

# CAREER OPPORTUNITIES IN SECURITY

**ASIS**  
INTERNATIONAL  
*Advancing Security Worldwide*



Career Opportunities in Security

Copyright © 1990, 1998, 2005, 2013 by ASIS International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of the copyright owner.

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1



# CAREER OPPORTUNITIES IN SECURITY



## TABLE OF CONTENTS

INTRODUCTION . . . . .	2
WHAT IS SECURITY? . . . . .	4
ACADEMIC PROGRAMS IN SECURITY . . . . .	6
CERTIFICATIONS . . . . .	7
SECURITY DISCIPLINES . . . . .	9
SECURITY SPECIALTY AREAS . . . . .	11
Banking and Financial Services Security . . . . .	12
Commercial Real Estate Security . . . . .	13
Communications Security . . . . .	14
Crisis Management and Business Continuity . . . . .	15
Cultural Properties Security . . . . .	16
Food Defense and Agriculture Security . . . . .	17
Gaming and Wagering Security . . . . .	18
Government/Industrial Security . . . . .	19
Healthcare Security . . . . .	20
Information Systems Security . . . . .	21
Lodging and Hospitality Security . . . . .	22
Manufacturing Security . . . . .	23
Petrochemical, Chemical, and Extractive Industry Security . . . . .	24
Pharmaceutical Security . . . . .	25
Retail Loss Prevention . . . . .	26
School Safety and Security . . . . .	27
Security Engineering and Design . . . . .	28
Security Investigations . . . . .	29
Security Sales, Equipment, and Services . . . . .	30
Transportation and Supply Chain Security . . . . .	31
Utilities and Nuclear Security . . . . .	32
OTHER SECURITY SPECIALTY CAREER OPPORTUNITIES . . . . .	33
ASIS INTERNATIONAL . . . . .	35

## INTRODUCTION

While the information contained in this brochure will be of interest to anyone who wants to learn more about the field of security, it has been prepared primarily for the following categories of individuals:

- Individuals seeking to pursue a degree in security management, asset protection, or a related discipline.
- Individuals entering the security field after obtaining a degree in security management, asset protection, or a related discipline.
- Individuals already in the security field who seek a management-track position after obtaining a degree in security management, asset protection, or a related discipline.
- Individuals transitioning from other careers into the public or private security field who seek a management-track position.

To gain entrance into the security field at the non-management entry-level, there are some typical prerequisites. They include having a high school education or above, having no criminal record, being 18+ years of age, and having obtained or be in the process of obtaining some general security knowledge or experience. For example, many jurisdictions require a certain amount of training before an individual can be employed as an armed or unarmed security officer. Many of the duties performed by individuals in these positions are likely to be similar, regardless of the security industry sector in which the individual is employed. Those duties can include such activities as routine patrolling, public relations, controlling access to facilities, and basic report writing.

Individuals interested in these kinds of positions should consult publications from organizations such as the International Foundation of Protection Officers (IFPO) at <http://ifpo.org/>

Information from a number of security specialties has been compiled to give the reader a better idea of the prerequisites for entering management-track supervisory and non-supervisory positions in those specialties. In addition to the entry-level data, there is information concerning the duties of mid-level management and non-management personnel in those specialties.

Chief security officer (CSO) and equivalent senior and executive-level positions are outside the scope of this booklet.



Unless otherwise indicated, in dealing with these specialties the following terminology has been used:

- **Management** refers to the direction of activity at the second-line supervisory level or above.
- **Non-management** refers to non-supervisory line positions; first-line supervisor positions and staff positions.
- **Entry-level** refers to management-track supervisory and non-supervisory positions.
- **Mid-level** refers to management and non-management level positions at the branch, area, region, or division level.
- **Jurisdiction** includes towns, cities, counties, districts, provinces, states, countries, and other governmental entities.



## WHAT IS SECURITY?

### A Wide-Ranging Field

To the average person the idea of a career in security may be limited. The tendency for many people is to think only in terms of uniformed security officers on patrol, monitoring alarms, or controlling access to a facility. Those who may be interested in a career as a security professional need to understand that a wide range of administrative, technical, supervisory, and managerial opportunities also exist in the security field.

### A Dynamic Industry

Security is one of the fastest-growing professional careers worldwide. A career in the security field provides a multitude of opportunities. These opportunities range from entry-level security officer positions to investigators specializing in specific areas and managers and directors of security at major corporations and organizations around the world. The demand for heightened security is being increased by theft of information, workplace violence, terrorism, and white collar crime.

The security industry in the U.S. is a \$350 billion a year business and growing.<sup>1</sup> Opportunities exist at all levels within the security industry. All businesses, no matter how small, have security concerns such as fraud, theft, computer hacking, economic espionage, or workplace violence. All organizations need to protect themselves from activities that disrupt their normal operations. Each specialty within the security field has its own requirements and issues. Shoplifting continues to be a problem for retail organizations, while hospitals face privacy rights issues, and hotels have to reconcile fire and safety regulations with security requirements. In addition, government and private industry have differing security needs. Individuals wishing to pursue a career in a security specialty field should become more knowledgeable of the latest trends, issues, and concerns within that specialty.

### A Diverse Industry

In today's downsizing corporate world and changing environment, it is essential for students and individuals seeking career changes to be able to identify opportunities in the security marketplace. Women, minori-

---

<sup>1</sup> ASIS International and Institute of Finance and Management. (2013). *The United States Security Industry: size and scope, insights, trends, and data*. Alexandria, VA: ASIS International.

ties, and physically challenged individuals are becoming valuable for organizations in need of security professionals.

## Proprietary or Contract Security

Proprietary security personnel are employed directly by the organization whose assets are being protected. As a general rule, proprietary security operations occur in businesses, institutions, and agencies large enough to warrant full-time attention to the issues of assets protection.

The security services industry provides security products and services under contract to an organization. Equipment suppliers include a wide range of firms that sell, install, and maintain equipment such as access control, intrusion detection, protective lighting, and closed circuit television systems. There are other contract firms that provide uniformed security officers, conduct investigations, perform risk assessments, design security systems, transport high-value shipments, protect high-risk personnel, and offer other security services.

