Careers in Cybersecurity

Learning Objectives

After reading this chapter, you will be able to:

- Understand important of information security as profession.
- Get an overview of information security (IS) Organization.
- Learn different roles and responsibilities from IS Organization.
- Understand different career paths.
- Discover career guide path and respective certifications.

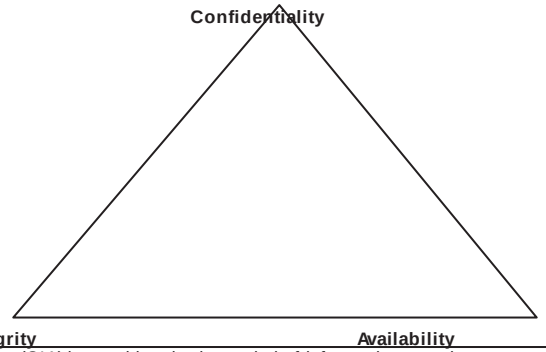
12.1 Introduction

Cybersecurity refers to information security; it is all about protecting the confidentiality, integrity and availability of information (see Fig. 12.1). Information security means not only protecting information but also protecting information systems and information assets from unauthorized access, use, disclosure, disruption, modification or destruction.[1]

All organizations, including government organizations, military, financial institutions, hospitals and private sector companies, gather, process and store a great deal of confidential information about their products and services, Research and Development (R&D), employees, vendors, contractors, customers and financial operatioans. Electronic media is predominantly used to collect, process and preserve these informa- tion and then the information is transmitted across the boundaries through Internet. Every organization operates on E-Mail system, and on Intranet of the Organization, as a minimum IT Infrastructure; thus, computer network became a backbone to every business. Many organizations also use virtual private net- works (VPN) for securing communication channel.

Protecting confidential and sensitive information is a business requirement, and in many cases it became an ethical and legal requirement. Businesses also need information security to protect their trade secrets, pro- prietary information and personally identifiable information (PII) of their customers or employees (see Fig. 12.2 and Section 5.3.1, Chapter 5 to know more on this topic). Besides business, for an individual, infor- mation security has a significant effect on privacy, which can result in ID theft. Therefore need for informa- tion security as well as for information assurance is on the verge of a new millennium.

Importance of cybersecurity to companies, government organizations and to individuals is continuously increasing due to rise in cyberattacks every year (see case illustrations and examples provided in Chapter 11 in CD and also see the discussion in Chapter 9). Privacy and the protection of data has become a key issue with the concerns over identity theft and related cybercrimes.



*C*onfidentiality, *I*ntegrity and *A*vailability (CIA) is considered to be a triad of information security components. The security objective can be considered as achieved when the information is disclosed to only those who have the right to know (confidentiality), information is protected against unauthorized changes (integrity), information systems are available and usable (availability) and transactions are not disputed (non-repudiation and authenticity). Information systems are decomposed into three main portions, namely, hardware, software and communication channels with the purpose to identify and apply information security industry standards,
as mechanisms of protection and prevention, at three levels or layers such as physical, personal and organizational. Essentially, procedures or policies are implemented to educate the workforce (administrators, users and operators) and how to use products to ensure information security within the organizations.

Figure 12.1 | CIA triad.

I. Organization – Internal Information
- About
  - (a) Employees
  - (b) Prospective employees
  - (c) Former employees
- Documentation
  - (a) Corporate policy
  - (b)) Organizational Guidelines to Protect information about Employees
  - (c) Corporate Instructions

II. Customer Information
- About
  - (a) Current customers
  - (b) Potential customers
  - (c) Former customers (as long as information is required for business purposes)
  - (d) Visitors to organization websites
- Documentation
  - (a) Corporate Instructions on Marketing and Legal

III. Commercial Information
- About
  - (a) Customers of organization's/customers (e.g., banking customers of a financial segment customer)

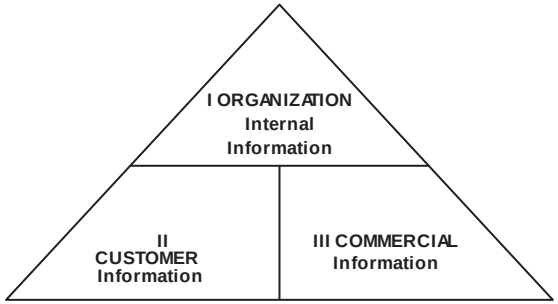


Figure 12.2 | Types of personal information in organizations.

