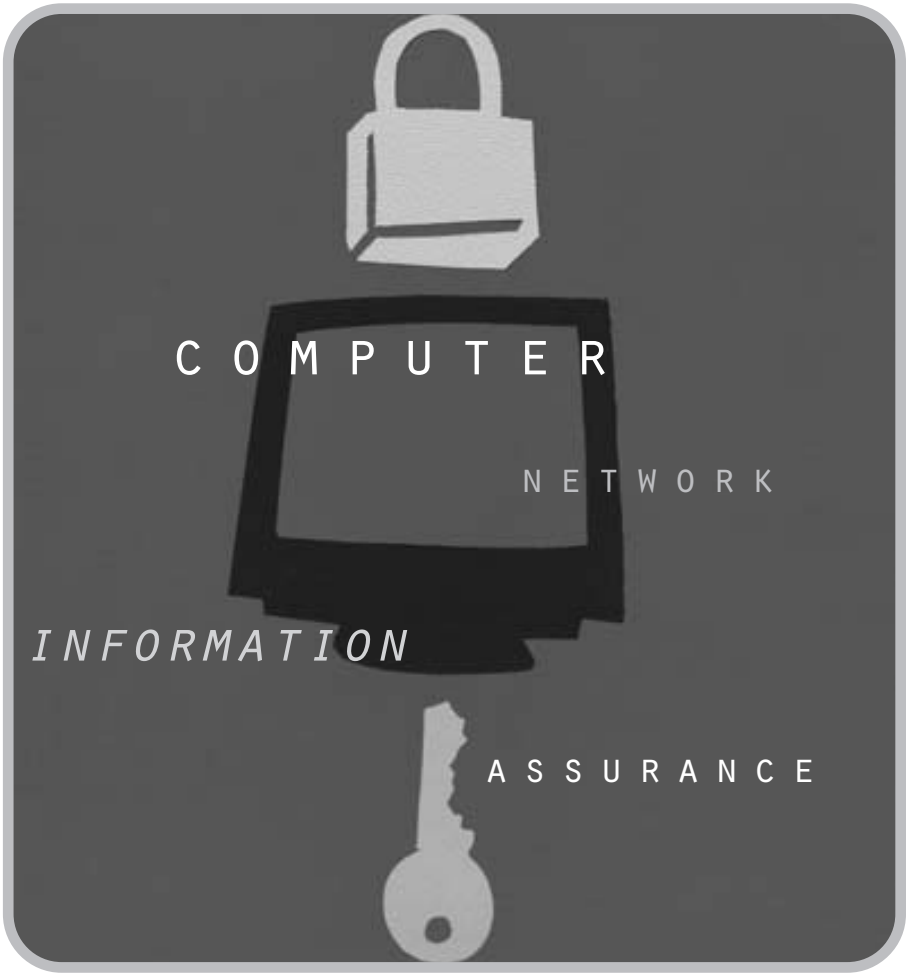
What's in a Name?

The labels associated with security—computer, network, information, information assurance—have multiple implications for higher education

By **Rodney Petersen** with **Ronald Larsen, Corey Schou,** and **Lee Strickland**

As colleges and universities attempt to ramp up the security of their computer networks, a common strategy has been to employ dedicated security staff and establish a central IT security office. Additionally, the Gramm-Leach-Bliley Act[1] requires the development of "a comprehensive information security program." And there has been an increased emphasis on personal safety, physical security, and the protection of critical infrastructures since 9/11. Yet, a diverse set of job titles, an array of segmented job functions, a range of reporting relationships, and a plethora of organizational models are found in colleges and universities to describe how they are approaching the privacy of data and personal information, security of computers and networks, and protection of intellectual property or other assets of the institution.



According to an October 2003 study by the EDUCAUSE Center for Applied Research,[2] 22.4 percent of higher education institutions have a chief IT security officer or the equivalent. Of those, 95 percent report to a senior administrator in the IT office, including 50 percent who report to the CIO. The ECAR study revealed a clear, steady pattern of growth for the creation of IT security officer positions in higher education beginning in 1994. It is not surprising that this evolutionary process sees campuses struggling with job titles and reporting structures for the newly conceived positions in IT security. In fact, similar dilemmas face industry and government. The Global Council of CSOs has established as one of its objectives to "define the proper role, background, and reporting arrangements for CSOs within business organizations."[3]

The issue of nomenclature is compounded in institutions of higher education because academic programs designed to educate the next generation of security professionals increasingly fall under the label of "information assurance" education and training. For example, more than 50 colleges and universities have been designated as Centers of Academic Excellence in Information Assurance Education by the National Security Agency.[4] Combined with the confusion generated between the title "IT security officer" and the role traditionally assumed by campus public safety or police departments (often staffed by security officers), cam-

pus telephone operators must be puzzled when they get external requests related to "security."