## Law Enforcement vs. Security

Law enforcement focuses on reaction to crime and the enforcement of public laws and ordinances. Security professionals, on the other hand, are more proactive and focus on identifying and preventing a problem before it occurs. In addition, security personnel are more likely to be involved in protecting assets and carrying out an organization's policies and procedures than in enforcing criminal statutes.

## Public Sector as well as Private Sector

Many people think of the security field as being synonymous with the private sector, and to a large extent, that is true. However, there are many security opportunities in government agencies, and security professionals who provide security in the public sector may be involved in many of the same functions as in the private sector, depending on the level and size of the jurisdiction. For example, there may be individuals involved in physical security, personnel security, information security, and information systems security. In addition, those engaged in government security can deal with the security of a wide variety of assets, ranging from office buildings to intelligence facilities, laboratories, logistical facilities, and cultural properties.



## ACADEMIC PROGRAMS IN SECURITY

A number of colleges and universities offer security education programs of one degree or another at the associate, baccalaureate, or graduate level. Some of these offer a major in security management, asset protection, or a similar discipline while others offer an area of concentration, a minor or a series of courses in security. Some institutions, particularly at the community college level, may offer weekend seminars in selected security topics. While ASIS views security management as a distinct field of academic study, separate and apart from criminal justice (CJ), administration of justice (ADJ), or criminology, some institutions offer security education programs aligned with CJ, ADJ, or criminology programs or departments.

A listing of many of the institutions that offer security education programs is available on the ASIS Career Center website or Academic & Student Center section on the ASIS International website [<http://tinyurl.com/asisaplist>]

Security is a business function and is not a subset or spin-off of the criminal justice system. Students seeking careers in security should pursue course work in security management, business, information or systems technology, computer science, law, terrorism studies, emergency management, and personnel and information management. Students should also consult the specialty pages in this booklet for education requirements that may relate to a particular specialty.

Students are also encouraged to seek involvement in internships, co-ops or work study programs with security employers. In addition, students should seek out security professionals who work in the security specialties or disciplines that the student may wish to pursue, with a view to learning more about the specialty through activities such as site visits and networking.





# CERTIFICATIONS

## Certifications from ASIS International (ASIS)

Certification is a significant voluntary investment in a security professional's future, and it offers an edge in the increasingly competitive security job market. Companies, contractors, and governments are now taking additional steps to ensure that they are hiring or working with the most skilled and knowledgeable individuals. Board certifications from ASIS offer them a screening tool that has the backing and credibility of the leading organization in the world for security professionals. And for individuals, certifications could make the difference when bidding on contracts, applying for jobs, or transitioning to private security. Certifications are objective means of distinguishing competent security practitioners from those who claim to be. The three board-certified designations of ASIS all meet stringent, internationally accepted requirements for education, experience, and examination. Being certified allows you to:

- demonstrate your knowledge and skills
- gain instant professional credibility
- differentiate yourself from others
- enhance your personal and professional development
- increase your earnings potential

### ASIS offers three certifications:

**Certified Protection Professional (CPP)** is the preeminent designation awarded to individuals whose primary responsibilities are in security management and who have demonstrated advanced knowledge in security solutions and best business practices. CPPs must have nine years of security experience, with at least three of those years in responsible charge of a security function; or a bachelor's degree and seven years of experience, with at least three of those years in responsible charge of a security function. Eligible individuals must then pass an examination.

**Professional Certified Investigator (PCI)** is a technical designation awarded to those individuals whose primary responsibilities are to conduct investigations and who have demonstrated in-depth operational knowledge and competence in this area. PCIs must have a high school diploma or GED equivalent and five years of investigations experience, two of which must be in case management. Eligible individuals must then pass an examination.





**Physical Security Professional (PSP)** is a technical designation awarded to those individuals whose primary responsibilities are to conduct physical security surveys, design integrated security systems, or install, operate, or maintain those systems and who have demonstrated in-depth operational knowledge and competence in this area. PSPs must have a high school diploma or GED equivalent and five years of physical security experience. Eligible individuals must then pass an examination.

## Other Certifications

In addition to ASIS certifications, a number of specialized security and security-related certifications are offered by other organizations. A select few are mentioned in this booklet, if appropriate to an industry sector.

**Certified Fraud Examiner (CFE)** offered by the Association of Certified Fraud Examiners.

**Certified Forensic Interviewer (CFI)** offered by the International Association of Interviewers (IAI).

**Certified Healthcare Protection Administrator (CHPA)** offered by the International Association of Healthcare Security and Safety Professionals (IAHSSP).

**Certified Information Systems Security Professional (CISSP)** offered by the International Information Systems Security Certification Consortium (ISC)<sup>2</sup>.

**Certified Lodging Security Supervisor (CLSS)** and **Certified Lodging Security Director (CLSD)** offered by the Educational Institute of the American Hotel and Lodging Association (AH&LA).

**Certified Security Consultant (CSC)** offered by the International Association of Professional Security Consultants (IAPSC).

**Certified Security Project Manager (CSPM)** offered by the Security Industry Association (SIA).

**Global Information Assurance Certificate (GIAC)** offered by SANS Institute.

**Industrial Security Professional (ISP)** offered by the National Classification Management Society (NCMS).

**Loss Prevention Qualified (LPQ)** and **Loss Prevention Certified (LPC)** offered by the Loss Prevention Foundation (LPF).

# SECURITY DISCIPLINES

The security field is divided into a number of specialized disciplines. In a large organization, a security professional may work full-time in one of these disciplines. In smaller organizations, a security professional may need to have some proficiency in each of them. These disciplines may be found in most of the security specialty areas listed in the next section of this booklet.

**Physical Security** focuses on the protection of people, property, and facilities through the use of security forces, security systems, and security procedures. Physical security personnel oversee proprietary or contract uniformed security operations, identify security system requirements, assess internal and external threats to assets, and develop policies, plans, procedures, and physical safeguards to counter those threats. Physical security can include the use of barriers, alarms, locks, access control systems, protective lighting, closed circuit televisions, and other state-of-the-art security technology.

