Foreword

The modern era can be characterized by increasing rates of change within every dimension of the environments in which we operate. Global economic and political conditions, technological infrastructure, and socio-cultural developments all contribute to an increasingly turbulent and dynamic environment for those who design and manage information systems for use in business, government, military, and other domains. Even weather patterns and events seem to change more rapidly in recent years! As our institutions (economic, political, military, legal, social) become increasingly global and inter-connected, as we rely more and more on automated control systems to provide our needs for energy, food, and services, and as we establish Internet-based mechanisms for coordinating this global interaction, we introduce greater vulnerability to ourselves as individuals, for companies, and for our governments, including their military organizations. This increased dependence on cyberspace also inflates our vulnerability – isolation is no longer an option. Perhaps no aspect of this phenomenon is as alarming and challenging as the need to understand the various risks to the security of our information systems and the methods for addressing them.

These risks arise from a plethora of sources and motivations. Some are natural; in recent years we have seen significant weather events (Asian Tsunami, Hurricane Katrina, major earthquakes, etc.) that threaten organizations and their physical resources, including information servers. Some risks are from intentional human activity, and the world is now full of new, more sophisticated hackers, spies, terrorists, and criminal organizations that are committed to coordinated global attacks on our information assets in order to achieve their many goals. Some wish to inflict damage and loss for political reasons or for military purposes, some are seeking "trade secrets" and proprietary corporate information, and others are seeking financial information with which to conduct fraud, identity theft, and other criminal acts. Another category of risks has arisen from new classes of increasingly-devious and effective malware capable of penetrating even the most recent perimeter defenses. These include not only viruses, worms, and trojans, but now also rootkits, distributed botnet attacks, and a new scary sophisticated category called the "Storm" class of malware, which includes programs which are self-propagating, coordinated, reusable, and self-defending peer-to-peer tools that use decentralized command and control and seem to use intelligence to dynamically defend themselves from users and software.

Perhaps the greatest threat of all is the insider threat – the organizational member who is a "trusted agent" inside the firewall. This employee or other constituent with a valid username and password regularly interacts with the information assets of the organization, and can initiate great harm to the confidentiality, integrity, or availability of the information system through deliberate activities (consider the disgruntled employee or the counter-spy). Or they may introduce risk via passive noncompliance with security policies, laziness, sloppiness, poor training, or lack of motivation to vigorously protect the

integrity and privacy of the sensitive information of the organization and its partners, clients, customers, and others. I call this problem the "endpoint security problem" because the individual employee is the endpoint of the information system and its network – the employee has direct or indirect access to the entire network from his or her endpoint and can inflict great harm (and has!). The insider threat has repeatedly been called the greatest threat to the system, and yet this is often overlooked in a rush to protect the perimeter with ever-increasingly sophisticated perimeter controls (intrusion detection systems, firewalls, etc.). Greater emphasis on hiring, training, and motivating employees to act securely will generate great payoff for the organizations that pursue this strategy. Mechanisms to support this goal are paramount to the future security of our information assets.

Developing and testing creative solutions and managerial strategies to identify these threats, analyze them, defend against them, and also to recover, repair, and control the damage caused by them is a critical management imperative. Leaders in government and industry must actively and aggressively support the ongoing design and implementation of effective, appropriate solutions (technologies, policies, legal strategies, training, etc.) that can be targeted to these diverse threats to our information assets and to the smooth functions of individuals, teams, organizations, and societies in our global network of systems. New methods of analysis (e.g. threat graphs, evolving standards, government actions) and new solutions (e.g. honeynets, firewall designs, improved training and monitoring) will be required to keep up with the ever-changing threat environment. Research in this area is critical for our protection in this new age of global inter-connectivity and interdependence. We need to continually seek new and better solutions because the enemy is constantly improving the attack vectors. The alternative is not acceptable. The costs are too high. We must prevail.

Merrill Warkentin
Mississippi State University

Merrill Wakentin *is Professor of MIS at Mississippi State University. He has published several books and over 150 research manuscripts, primarily in computer security management, eCommerce, and virtual collaborative teams, in books, Proceedings, and in leading academic journals. He is also an Associate Editor of Management Information Systems Quarterly (for security manuscripts), Information Resources Management Journal, and Journal of Information Systems Security. Professor Warkentin is Guest Editing the special issue of the European Journal of Information Systems on Computer Security and has chaired several global conferences on computer security. He has Chaired the Workshop on Information Security and Privacy (WISP) twice and the Information Security Track at DSI. He has served as Associate Editor for the Information Security tracks of AMCIS and ICIS several times, and will co-Chair the IFIP Workshop on Information Security in 2009. At Mississippi State, Dr. Warkentin directs research projects and doctoral student dissertations in the various areas of computer security and assurance research, including behavorial and policy studies, design of password systems, and managerial controls for computer security management. He serves as a member of the research staff of the Center for Computer Security Research. He has also served as a consultant to numerous organizations and has served as National Distingushed Lecturer for the Association for Computing Machinery (ACM). His PhD in MIS is from the University of Nebraska-Lincoln. He can reached at mwarkentin@acm.org and his website in www.MISProfessor.com.*