Different Viewpoints

What lies behind the evolution of these terms? What implications do the varying titles and terms have for the related academic disciplines and operational roles? How can colleges and universities collectively get ahead of the confusion by developing a vocabulary that constructively addresses the underlying foundations of the profession and the long-term needs of the academy? Some academic experts in diverse disciplines provide their perspectives on these issues here.

Ronald L. Larsen, Dean, School of Information Sciences, University of Pittsburgh:

The definitions of various terms are not standardized. Information security and computer security are often used as synonyms. While many feel information security is a more encompassing term, others are attracted to the perceived greater technical specificity of computer security. Information assurance, while slowly gaining acceptance, is still not clearly distinguishable from the term information security. This confusion can be seen, for example, in the name of Purdue University's Center of Education and Research in Information Assurance and Security (CERIAS), a well-known leader in this emerging discipline. The name suggests that information assurance and security are distinct, nonoverlapping concepts.

The term computer security has traditionally emphasized protection of computer system resources and operations. Although protection of information is addressed and is particularly visible in some security models (such as information flow models), it has not been the primary objective. Traditional computer security concepts implicitly assumed a more centralized, single-system approach in contrast to the networked, distributed systems spanning multiple administration domains that we see today. With the development of networking technologies (particularly, the Internet) and the growing reliance

Absolute security is not practically achievable, despite early definitions of security that included security assurance as a goal.

on computer infrastructures for processing information, network security and information security have become more widely used terms.

There is also a distinction made between database security and communications security. The database security community employed security models to address protection of [stored] information, whereas the communications security community used encryption mechanisms and cryptography to protect information in transit. Early uses of the term "computer security" were associated with problems of database security, whereas communications security was more closely associated with network security and cryptography. The phrase information security is now being more widely adopted, as it recognizes a broader understanding of information protection requirements, whether stored or in transit. Nonetheless, network security remains largely the term of preference as a more specific, technical, and marketable term than information security.

Security professionals are coming to understand that information security is a multifaceted problem, including nontechnical factors that contribute to ensuring the protection of information systems. "Information assurance" captures this broader notion of assuring that information is well protected and reliably available. It also addresses the realization that absolute security is not practically achievable, despite early definitions of security that included security assurance as a goal.

Lee Strickland, Professor, College of Information Studies, and Director of the Center for Information Policy, University of Maryland:

From a definitional, practical, and historical perspective, the terms computer security, network security, information security, and information assurance must be considered in context—understanding that no common vernacular exists within the security community. As such, definitions and usage tend to be vague at times and quite variable. For example, network security generally is considered to address the protection of data in motion and would include physical protection, policy protection, and technical protection by means such as encryption. Yet today, networks are an intrinsic part of computer systems, and thus network protection could be subsumed within the more general term of computer security.

Similar debate could occur over the terms computer security and information security. Does the former include the latter? Or does it depend on perspective and context? For example, a policy, legal, or information management expert will identify with the information security term, thinking in terms of protecting sensitive government or business information from unauthorized access, or from authorized access but unauthorized dissemination. Even here, focus can become diffused because information security also has a significant personnel security component as well as a physical security component and is equally concerned with inchoate knowledge, paper documents, and electronic information. A computer security expert will typically think in terms of unauthorized access to corporate electronic systems, from the inside or outside, with the intent to cause damage or access information, but the focus is the

security of, and hence access to, the electronic systems. This is not to suggest some rigid dichotomy between the terms because there is not; it is simply to suggest that context and focus are critical in determining the meaning.

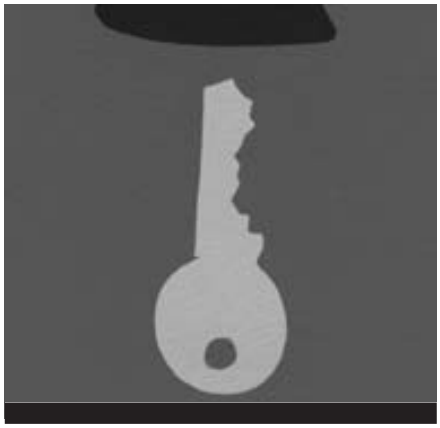
The one term that is well defined is information assurance. Arising in the defense and intelligence world, information assurance encompasses the policies and activities needed to ensure the objectives generally known as the "five pillars" of information assurance—availability, integrity, authentication, confidentiality, and nonrepudiation of information systems.