**Information Security** involves safeguarding sensitive information. Although information security has traditionally been associated with protection of U.S. Government classified information, it can also include privacy data, proprietary information, contractual information, and intellectual property. Information security deals with issues such as who should access the data and how the data is stored, controlled, marked, disseminated, and disposed of.

**Information Systems Security** involves maintaining the confidentiality, reliability, and availability of data created, stored, processed and/or transmitted via automated information systems. Information systems security personnel develop procedures and safeguards to protect against hackers and other unauthorized efforts to access data, viruses, and a number of other threats to information systems.

**Personnel Security** deals with ensuring the integrity and reliability of an organization's workforce. Personnel security encompasses background investigations, drug testing, and other preemployment screening techniques, as well as adjudication of results and granting security clearances and other information access privileges.





**Homeland Security** – In the aftermath of September 11, 2001, there has been significant emphasis on “homeland security.” The term has been applied to activities ranging from, but not limited to, the protection of U.S. airspace to the response to chemical or biological attacks, and from protection against cyber attacks to the security of rail lines and seaports from terrorist attacks. Unfortunately, there is little consensus on exactly what the term means. Since “homeland security” has such a broad connotation, it is treated in this booklet as a cross-cutting discipline rather than a security specialty.

**Critical Infrastructure Protection (CIP)** is another cross-cutting specialty that has emerged, in its current form, in recent years. Many would describe it as protecting the information systems that control elements of the infrastructure, such as petroleum pipelines, telecommunications systems, and nuclear power plants, from terrorist attacks. Others consider it as covering the protection of not only the information systems that operate and control the infrastructure, but the infrastructure itself, whether it be a bridge, a telephone switching center or a food processing plant. Due to the varying connotations applied to CIP and the extensive scope of the infrastructure, it too is treated in this booklet as a cross-cutting discipline rather than a security specialty.

# SECURITY SPECIALITY AREAS

The following areas represent some of the specialties within the security field. Each specialty area provides a brief description of the specialty in addition to prerequisites for entering management-track supervisory and non-supervisory positions in those specialties. In addition to the entry-level data, there is information concerning the duties of mid-level management and non-management personnel in those specialties.

## Scope of Duties

Duties performed in entry-level management-track positions can vary significantly, depending upon the specialty. Duties performed in mid-level positions, regardless of the specialty, may include typical responsibilities such as planning, organizing, staffing, controlling, budgeting, coordinating, presenting, directing, and writing reports. In addition to these functions, mid-level positions may include specialty-specific responsibilities.

## International Applicability

Many, if not most, of the security specialties described in this brochure may be found in various countries around the world. While the descriptions of specialty functions should have global applicability, it is quite possible that the education and experience requirements may vary from one country to another, since systems of higher education are not the same in all parts of the world. Therefore, an individual aspiring to a management-level security position may want to contact the nearest ASIS chapter or region, or a local professional security association to determine the education and experience requirements that apply in that jurisdiction.

## Licensing and Regulatory Requirements

Licensing and government control of management-level security professionals is not the norm in the United States. However, that may not be the case for all specialties or for all areas inside or outside the United States. Therefore, individuals should be cognizant of the licensing or other regulatory requirements that may apply within the jurisdiction in which they desire to work.

## Legal, Ethical, and Compliance Issues

As with licensing and government controls, legal, ethical, and compliance issues may vary from one jurisdiction and from one specialty or industry sector to another. Security professionals need to be cognizant of the requirements that apply to their particular security discipline or security specialty, industry sector, and jurisdiction.



## Banking and Financial Services Security

Careers in this field include those associated with banking (including retail banking, mortgage, credit/debit cards, internet banking, commercial and consumer lending), stock brokerages, insurance companies, and other financial institutions. As a key component to the critical infrastructure of every nation, the financial services industry is regulated by various government agencies. Financial institution security directors and managers must deal with a wide variety of concerns including theft, fraud, workplace violence, information security, investigations, executive protection, business continuity, physical security, and operational risk issues in order to adequately protect their institution. Security managers must be effective leaders within their organization and able to successfully influence change.

Because of the increasing complexity of the financial services industry, companies continue to seek the best and the brightest from the military and law enforcement agencies, colleges and universities, and from within other private sector companies, both within and outside of the financial services sector.



### ENTRY-LEVEL

Entry-level management positions in financial services generally require a degree in business, finance, or security management from an accredited institution as well as three to five years experience either in law enforcement, military, or security.

### MID-LEVEL

Mid-level management positions, requiring expertise in multiple security disciplines, generally call for a bachelor's degree in an appropriate discipline, general management and technical skills and three to seven years of demonstrated success in the field. Professional certifications such as the CPP or other ASIS certification and CFE (as well as the CISSP for technical positions) are often desired as an indicator of professionalism and qualifications.

# Commercial Real Estate Security

Security in the commercial real estate industry provides opportunities not only in commercial high-rise office buildings but also in residential buildings and shopping malls. Commercial real estate ranges from the environment in which people spend their working hours to where they live and where they shop. Each venue has challenges and aspects that while not unique to the security industry, must be addressed in an appropriate and cost effective manner. Regardless of the venue, the primary focus is on personnel and asset protection. This is accomplished by solid liaison with local law enforcement, knowledge of staffing requirements, and electronic security systems. All vulnerable areas of a facility must be identified and protected with appropriate resources.

## ENTRY-LEVEL

Entry-level management positions generally require a degree in security or a related field from an accredited institution as well as one to two years experience in law enforcement or security.

## MID-LEVEL

Mid-level management positions, requiring expertise in multiple security disciplines, generally require a degree in security or a related field from an accredited institution, as well as five to seven years of demonstrated success in the field. Professional certifications such as the CPP, PCI, and PSP are often desired as an indicator of professionalism and qualifications.



