Preface

Information Systems and Technology have evolved to a level that its use is becoming a common occurrence. While the academic profession is still debating the utility or value of Information Systems and Technology, its use in organizations all over the globe is rising at an increasing rate. However, this widespread use of information systems and technology is not without its associated problems. While several emerging information and internet ubiquitous technologies provide tremendous positive opportunities, there are still a number of vulnerabilities and risks associated with technology systems. Organizations invest heavily in the latest firewalls, intrusion detection systems and other advanced security technologies, yet losses from security incidents continue to grow each year. According to the Computer Emergency Response Team at Carnegie Mellon University, during 2003 and 2004, approximately 42,000 cyber incidents were reported. As technologies advance, hackers also advance their tools, techniques, and methods to break-ins. Up until a few years ago, phishing attacks (phony e-mails designed to entice users to give up personal information) were unheard of. Now they are relatively common and pharming (creating phony Web sites designed to extract personal information) has become one of the latest strategies employed by identity thieves. Security experts noted that the legions of infected computers are adding to the number of bot networks controlled by hackers. Symantec observed an average of 10,352 active bot network computers per day, an increase of more than 140 percent from the previous reporting period's 4,348 bot computers. According to Symantec, denial-of-service attacks grew from an average of 119 per day to 927 per day since January 2005, a 680 percent increase over the previous six months.

As a result of the above risks associated with the deployment of Information Systems and Technology, information assurance and security has become an important research issue in networked and distributed information sharing environments. Finding effective ways to protect information systems, networks, and sensitive data within the critical information infrastructure is challenging even with the most advanced technology and trained professionals. Information assurance and security has become an important research issue in networked and distributed information sharing environments. In today's companies, information systems not only support business functions but are also an integral part of business operations. For example, ERP systems (Enterprise Resource Planning) are now essential for organizations and their supply chains. Incorrect information in ERP systems can have serious consequences for the inter-networked companies. Information security means protecting information from malicious threats and damage due to external or internal sources. Assurance in computer security is a measure of confidence that the security features and architecture of an automated information system accurately mediate and enforce the security policy.

Information assurance combines the requirements of information security, integrity, and significance. Assuring information means having a safe information system, which guarantees that information is secure and at the same time keeps its integrity and its significance during its lifetime. The goal of information assurance is to provide trustworthy and significant information to users in operational, service systems that rely on the information for the fulfillment of their objectives. However, despite an organization's best efforts at protection, there have been and will continue to be breaches, even as IT security improves. The difference now is that companies are required to report on more of their financial information than ever before. Sarbanes Oxley, Gramm-Leach-Bliley, PCI standards, and HIPAA regulations, each in different ways, mandate that companies and executives be accountable for the integrity of their customers' data as well as the company's bottom line.

The security breeches with more advanced tools necessitate enterprises to reexamine their security frameworks, tools, methods, policies, and procedures to protect their enterprise data and systems. The purpose of this handbook is to make readers understand the need for enterprise security strategies, current security tools, procedures and processes, techniques, and tools that are required to protect data and systems. An enterprise security handbook that includes methodologies, techniques, and methods to protect data and systems would be a great contribution to practitioners as well as academicians.

To create such a handbook of research on information assurance and security, we decided to launch this handbook project where researchers from all over the world were invited to contribute. The primary objective of this project was to assemble as much research coverage as possible related to the information security and assurance. As you would agree that information security and assurance subject is not only challenging but also continuously changing. The idea behind this project was to gather latest information from researchers worldwide on information security and assurance. Therefore, in order to provide the best balanced coverage of concepts and issues related to the selected topics of this handbook, researchers from around the world were asked to submit proposals describing their proposed coverage and the contribution of such coverage to the handbook. All proposals were carefully reviewed by the editors in light of their suitability as well as the researchers' record of similar work in the area of the proposed topics.

The goal was to assemble the best minds in the information security and assurance field from all over the world to contribute to the handbook. Upon the receipt of full chapter submissions, each submission was forwarded to expert external reviewers on a double-blind, peer review basis. Only submissions with strong and favorable reviews were chosen as chapters for this handbook. In many cases, submissions were sent back for several revisions prior to final acceptance. As a result, this handbook includes 47 chapters highlighting current concepts, issues, and emerging technologies. All entries are written by knowledgeable, distinguished scholars from many prominent research institutions around the world. The authors who have contributed to this book are well known security experts who have been doing research on various aspects of information assurance and security for several years and have tried to present their technical work in most lucid and simple words. It is hoped that readers will find it easy to understand and implement some of suggested approached to protect their organizations from various kind of security attacks and breaches.

This handbook or organized into four broad sections to cover a variety of topics related to the identification, specification, correction, and mitigation of the security threats in varying conditions. In each case, the role of information assurance and security are clearly identified. Brief description of each section and the coverage of various chapters in each section is provided below.

