

An Exciting Program Essential for National and Organizational Security

Glenn A. Dunki-Jacobs Chair of Department of Technology at Mt. Sierra College speaks about Information Security

Glenn A. Dunki-Jacobs joined Mt. Sierra College in 1997 and currently serves as the Department Chair of Technology. He has more than 22 years experience as a college instructor and in business. Dunki-Jacobs earned his bachelors degree from the University of Texas in Austin, Texas.

Dunki-Jacobs currently serves as a consultant to businesses in the Southern California area.

[QUESTION] Please give us a briefing on Information Security.

[Glenn A. Dunki-Jacobs] Information security, or sometimes Information Systems Security (INFOSEC), deals with several aspects of information and its protection. Another similar term is Information Assurance (IA), but INFOSEC is a subset of IA. In theory, information security is not necessarily confined to computer systems, nor to information in an electronic or machine-readable form. The term applies to all areas of safeguarding information or data, in whatever form. The U.S. Government's National Information Assurance Glossary defines INFOSEC 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 or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

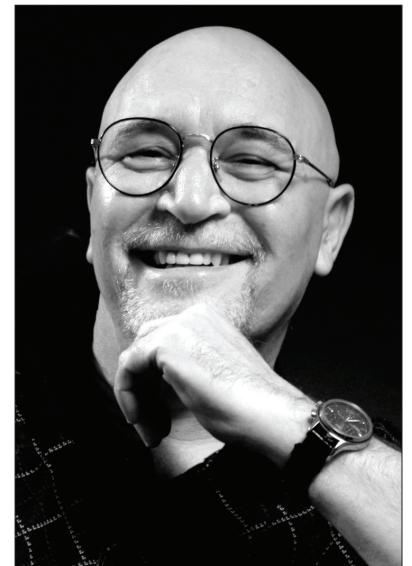
[Q] Is there often a misconception about the definition of Information Security?

[GDJ] I think so. As I mentioned before, most definitions of information security tend to focus, sometimes exclusively, on specific usages or particular media. Information Security is not just about protecting electronic data from unauthorized use.

It is a common misconception that Information Security is synonymous with computer security, such as computer and network security, information technology (IT) security, information systems security, and information and communications technology (ICT) security. Each of these has a different emphasis, but the common concern is the security of information in some form (electronic in these cases). Therefore all are subsets of Information Security. Conversely, Information Security covers not just information but all infrastructures that facilitate its use processes, systems, services, and technology, including computers, voice and data networks.

[Q] Can risks of security be eliminated altogether?

[GDJ] No, of course not. No one can ever eradicate all risk of improper use of any information. The level of information



security sought in any particular situation should be judged with the value of the information and the loss, financial or otherwise, that might accrue from improper use disclosure, degradation, denial, or whatever.

[Q] Are there different attributes of Information Security?

[GD] There are three widely accepted elements of information security. These are: confidentiality, integrity and availability. Interestingly, these can be remembered by the mnemonic 'CIA' and are also referred to as the CIA triad.

[Q] Are any of these elements more important than the others?

[GD] Historically, up to about 1990, confidentiality was the most important element of information security, followed by integrity, and then availability. By 2001, changing use and expectation patterns had moved availability to the top of most versions of this priority list. The first goal of modern information security has, in effect, become to ensure that systems are predictably dependable in the face of all sorts of malice, and particularly in the face of denial of service attacks.

Recently, NIST Special Publication 800-33 Underlying Technical Models for Information Technology Security added 'assurance' as an essential element as well. Without it the other objectives are not met. Assurance is the basis for confidence that the security measures, both technical and operational, work as intended to protect the system and the information in processes and that the other four security objectives have been adequately met by a specific implementation.

[Q] Mt. Sierra College offers a Bachelors Degree in Information Security. It is not a degree offered in too many institutions. How did this come about?

[GD] As information security was becoming an ever-increasing concern and securing our national information highway was seen as essential, Mt. Sierra College embarked on designing its Information Security Bachelors Degree program to meet the standards of the United States National Security Agency training standards for information security program (INFOSEC) professionals. Mt. Sierra College now offers a Bachelors Degree in Information Security. The degree can be completed on-campus or online, in three years or less.

[Q] What should students expect if they are planning to earn their Bachelors Degree in Information Security at Mt. Sierra College?

[GD] Students completing their degree in Information Security will possess the ability to understand the fundamentals of security, understand how security flaws are exploited, design and develop rational and appropriate security measures, understand how different operating systems address security concerns, assemble and manage strategic security management teams, and apply appropriate security standards and measures for different computer environments.

Students receiving their degree in Information Security receive coursework in nine major areas: security fundamentals, security policy development and management, cyber law and ethics, cryptology, computer and data forensics, applied LAN, WAN and wireless security, disaster recovery, security development life cycle management, and general education.

[Q] And what kind of careers should they look forward to?

[GD] Opportunities in the field of Information Security are ever growing. As a Security Analyst, for example, one would plan, coordinate and implement an organization's security. A Security Software Developer would design software to protect against viruses, hackers and spam. A Security Forensics Professional would combine knowledge of information technology and security with investigative techniques to identify unwarranted network activity. A Security Architect/Technologist would analyze security information to identify methods of penetration and further strengthen products, networks and services. And finally, a Security Design Engineer would solve design problems and apply computer technology to meet the individual security needs of an organization or a company. These are exciting career choices for students!

For more information on the Information Security Program visit mtsierra.edu/infosec or call 888.532.5291

Copyright 2006 Mt. Sierra College
101 East Huntington Drive Monrovia CA 91016