## Communications Security

Once only considered to be traditional landline telephone services, this business has evolved to include many different types of communication with the development of interconnected wireline, wireless, satellite and VoIP transmissions. The sector is considered an integral component of the U.S. economy and has been identified as critical infrastructure, providing a support function for all other critical infrastructure sectors. Security professionals in this field are primarily concerned with protecting the network and preventing disruptions that may result in outages of services. These impacts may be a result of a physical or technical breach. Additionally, communications service providers have support organizations such as retail sales, customer call centers, corporate centers, and information technology. Security managers must effectively work across the enterprise and be able to work as a business partner with the various organizations.

Due to the complexity of the communications sector, security functions required by a service provider typically include investigations, physical security, loss prevention, fraud prevention, and technical security.

### ENTRY-LEVEL

Depending on the size of the organization and the position, entry-level managers usually require a four-year degree and three to five years of experience in a related field. In some cases, additional experience may be considered in lieu of a degree. Certifications such as the CPP, PSP, PCI, or CISSP are preferred.

### MID-LEVEL

Mid-level managers normally require a four-year degree (or graduate degree depending on the organization) and at least eight to ten years of direct experience in their respective field. Certifications such as the CPP, PSP, PCI, or CISSP are preferred and in some cases may be required.





# Crisis Management and Business Continuity

Crisis management (CM) and business continuity (BC) address the activities required to prepare for, and respond to, critical incidents, and to continue business operations with minimal to no stoppage. BC in the public sector is called continuity of operations (COOP). COOP focuses on mitigating disruptions and restoring operations of agency or community services and infrastructure, while BC focuses on effectively mitigating business disruptions within defined timeframes regardless of the adverse circumstances. Information technology (IT) disaster recovery (DR) is considered a subset of BC and COOP, focusing on restoration of lost or disrupted IT data and systems.

While there is presently no crisis management certification per se, relevant professional certifications are highly desirable and in many cases required. Selecting the appropriate certification for the position of interest is necessary, e.g., the CISSP is highly desirable for DR positions because this is primarily an IT security certification with required knowledge of BC/DR.

**ENTRY-LEVEL** Entry-level CM and BC positions often require a relevant bachelor's degree in a related field such as emergency management (EM), communications, risk management, or related social sciences. Military and law enforcement professionals may be able to transition into this field if they have sufficient training and experience in the crisis management field.

**MID-LEVEL** Mid-level CM and BC positions most often require a relevant bachelor's degree; a graduate degree is often preferred in a related field such as those indicated above, or computer sciences. Several universities provide degrees in crisis or emergency management and graduates are expected to have a breadth of training and education desirable to potential employers. DR positions require a solid background and education in computer systems. Experienced professionals are often able to move between public and private sectors, but the diverse focus and culture of these sectors can make transition difficult.



## Cultural Properties Security

Museum and Cultural Properties' common denominator is making a unique contribution to the public by collecting, preserving, and interpreting the things of this world. Their numbers include both governmental and private museums of anthropology, art history and natural history, aquariums, arboreta, art centers, botanical gardens, children's museums, historic sites, nature centers, planetariums, science and technology centers, zoos, libraries, and archives.

Protection and security service careers in cultural properties provide paths to security operations (security and/or law enforcement officers, investigators, supervisors, and managers), technical services (physical and electronic security specialists), fire protection specialists, health and safety services, administrative (payroll, recruiting, training), and visitor services.



### ENTRY-LEVEL

Entry-level management positions desire an associate's or bachelor's degree. Protection-related and/or liberal arts and humanities fields of study are acceptable. Past work experience in public service or educational tourism is desirable.

### MID-LEVEL

Mid-level management positions desire a bachelor's degree appropriate to the chosen career path.

Operations managers: security or criminal justice related.

Technical managers: electrical and/or locksmith related.

Health and Safety: science related.

Administrative: liberal arts and business related.

Three to five years related work experience is normally a prerequisite for mid-level management positions.

# Food Defense and Agriculture Security

Food defense is a public health issue, and the risk to food is increasing due to globalization. Participants in the global food supply chain must consider the security/safety of all business partners as well as their own. From farm to fork, maintaining a safe food supply involves an extensive supply chain—from food production (livestock and crops) to the transporting, warehousing, processing, and manufacturing facilities, to wholesalers and retail food purveyors such as grocery stores, bakeries, restaurants, and even vending machines. A security career in this specialty involves protecting the food supply from intentional threats. Protecting against agroterrorism, inspecting and auditing food processing plants and research laboratories, ensuring compliance with import/export laws and regulations, and even dealing with food worker health and hygiene are a few examples of the wide variety of security responsibilities in this specialty.

**ENTRY-LEVEL** Entry-level management positions generally require an associate's or bachelor's degree. Most positions require two-plus years of general security experience and may require some specialty-specific training or experience. A CPP designation is preferred for many positions.

**MID-LEVEL** Mid-level management positions generally require a bachelor's degree and five-plus years of general security experience and may require some specialty-specific training or experience. A CPP designation is required or desired for many positions.



## Gaming and Wagering Security

As the gaming sector continues to grow globally, one thing has always remained true: at its core, the gaming business is entertainment. With advancing technology in the gaming and wagering industry now offering online, lottery, sports betting, commercial land or sea, and tribal gaming operations, and with the tremendous growth of the industry itself, come new opportunities and responsibilities for security practitioners. Gaming's entertainment value requires security practitioners to provide adequate security and to protect the public trust while allowing guests and gamblers to experience this unique and ever-changing environment in a responsible manner.



### ENTRY-LEVEL

Entry-level management positions require a high school diploma or equivalent and a minimum of three years' experience in law enforcement, security, or surveillance systems operation, with emergency management technician (EMT) certification or professional certification, with previous gaming experience preferred.

### MID-LEVEL

Mid-level management positions require a minimum of five or more years in law enforcement, casino security, or surveillance systems operation, as well as an associate degree in criminal justice, homeland security, or a related field, and a CPP or other ASIS certification is preferred.

