# Global Information Assurance Certification Paper

The Organizational Challenges and Training of a Chief Security Officer
Joseph P. Gandiosi
GSLC – V.10
July 8, 2003

**INTRODUCTION:**
Since or even before the terrorist attack of September 11, 2001, companies have been focusing on information systems security. The healthcare industry, HIPAA (Health Insurance Portability Accountability Act) was passed by congress and became law on August 21, 1996. HIPAA is about information efficiency, privacy, and security in the United States healthcare industry. The result of HIPAA is the rise of Chief Security Officer (CSO) and Chief Privacy Officer (CPO) positions within the larger healthcare facilities and the rise of certified security consultants for smaller healthcare facilities. The Financial Industry, GLBA (Gramm-Leach Blileg Act established in 1999 has also lead to the rise of the CSO. This paper focuses on the challenges and training of the Chief Security Officer (CSO).

**DEFINITION:**
The Chief Security Officer or Chief Information Security Officer plans and oversees information security for the entire corporation. According to Bill Boone[1], CISO at Motorola, the CSO or CISO must understand the business, understand what makes it successful, identify the factors that can put that success at risk and then find ways of managing that risk through technical, operational or procedural safeguards.

**CHALLENGES:**
There are at least 2 major challenges a Chief Security Officer may encounter. The first is, reporting structure and the second challenge is acceptance by others within the organization. There are many other challenges the CSO will encounter this practical focuses on the organizational challenges.

Reporting Structure:
There have been numerous discussions by corporate executives, auditors and IT executives about this very question. Some believe the CSO should remain under the Chief Information Officer and others believe the CSO should report to the Chief Executive Officer. According to Marc Lewis[1], head of IT Practice at Cleveland executive-recruitment firm of Christian and Timbers, says a company should have its CSO report to the CEO or Chief Operating Officer if the job includes information and physical security. Because security has grown into an organization wide concern, it may not make sense to keep it within IT.
Yet, according to David Bauer[1], Chief Information Security and Privacy Officer at Merrill Lynch & Company in New York, “you want your information security department to be the solution provider and facilitator of risk management for IT.

Otherwise security will be just another audit department, and the IT guys will buy whatever security solution they want".
This question may never have a clear answer because the idea of a Chief Security Officer is still relatively new and some companies even question the need and expense of such a position. Some executives believe their CIO should champion IT security with the help of other departments within the organization.

Acceptance:
The second challenge for a newly appointed Chief Security Officer is acceptance by others within the organization. This can be very difficult because the role of the CSO is to insure information security and physical security already being performed by other departments. This is especially true when dealing with the IT group.
To avoid problems there must be careful planning by the senior management before introducing a CSO position within the organization. A job description, responsibilities and reporting structure must be created and understood by all participating executives. Doing this will not only help with the acceptance of a CSO position but will also help the pave the road for a newly hired CSO.

**KNOWLEDGE:**
The Chief Security Officer is a top security executive position within a company. The CSO generally oversees all security both information and physical, therefore the knowledge level must be diverse as well as business oriented. A CSO should be well versed in many security topics including but not limited to:

Network Security software and hardware, including firewalls, VPNs, wireless and penetration testing and other security devices.

Business Contingency planning including auditing and risk

Disaster Recovery planning including auditing and risk

Security policies, standards, guidelines and procedures

Basic security rules and regulations and also specific rules and regulations depending on the organization's business, such as Health Insurance Portability and Accountability Act (HIPAA) for the healthcare industry and Gramm-Leach Blileg Act (GLBA) for the financial industry.

The above examples are only a small portion of what a CSO must know in order to fulfill the knowledge requirements. Some companies may have their own agenda of requirements. These requirements will vary from organization to organization.

**TRAINING:**
The Chief Security Officer (CSO) training requires a wide range of skills. A well-trained person in all ranges of security ensures expertise in understanding the business strategy and ensures security strategies. More and more companies are requiring security certifications obtained through reputable security training organizations. Some of the certification programs are:

The International Systems Security Certification Consortium² (ISC)² was formed back in 1989 to develop industry standards for information security. In 1992 (ISC)² provided the industry standard for professional security certification known as Certified Information Systems Security Professional (CISSP). This certification program has been accepted throughout the world as a measure of information security knowledge. This comprehensive examination covers ten (10) test domains pertaining to the Common Body of Knowledge (CBK). They are:

Access Control Systems & Methodology
Applications & Systems Development
Cryptography
Law, Investigation & Ethics
Operations Security
Physical Security
Security Architecture & Models
Security Management Practices
Telecommunications, Network & Internet Security

The (ISC)² has another certification known as SSCP Certification. The focus of this is on practices, roles and responsibilities of practitioners of Information Security. The examination covers seven (7) Information security domains. They are:

Access Controls
Administration
Audit & Monitoring
Risk, Response & Recovery
Cryptography
Data Communications
Malicious Code/Malware

The above certifications programs are complete information security certifications. In fact, anyone who has the desire to obtain any certification from (ISC)² should visit the website for further information and requirements. The website is www.isc2.org.

The SANS Institute founded the GIAC (Global Information Assurance Certification) in 1999. The GIAC certification validates the skills of security professionals. The GIAC certifications address a wide range of skill sets including entry level for information security officer as well as advanced security topics.[3] The www.giac.org has complete details of these certification programs.

There are other general certification programs available but the two mentioned above are by far certifications accepted worldwide. There are also industry specific security certifications such as the healthcare industry and the financial industry.

Healthcare:
There are certifications available for the healthcare industry. The training deals with all facets of healthcare to ensure the security of patient information internally as well as externally. These certifications programs can be found at the HIPAA Academy website, www.hipaaacademy.net

Financial:
GLBA (Gramm-Leach Blileg Act) training is available at a number of facilities. Training generally includes an overview of the GLBA Act of 1999 as it pertains to the security of financial institutions and general systems security. Although there is no specific certification for GLBA, the financial industry is requiring some form of security certification and requires understanding of the GLBA Act. One of the websites, www.certifiedtrainers.com specializes in GLBA training.

In terms of training for the CSO, it varies from general security certifications to industry specific certifications. What is sure is, organizations are requiring security professionals to have one form of information security certificate. This insures them the professional has had the necessary training to perform the requirements of a Chief Security Officer.

**SUMMARY:**
In summation, there are many unanswered questions of the role, challenges knowledge and training for a Chief Security Officer. This role has been defined and redefined by executives and by leaders around the world. What they are sure of is the need of a Chief Security Officer to insure the integrity, the confidentiality and the availability of information, the three fundamental principles of Information Security.

**REFERENCES:**

1. http://www.informationweek.com/story/showArticle.jhtml?articleID=6500913 (Where The Chief Security Officer Belongs by Mary Hayes. February 2002).

2. https://www.isc2.org/cgi/content.cgi?category=19
3. http://www.giac.org/overview.php (Overview by David Hoelzer, Director)