

Foreword

The advent of the computer age brought us the ability to gather and process large quantities of information in ever decreasing time. Unfortunately, this new age also arrived with a host of new challenges. First Grace Hooper identified the first computer bug, and, I might add, successfully repaired the problem. Then soon afterward we discovered that some users had learned to use the computer systems to exploit the information to their own desires. Similarly we discovered that other well-meaning users and information system managers had inadvertently caused equally challenging problems. Thus we learned to develop methods and procedures to preserve the confidentiality of the information, maintain the integrity of the data, ensure the availability of the information systems, and to enforce the accountability of the users and processes. A cadre of information systems security professionals quickly rose to the challenge and began to identify and then attempt to solve the security issues.

Our early attempts first sought to identify the threats, vulnerabilities, and risk through risk assessments, certification and accreditation, vulnerability testing, penetration testing, red and black teams and a host of other methods to identify the security issues. Then like our medieval kings we built fortresses (firewalls) to protect our enclaves by walling off our information and systems from outside intruders. However, like the medieval leaders that too late discovered the fundamental management error in allowing the first Trojan Horse into their enclave, our IT management professionals continue to be faced with challenging issues. While some of the security community advocates new technology as the solution to all security, others continue to advocate the timeless process of security evaluations and assessments. Neither by themselves will be sufficient. We certainly need the technological advances of intrusion detection and prevention systems, security operations centers, and incident response tools, but this technology does not hold all the answers. Similarly we must learn to conduct the proper evaluations and assessments in a manner that not just produces a report but also instead leads to actionable recommendations. The security problem has raised to the attention of both industry and government leaders. The US congress has mandated that government leaders address, and report, their progress on resolving the security issues. The US Government is also searching for ways to successfully motivate industry leaders to the security challenges in the private sector.

Today's Information Technology managers are faced with ever increasing issues. Many have hundreds, and some tens of thousands, of systems and applications. Yet many of us as security professionals continue to attack the issues on a system-by-system basis with the same tools we have always used. Instead we must address the hard management issues of developing enterprise level security architectures, configuration control, patch management, user management, and user training. The challenge facing us as security professionals is now to bring both the technology and management processes to bear on the security problems in a synergistic approach by providing security solutions, not more system level assessments.

Our IT managers have long recognized the need for more experienced and well rounded security professionals. Thus the need arose for a method to identify qualified security professionals. At one level this rests with qualifications such as the Certified Information Systems Security Professional (CISSP) and now at the next level for the government with the Information System Security Engineering Professional (ISSEP) certification. Our new ISSEP's will be knowledgeable of the US Government information assurance regulations, practices and procedures as well as the latest security technology. These qualifications provide one path for managers to identify those security professionals that have taken the initiative to advance their careers with independent study and have proven themselves with their certifications.

I wish each of you the best success as you move forward in your security career.

Barry C. Stauffer

December 2003

Mr. Stauffer is the Chief Information Assurance Officer of BAE SYSTEMS and the founder and former CEO of Corbett Technologies, Inc. In 1981 Mr. Stauffer entered the security community as a Naval Officer on the Department of Defense Joint Staff. Since that time he has been involved in both industry and government in the development of security practices, procedures and management approaches. He led the development of the DITSCAP and NIACAP and has been directly involved in the certification and accreditation of numerous systems and the development of large-scale Government security programs.