# Government/Industrial Security

Government/industrial security professionals are results-oriented individuals with effective technical, leadership, and communications skills who specialize in the protection of National Security Information. These professionals develop and implement programs in accordance with the National Industrial Security Program (NISP). The NISP is a security partnership between the U.S. Government and industry that was created to safeguard Federal Government classified and sensitive information that is released to contractors, licensees, and grantees of the U.S. Government. Security professionals within this specialty must meet the requirements, restrictions, and other safeguards within the constraints of applicable law and the Code of Federal Regulations, necessary to prevent unauthorized disclosure of National Security Information released by U.S. Government departments and agencies to their contractors.

**ENTRY-LEVEL** An academic degree in security management or business is preferred for entry-level positions. Experience in government or industrial security is always a plus. Specific experience in, or exposure to, security regulations, compliance, communication, and execution would be applicable. Other positive attributes include a proven, positive track record in problem solving, communication, and customer relations.

**MID-LEVEL** Management positions require a baccalaureate or advanced degree from an accredited institution and five to ten years' experience in the government or industrial security field with supervisory or previous managerial experience. Necessary specialty-specific training or experience includes professional certification (CPP, PCI, PSP, ISP, CFE) preferred, or a documented record of professional security training from U.S. Government-sponsored training sessions. Other preferred prerequisites include a proven track record in problem solving, communication, leadership, policy development, customer relations, successful application of security regulations, and budgetary development.



## Healthcare Security

Security in the healthcare industry provides many diverse opportunities not only in hospitals, but also in clinics, psychiatric facilities, long-term care centers and teaching hospitals. Healthcare security is a multi-faceted, challenging field, which includes dealing with immobile, unconscious, emotionally disturbed and distraught patients and their families. It can also entail dealing with high-profile or celebrity visitors and patients, and with the media and public interest that such individuals may generate. Responsibilities can involve providing security support to a wide range of functions and facilities, including emergency and trauma centers, pharmacies, laboratories, birthing centers, parking facilities, and food and retail activities. Healthcare security professionals may also become engaged in providing security support for high-value diagnostic and patient care equipment, some of which may have radioactive components, and for HIPAA and other sensitive information. In addition, security personnel may have to deal with specialized security and response activities related to decontamination, isolation, or quarantine procedures.

Thorough and comprehensive investigation plays a substantial role in asset protection and reducing losses. The work environment is oriented toward patient, visitor and staff protection and service, and may also include safety and community emergency management. Security opportunities may include being a security supervisor, security manager, security director, or chief security officer.

### ENTRY-LEVEL

Entry-level management positions typically require a bachelor's degree in security or a related field, or equivalent experience. Two years of security supervisory experience are required and experience in health care security or customer service is desired. In addition, training and experience in business management and human resources are desired.

### MID-LEVEL

Mid-level management positions require a bachelor's degree in security or a related field, or equivalent experience. A master's degree is desired. Five years as a senior supervisor or entry-level manager are required and experience in healthcare security or customer service is desired. In addition, training and experience in business management and human resources are desired. The CHPA and CPP are preferred designations.



# Information Systems Security

Information systems security (ISS) is one of the most important security career fields in the market today—one that focuses on protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The goals of information security include protecting the confidentiality, integrity and availability of information.

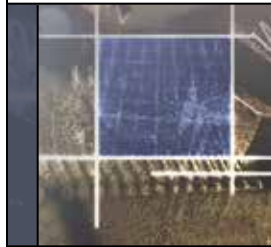
All organizations, including governments, military, financial institutions, hospitals, and private businesses, gather and store a great deal of information about their employees, customers, products, research, and financial operations. Most of this information is collected, processed, and stored electronically and transmitted across networks to other computers. Today, mobile devices and cloud infrastructures are in wide use—increasing the risk of data breach. Protecting confidential information is a business requirement, and in many cases is also an ethical, legal and national security requirement.

The field of ISS has grown dramatically in recent years. There are many areas for specialization such as information systems auditing, security architecture, security engineering, incident response, penetration testing, and digital forensics. Specific ISS technical certifications can assist in getting started in this field including CISSP, CEH, CISA, CISM, CRISC, and SANS GIAC—in addition to security certifications such as CPP and PSP. Specific platform certifications (CCNA, MCSE, and CCIE) are also useful.

For computer, network, and application security professionals, such positions require a thorough understanding of infrastructures, technical standards, accepted security frameworks, regulations, and hands-on experience with such technologies as firewalls, IDS/IPS, SIEM, proxies, EPP, and network/app scanners. In addition, there is a growing need for experience with mobile and cloud technologies.

**ENTRY-LEVEL** These positions traditionally require a four-year degree (or equivalent experience) in computer science or a related field, and at least two to three years of progressive experience in security engineering and architecture. Industry certifications and platform-specific certifications are desired. Typical job titles include security analyst, security consultant, and security specialist.

**MID-LEVEL** These positions require a four-year degree or equivalent (or a graduate degree depending on the organization), at least five to ten years of experience in a direct ISS role and evidence of success in managing a specific ISS function (such as network security, application security, database security, compliance). Industry certifications and platform-specific certifications are desired. Job titles include network/application security manager, information assurance manager, information security officer, or IT audit manager.



## Lodging and Hospitality Security

The hospitality, entertainment, and lodging industry has increased its interest in, and dedicated additional resources to, the security function. Hotel owners and property managers are cognizant of the need to protect their guests and assets in order to have their properties perceived as safe havens. To meet these needs, there is increased emphasis on recruiting and hiring knowledgeable security professionals. Hotel security positions generally pay well and include excellent benefits. The work environment is professional, demanding, and complex, while routine responsibilities include extensive interaction with guests and employees. The outlook, in general, is promising with career opportunities continuing to expand.



### ENTRY-LEVEL

Entry-level management positions often require a certificate in security management and/or a bachelor's degree, as well as one to three years of general employment, plus one year of lodging-specific security service. The CLSS designation is preferred but not required.

### MID-LEVEL

Mid-level management positions require a bachelor's degree, three to five years of general employment, plus one year of lodging-specific security service. In addition, successful managers should be computer proficient, articulate, and possess excellent interpersonal skills. The CLSD and CPP designations are preferred.