Section I, titled ***Enterprise Security***, starts the discussion of informaion assurance and security issues. As enterprises are becoming increasingly dependent on their information systems, Information assurance and security has become an important aspect for safety of their data, information, and systems. Finding effective ways to protect information systems, networks, and sensitive data within the critical information infrastructure is challenging even with the most advanced technology and trained professionals. Information systems security and assurance is a complicated subject, and historically only tackled by well-trained and experienced experts. However, as more and more companies are networked and have started using pervasive computing technologies, an increasing number of people need to understand the basics of security in a networked world. Enterprise security is important to almost all organizations. As new technologies emerge, organizations must recognize the need for enterprise security solutions. The seven chapters in Section 1 discuss various kinds of security threats that enterprises face today. Various chapters in this section also dwelves upon the risk management, audit, and control approaches that could be used for security assurances in a variety of business environment, including e-commerce.

Section II, called ***Security Approaches, Frameworks, Tools, and Technologies,*** deals with the approaches, frameworks, methods, tools, and technologies that have been developed and are available for use for information assurance and security in organizations. Attacks on computer systems are becoming much more sophisticated—and potentially devastating—than they ever were in the past. As such, organizations need to stay abreast of the latest protective measures and services to prevent cyber attacks. It is becoming imperative that networks must have self-defending capabilities to mitigate security threats before they affect operational continuity. Despite the increased awareness, the recent frequency of security breaches seems to indicate that many companies have not adequately responded to the issue of data security within their organizations. Therefore, new and effective tools and technologies are needed to prevent, detect, and correct the security breeches in organizations. Sixteen chapters in Section 2 of this handbook describe the development, implementation, and application of various approaches, tools, technologies, and frameworks for effective information assurance and security protection in various types of organizations in centralized and decentralized modes of operations.

Section III, titled ***Security Policies and Procedures,*** is devoted to the important topic of Information security polices and procedures. Security Policy is a foundational element in any Security Program. The purpose of a general security policy is to outline the legal, privacy, and security-related responsibilities that members of the institution have. Because probing a network for vulnerabilities can disrupt systems and expose private data, organizations need a policy in place to address Acceptable Use Policies. There is also a need for policies and ethical guidelines for making employees understand the appropriate action when illegal materials are found on their systems during a vulnerability scan. Eight chapters in Section 3 discuss those various security policy related concerns and issues and offer suggestions for the information assurance and security researchers and practitioners. The discussion in these chapters also discusses the need for effective business continuity and disaster recovery plans and the means to develop, implement, and use these plans to minimize the disruptions in business continuity.

Section IV of this handbook deals with is the topic of ***Mitigating Security Risks***. While the new regulations and statutes are sure to get some attention, the pressure to mitigate data security risks certainly increases. It is becoming increasingly obvious then that inadequate data policies and data security measures can have very costly consequences. Regardless of the solutions employed to reduce the risk of data security breaches, a balance of prevention strategies and mitigation efforts is likely the best possible protection. In fact, given how dependent modern business is on electronic data transmissions, it may no longer be an option to develop a data protection strategy. In order to mitigate security risks, organizations invest substantial resources in developing complicated solutions that are critical to daily operations and long term success. Fifteen chapters in this final section of the handbook describe various developments in identifying and mitigating information assurance and security risks in various types of organizations. The authors of these various chapters also suggest some guidelines to effectively implement risk mitigating solutions including the use of biosecurity measures to understand and mitigate the bioterrorism threats.

This handbook is written with the basic computer user and information systems manager in mind, explaining the concepts needed to read through the hype in the marketplace and understand risks and how to deal with them. Companies need not only to invest in more sophisticated security tools and technologies but also to educate their employees about security and assurances. The market is challenged with an increased need for security and assurance to present security in terms the audience can understand and hopefully this book will do an excellent job of meeting that challenge. Therefore, this handbook is also written for the academic and professional researcher interested in developing appropriate and state-of-the-art tools, techniques, and approaches to deals with various issues arising in information assurance and security.

It is hoped that the diverse and comprehensive coverage of information security and assurance in this authoritative handbook will contribute to a better understanding all topics, research, and discoveries in this evolving, significant field of study. Furthermore, we hope that the contributions included in this handbook will be instrumental in the expansion of the body of knowledge in this vast field. The coverage of this handbook of research on information assurance and security provides a reference resource for both information science and technology researchers and also decision makers in obtaining a greater understanding of the concepts, issues, problems, trends, challenges, and opportunities related to this field of study. It is our sincere hope that this publication and its great amount of information and research will assist our research colleagues, faculty members, students, and organizational decision makers in enhancing their understanding of the current and emerging issues in information assurance and security. Perhaps this publication will even inspire its readers to contribute to the current and future discoveries in this immense field, tapping possibilities to assist humankind in making the world a better place to live for all its inhabitants.

Jatinder N. D. Gupta
The University of Alabama in Huntsville

Sushil K. Sharma
Ball State University