As we have considered, the security of electronic systems and information is better understood in terms of functions than terminology, which tends to be vague and have inconsistently utilized definitions. What is important today is the realization that the computer system, the network, and the information are essentially intertwined for purposes of security. For example, encryption is no longer just an issue for network operations—it is as important when information is at rest as when it is in motion. It follows in my judgment that the term information assurance, defined as I have, properly encompasses the unity of systems, networks, and information today.

Corey Schou, Professor, National Information Assurance Training and Education Center (NIATEC), Idaho State University:

An abstract research and pedagogic framework for the INFOSEC [information systems security] discipline was introduced by John McCumber in 1991.[5] It represented an attempt to integrate heretofore separate disciplines such as personnel security, computer security, communications security, and operational security into a coherent identifiable profession. Historically, information systems security came to be defined as

> Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.[6]



All organizations should view information assurance as a planned, integrative, systematic objective at the highest level.

In today's information-intensive environment, security professionals have expanded the scope and thus the understanding of information and systems protection under an umbrella term referred to as information assurance. The National Security Telecommunications and Information Systems Security Committee (NSTISSC) and the Committee on National Security Systems (CNSS) define information assurance as

> Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.[7]

Information assurance is both art and science; it is an interdisciplinary activity that protects the most complex organizational asset—its data and the systems upon which that information resides and is produced. Most organizations profess an interest in some aspects of information assurance; however, all organizations should view information assurance as a planned, integrative, systematic objective at the highest level.

Conclusion

What's in a name? The evolution of terms appears to reflect a changing landscape, largely influenced by rapid developments in technology and the maturity of a relatively young profession and an emerging academic discipline. The differences also seem to reflect the different lens applied by experts from diverse fields such as computer science, business and management, information policy, public policy, and law. These differing viewpoints have implications for practice in institutions of higher education.

First, the confusion, at least for practitioners, will only get worse if there are not efforts, most likely led by members of the academic community, to generate greater consensus around terminology and models that resonate with the broad range of constituents, including scholars and security practitioners from both the public and private sectors. Because of the interdependencies involved across sectors, it will be useful to have a common framework or language by which security professionals can communicate and exchange information.

Second, the focus on the security of computers and networks versus the security of information or other organizational assets will likely dictate where security professionals are positioned in the campus organization and to whom they report. The continuing emphasis on computer and network security is likely to result in the establishment of IT security officers who are part of the IT organization, reporting to the CIO or directors of networking or IT systems. Information security or information assurance functions cut across the organization of campus administrations and will require extensive partnerships among the various campus stakeholders. Alternatively, they will require the establishment of a hybrid organizational structure led by professionals who are given the appropriate authority and who are perceived as neutral advocates for advancing effective security practices, similar to the manner in which institutions position auditors, compliance officers, or ombudsmen.

Finally, information assurance needs to be tackled through multidisciplinary efforts. In particular, the legal, ethical, social, and economic aspects of information assurance are particularly significant and relatively unexplored. Creation of multidisciplinary centers and collaborations among information assurance centers—and with information assurance practitioners—to conduct research and development in information assurance are crucial if we are to realize broad acceptance and achieve significant progress in this field. *e*

Endnotes

1. The Gramm-Leach-Bliley Act was passed by Congress in 1999 to protect the privacy and security of customer financial information. For more information, see <http://www.educause.edu/issues/issue.asp?issue=glb> (accessed June 16, 2004).
2. R. B. Kvavik et al., *Information Technology Security: Governance, Strategy, and Practice in Higher Education* (Boulder, Colo.: EDUCAUSE Center for Applied Research, Research Study, Vol. 5, 2003); <http://www.educause.edu/asp/doclib/abstract.asp?ID=ERS0305> (accessed June 15, 2004).
3. See <http://www.csocouncil.org/> (accessed June 15, 2004).
4. See <http://www.nsa.gov/ia/academia/caeiae.cfm> (accessed June 15, 2004).
5. J. McCumber, "Information Systems Security: A Comprehensive Model," in *Proceedings 14th National Computer Security Conference* (Baltimore, Md.: National Institute of Standards and Technology, October 1991).
6. CNSS Instruction 4009, "National Information Assurance Glossary," Committee on National Security Systems, May 2003. Formerly NSTISSI 4009 (National Security Telecommunications and Information Systems Security Committee). See <http://www.nstissc.gov/Assets/pdf/4009.pdf> (accessed June 16, 2004).
7. Ibid.

Rodney Petersen (rpetersen@educause.edu) is a policy analyst and Security Task Force Coordinator for EDUCAUSE.