# Manufacturing Security

Manufacturers make products which, in turn, are sold either to wholesalers, distributors, or directly to consumers. Professionals within the manufacturing security specialty are responsible for issues involving not only sales transactions, but transport issues, ordering and purchasing of raw materials, and the protection of resources against loss or theft. Manufacturers are becoming increasingly aware of the potential for loss. Prevention of loss can be accomplished only through employing competent security directors and managers who can help integrate the security function into the total operation rather than allowing it to remain isolated. Depending on the products being manufactured, individuals in this specialty may work in a variety of environments, including exposure to varying weather conditions and involvement with chemical processing areas.

**ENTRY-LEVEL** Entry-level management positions generally require at least an associate's degree and often a bachelor's degree. Most positions require two-plus years of general security experience and may require some specialty-specific training or experience. A CPP designation is preferred for many positions.

**MID-LEVEL** Mid-level management positions generally require a bachelor's degree and five-plus years of general security experience and may require some specialty-specific training or experience. A CPP designation is required or desired for many positions.



## Petrochemical, Chemical, and Extractive Industry Security

Extractive industries refer primarily to the oil & gas and mining industries (predominantly precious metals and gemstones). While these industries are distinctly different in their products, they deal with very similar challenges throughout all stages of their product's finite life cycle (exploration, project development, production, transportation, and reclamation). Typically, these facilities involve work in remote locations and are commonly located in developing countries. In addition, harsh climates often come into play, such as deep jungles, arctic tundra, high elevations, or vast desert regions. Security professionals deal with a variety of challenges, such as travel security in remote/hostile regions, isolated workforce, human rights concerns, and the protection of high-value or volatile products, which can be the target of either opportunistic or organized criminal groups, terrorist activity, or environmental groups.



### ENTRY-LEVEL

Entry-level positions generally require an associate's degree, preferably in security or a related field, and five years of military or law enforcement experience in fields such as security, surveillance system operator, systems technician or intelligence. ASIS certifications such as CPP, PCI, and PSP are preferred, and foreign language skills are also highly desirable.

### MID-LEVEL

Mid-level positions generally require a bachelor's or master's degree, preferably in security or business administration, and ten years of industry experience (or applicable military or law enforcement experience). ASIS certifications such as CPP, PCI, and PSP are preferred, and foreign language skills are also highly desirable.

# Pharmaceutical Security

Pharmaceutical security offers challenging yet rewarding management careers by providing high quality, safe medicines to patients through highly technical and complex supply chains. Supervisors to chief security officers (CSOs) provide a wide variety of experience and services to include but not limited to:

- investigation of product theft, adulteration, diversion, and counterfeiting;
- the implementation and management of regulated security programs (C-TPAT, AEO, CCSP, etc.);
- development and management of supply chain and transportation security programs;
- risk assessment and treatment;
- business continuity and crisis management planning and testing; and
- site security services and employee safety.

Security managers interact internally with virtually all departments (Human Resources, Operations, Legal, Finance/Accounting, Accounts Payable, Procurement, Sales, etc.) and externally throughout the supply chain to include setting and monitoring security standards for suppliers, affiliates, manufacturers, distributors, carriers, and other external entities that comprise the complete supply chain.

**ENTRY-LEVEL** Entry-level management positions require a bachelor's degree in security or a related field, or equivalent experience. Two years of security or related supervisory experience are required and experience in pharmaceutical security or customer service is desired. In addition, training and experience in business management and human resources are desired.

**MID-LEVEL** Mid-level management positions require a bachelor's degree in security or a related field, or equivalent experience. A master's degree is desired. Five years as a senior supervisor or entry-level manager are required and experience in pharmaceutical security or investigations is desired. In addition, training and experience in business management and human resources are desired. CPP is a preferred designation.



## Retail Loss Prevention

Retail loss prevention refers to the security practices employed in the protection of a retail company's assets. In the broadest sense, the loss prevention function is to detect, deter, resolve, and reduce the loss of monies, merchandise, and other assets. Loss prevention standards and practices, however, are more holistic in their role within company operations. Loss prevention focuses on policy, behaviors, logistics, training, education, hiring practices, and compliance to build a strategic foundation for improved company performance. Upon this base, loss prevention professionals use standard practices, analysis, personnel, and technology in a proactive approach to asset protection and profit enhancement. While minor differences in philosophy and focus may exist in subcategories such as grocery, restaurant, distribution or pharmacy, the major tenets of loss prevention practice remain the same.



### ENTRY-LEVEL

Entry-level management positions generally do not require an undergraduate degree, but in some instances it is preferred. General retail experience is required with some understanding of retail loss prevention. The LPQ and LPC are preferred designations.

### MID-LEVEL

Mid-level management positions demanding expertise in multiple security disciplines require an undergraduate degree in an appropriate discipline, as well as five to eight years of demonstrated success in the field in relevant retail-related LP functions. The CPP, CFI, and CFE are the preferred designations.

# School Safety and Security

The primary objective of school safety and security is to educate the campus community on the potential for crime both on and off-campus. The central themes of a campus crime prevention program are awareness, self-protection, and prevention. School safety and security has been a growing concern that has escalated in recent years. With increasing publicity about campus crime, it is likely that the trend will continue. The level of violence on and around educational institutions has brought about a great need for security at public and private educational institutions at both the elementary and secondary school levels. Many educational institutions operate a commissioned police department which makes police academy training or law enforcement certification a requirement. Interested college students can often enter this field by working for campus security departments on a part-time basis.

**ENTRY-LEVEL** Entry-level school safety and security management positions do not require an academic degree; however, a degree, general security experience, specialty-specific experience and professional certification are all desired.

**MID-LEVEL** Mid-level school safety and security management positions also do not require an academic degree; however, a degree, general security experience, specialty-specific experience, and professional certification are all desired.



## Security Engineering and Design

Architects and engineers create environments for people to live and work. These environments are created in response to aesthetic, budgetary, legal and program requirements. Historically, security has often been incorporated into design as an afterthought. Today, managers have learned that they must contain costs and collaborate with knowledgeable professionals who can incorporate security design into new or pre-existing facilities.

Costs for incorporating security features and systems skyrocket if security, like any other building feature or system, is considered after a facility is built or renovated. Inadequate security in today's climate increases the potential for loss. Risk mitigation and loss reduction can be accomplished through the employment of knowledgeable security professionals, who may also be licensed professional architects and engineers that practice in the field of security. This expertise will assist in integrating the security function into an environment at the conceptual stage while working with rapid technology innovations. The discipline is to determine the functional requirements and to let the experts handle the options.

### ENTRY-LEVEL

Entry-level positions for security consultants in architecture/engineering firms as well as architects and engineers generally require at least a bachelor's degree. Most security-related positions require some minimal experience in the field. For advancement, security design and/or engineering training as well as some specialty-specific training or experience could be required.

### MID-LEVEL

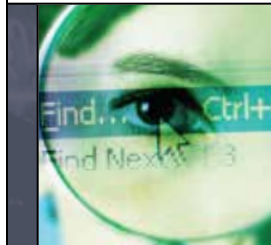
Mid-level positions generally require a bachelor's degree and five to seven years of security and/or engineering experience beyond the area of study and should require some additional specialty-specific training or experience. Professional licensing for engineers and architects should factor heavily for a mid-level position, and a PSP certification would be appropriate to indicate proficiency. Licensed and certified professionals tend to have a more global view of projects allowing them to integrate security better with other elements of building and site design. The CPP designation is not required, but it is desirable.

# Security Investigations

The process of investigation is an important function in both the public and private sectors. It is a very broad field and includes many specialties. Background investigation is an important aspect and involves gathering information used to determine the level of trust that should be granted to an individual. In the case of an organization, the term “due diligence” is generally used and is usually performed prior to a merger, acquisition, or establishment of a significant business agreement. In the commercial sector, investigators determine the facts in cases of theft, employee misconduct, computer system abuse, sabotage, threats, and potential workplace violence. They ferret out fraud, waste, abuse, financial mismanagement, and corporate ethics violations. Investigators use a variety of tools and techniques such as interviewing, evidence collection and processing, physical and technical surveillance, computer forensics, database searches, and crime analysis algorithms. Like most security measures, an effective investigations program serves both as a deterrent to crime and a response once a crime has been committed.

**ENTRY-LEVEL** Entry-level management positions generally prefer a four-year degree. A degree in security management will be beneficial in providing a grounding in security, though criminal justice has been popular and a business degree is acceptable. Depending on the position, no experience may be required but specialty areas usually require at least one to two years in the respective area. Experience from police or security investigations is taken into consideration.

**MID-LEVEL** Mid-level management positions, requiring expertise in multiple investigative and business disciplines, generally require a degree in an appropriate discipline, as well as five or more years of demonstrated success in the field. Professional certifications such as the PCI and CFE are often desired as an indicator of professionalism and qualifications.



## Security Sales, Equipment, and Services

This security specialty can be stimulating, challenging, and financially rewarding. New security-related products and services have resulted from emerging threats and evolving high technology, and the number of companies offering various security services has grown as a result. Sales positions can deal with products that range from barriers, alarm systems, sophisticated biometrics, and closed circuit television (CCTV), to biological detection equipment and risk management software. Services can range from uniformed security operations to security systems monitoring and security investigations, among others. Sales and service personnel may be employed by a product manufacturer to sell that particular company's products or by an independent dealer that represents a variety of products. Entry-level positions may involve making sales calls, handling advertising queries, staffing and organizing sales booths, demonstrating products and providing input on government proposal requests. In addition to typical management functions, mid-level management responsibilities may include directing and motivating sales personnel, organizing sales and marketing campaigns, preparing and presenting proposals, conducting briefings, and managing a trade show booth.



### ENTRY-LEVEL

Entry-level management positions may call for a college degree, depending on the size and nature of the employer. It is recommended that broad-based education and experience be achieved in areas such as accounting, industrial engineering, management, marketing, human resources, communications, statistics, or labor relations. The nature and extent of the desired education and experience and the entry-level salary range can vary depending on the type of product or service being provided, the size of the vendor, and other factors.

### MID-LEVEL

Mid-level management positions require the experience to perform a wide range of functions as indicated above. The ability to effectively deal with a range of people and the capability to present information verbally and in writing are particularly important.



# Transportation and Supply Chain Security

Security within the transportation sector includes a diverse range of activities across a range of different modes—including aviation, maritime, rail, surface, mass transit, and pipeline operations. It is one of the broadest domains in terms of the range of subjects and the environments in which people can apply their knowledge, skills, and abilities. Transportation security professionals may find themselves working for the government in policy, regulatory, and enforcement roles across any of the modes mentioned above. On the private sector side, they may be involved in protecting international supply chains, drafting protective plans, conducting guard operations or working to protect the persons, assets, information and operations at each step along the supply chain.

The challenges facing transportation security professionals are many. On one hand, they must have an understanding of terrorism, organized crime, internal loss prevention, localized crime, and how to prepare for and protect the organization from natural disasters. They must be able to work to protect a single asset within the system, or they may be involved in assisting in overseeing operations on a vast level, working to ensure the robustness, resilience, and availability of international supply chains. They may find themselves working in major infrastructure points (such as international airports or seaports) or in remote areas working to protect critical routes and trade routes. In all cases, this specialty has a wide range of challenges that have varying degrees of complexity.

**ENTRY-LEVEL** Those seeking entry level positions will benefit from a wide range of backgrounds—ranging from degrees in security management or law enforcement to civil engineering and transportation studies. They will also benefit significantly from having at least a broad understanding of civil engineering, supply chain management, airport operations, maritime operations, rail operations, trucking operations, physical security, network security, protection of automated control systems and how these relate to the various security domains. To operate in the international supply chain, the individual should also have a good understanding of geography, sociology, and cultural studies.

**MID-LEVEL** Those seeking mid-level management positions will typically require a bachelor's degree or equivalent professional experience. They must be prepared to undertake broader roles that may involve several activities and they may be called upon to participate in the coordination of multi-agency, multi-disciplinary activities. Mid-level managers should be able to relate the activities of one mode to how it may impact other modes.



## Utility and Nuclear Security

Utility operations refer to gas, water, electric, and nuclear power plants. Even though sources of power differ, there are common facilities to all utility operations. Electric sources include fossil fuel (gas, oil, and coal), water, and nuclear generation. Each facility maintains transmission and distribution systems that facilitate bulk transfers of electric, gas, and/or water over long distances and a system of smaller pipes and wires designed to distribute the commodity to the end user. Utility security professionals take appropriate measures and perform a range of duties for the protection of people, property, information, and other assets in the event of crime, natural disaster, technological emergency, resource shortage, civil disturbance, war, or terrorist activity.

### ENTRY-LEVEL

Entry-level management positions generally require a bachelor's degree, preferably in security, and five years of security or law enforcement experience. A CPP or PSP is preferred.

### MID-LEVEL

Mid-level management positions generally require a masters in business administration or security management and ten years of security or law enforcement experience. A CPP and PSP is preferred.

[Some of the information for this specialty was extracted from *Utility Security Operations Management*, authored by Clay Higgins and sponsored by the ASIS Utility Security Committee, 1989.]

# Other Security Specialty Career Opportunities

## Counterterrorism

Counterterrorism is an area that reaches beyond security, per se, but deals with a critical area of concern, of which security professionals need to be aware. Those who specialize or focus in this area may become engaged in preparing intelligence assessments of suspected groups or risk assessments of geographical areas, or conducting threat awareness briefings, or developing policies, procedures and countermeasures to deal with the potential threat, or other related activities.

## Executive Protection

Individuals who work in the executive protection field can perform a range of functions, from conducting a risk assessment of a protectee, to performing trip and site advances for a protectee's movements and coordinating plans to deal with a range of contingencies. The roles and responsibilities can extend well beyond the visible physical protection function that many people associate with this specialty.

## Security Consulting

Security consulting can involve a variety of specialties and activities, depending on the background and interests of the consultant. They can range from conducting security risk assessments to crafting security policies and procedures to preparing security equipment specifications to developing contract proposals among others.

## Security Education

Security education entails preparing and presenting security courses as a full-time or part-time faculty member, at the associate, baccalaureate, or graduate level. As an adjunct or part-time faculty member, practical experience involving the topics to be taught is particularly significant. Educators must have solid practical experience but also be able to develop and deliver course content in an academic environment (classroom and/or online) at the college or university level.



### **Security Training**

Security training includes a broad array of activities to ensure that an organization’s employees, managers and/or security staff are aware of threats, adverse impacts, and security policies and procedures. It can include training needs assessments, development of training material, and presentation of material in a wide variety of formats from live presentations to computer-based training, banners, posters, newsletters, and social media. Some security trainers fill proprietary positions while others are hired on a contract basis.

### **Special Event Security**

Special events can range from conventions and trade shows to concerts, rallies, ceremonies, and various sporting events. Some individuals in this specialty may coordinate security for events within their organization or facility while others work under contract to the activity hosting the event. Either way, this specialty can entail substantial coordination with an array of agencies and individuals.



# ASIS INTERNATIONAL

ASIS International (ASIS) is the leading organization for security professionals, with more than 38,000 members worldwide. For nearly 60 years, security professionals across the globe have relied on ASIS to provide the resources needed to succeed.

ASIS members represent virtually every industry in the public and private sectors. From students studying security management to entry level managers to chief security officers, from security veterans to consultants and those transitioning from law enforcement or the military—all find a professional home at ASIS.

ASIS promotes excellence and leadership in the security management profession through its diverse range of offerings including certifications, education programs, council service, and chapter events. In addition, ASIS offers security professionals access to the industry's largest, most comprehensive library; a robust online career center; peer-reviewed books and publications; indispensable industry standards; and the award-winning *Security Management* magazine. ASIS also advocates for security and security professionals, communicating the role, value, and concerns of its members and the industry to the business community, government officials, news media, and the public.

## Key Offerings

### ASIS International Annual Seminar and Exhibits

The world's most influential security event, the Annual Seminar and Exhibits attracts 20,000+ security professionals for four days of education, exhibits, and networking with peers from every industry sector.

### Board Certifications

ASIS offers three certifications that provide objective proof of an individual's knowledge, skills, and abilities: Certified Protection Professional (CPP), Professional Certified Investigator (PCI), and Physical Security Professional (PSP). ASIS was the first organization to offer a board certification specifically for security managers and our program remains the gold standard.





### **Standards and Guidelines**

An ANSI-accredited Standards Developing Organization, ASIS works with national and international standards-setting organizations to advance security practices worldwide through the development of standards and guidelines within a voluntary, non-proprietary and consensus-based process.

### **CSO Roundtable**

The CSO Roundtable provides a dedicated forum for the most senior security professionals from the largest and most influential organizations in the world.

### **ASIS Foundation**

The ASIS Foundation is a 501(c)(3) nonprofit organization dedicated to providing high-quality, contemporary research, and education opportunities that serve to enhance the security profession. Additionally, the Foundation awards dozens of scholarships each year to help ensure that those pursuing a security management career are able to achieve their professional goals.

### **Special Networking Groups**

ASIS offers 29 niche councils where security managers can learn from peers within their specific industry sector. From Crime and Loss Prevention to Crisis Management, there is sure to be a council that meets your professional needs. In addition, the ASIS Young Professionals and Women in Security Working Group provide specialized education, networking, and mentoring services to support these emerging communities within the membership body.

### **Connect with ASIS International on social platforms**



[www.youtube.com/ASISInternational](http://www.youtube.com/ASISInternational)

[www.facebook.com/ASISInternational](http://www.facebook.com/ASISInternational)

[www.twitter.com/ASIS\\_Intl](http://www.twitter.com/ASIS_Intl)

<http://bit.ly/asislinkedin>





1625 Prince Street  
Alexandria, VA 22314-2818  
USA  
703-519-6200  
Fax: 703-519-6299  
[www.asisonline.org](http://www.asisonline.org)