Information systems can generate many direct and indirect benefits and also as many direct and indirect risks. h ese risks have led to the gap between the need to protect systems and the degree of protection applied. h e gap is caused by

1. Widespread use of technology.
2. Interconnectivity of the system.
3. Elimination of distance, time and space as constraints.
4. Unevenness of technological changes.
5. D evolution of management and control.
6. Attractiveness of conducting unconventional electronic attacks against organizations.
7. External factors such as legislative, legal and regulatory requirements.

All these results in new risks that could have significant impact on critical business operations such as

1. Increasing requirements for availability and robustness.
2. G rowing potential for misuse and abuse of information systems affecting privacy and ethical values.
3. External dangers from hackers, leading to denial-of-service and virus attacks, extortion and leakage of corporate information.

Typically, to maintain and monitor the computer network, every organization designates Network Specialist titled as Network Administrator or Information Security Manager or N etwork Security Specialist. Along with protecting organization's computer network (i.e., LAN/WAN), information security has also become an integral part of their responsibilities. In the large organizations, group of people are deployed to cater security of IT infrastructure and Information processing facilities. h e field of information security has grown significantly in recent years. h ere are many areas for specialization including Information Systems Auditing, Business Continuity Planning and Digital Forensics Science – one of the most exciting segments of the cybersecurity field is cyberforensics and investigation. Experts in this field investigate cybercrime and attacks after they happen and attempt to track down the perpetrators. Local law enforcement agencies and central government agencies such as CBI or Federal agencies in USA such as the FBI all employ cyberse- curity professionals in this capacity. h is calls a need of a cybercrime lawyer to provide a legal advice to the victims of cybercrimes to file a case and recover the money and/or protect their information assets.

Sometimes, like many technocrats and cybersecurity professionals might work as independent contractors, hired by companies when they are designing a new system or have had some kind of cybercrime committed against them. h is system, while giving flexibility, also requires business savvy on the part of the employee to manage clients and continually look for work.

While cybersecurity has played a major role in the banking industry and other large corporate transac- tional businesses for some time, even small companies are facing cybersecurity issues today. With the advent of E-Commerce, network security has taken on an even larger role as financial transactions and personal information such as credit card numbers are passed along computer networks with even greater frequency. Cybersecurity is also an important function inside companies, as employee data must be kept private and confidential according to the law

9/11 terrorist attacks in New York, USA and 11/26 terrorist attacks in Mumbai, India have raised a new urgency to the problem of cybersecurity, and forced government agencies to put their efforts in the direction of cybersecurity research and monitoring. h e ongoing struggle against terrorism and the quest for emergency preparedness and disaster preparedness have put a continued urgency into the field of cyber- security as well. O rganizations are also facing a new scrutiny in how to handle their data in the wake of corporate scandals. In short, the cybersecurity field is growing, and those with the proper training and experience will find plenty of opportunities.

The US Department of Labor estimates that job growth for system administrators (a loose term including cybersecurity experts) will be one of the fastest growth among all professions, growing at a rate of approxi- mately 25% until 2014.[2] It is estimated by NASSCOM that the demand for cybersecurity professionals would be around 90,000 by 2010 in India, whereas worldwide this figure is estimated to be around 200,000; however, the industry estimates much higher demand in the local as well as overseas market. With such demands, it is estimated that there would be a shortfall of 35,000–45,000 cybersecurity professionals in India alone.[3]

The growing field of cybersecurity is about managing the risk inherent in these systems. The main contribu- tors toward rise in demand for IT security are:

1. Corporate scams.
2. Cybercrimes on the rise.
3. Compliance with various laws and regulations.
4. Competitive market – opportunities for professional certifications in IT security.
5. Rise in outsourcing.

Cybersecurity is a complex subject. To protect information system and Information Technology (IT) environ- ment one must understand the environment, fixes to be applied, difference between vendor applications and hardware variations and how attacks are preferred.

12.2 IT Security Organization

Information security activities should be co-coordinated throughout the organization to ensure consistent application of the security principles, axioms and policy statements. Although the Executive Directors have charged the Security Committee with the task of securing organizations' assets, however, each organiza- tion has their IT security organization structure established. One of the vital aspects behind understanding the management structure is to know the growth opportunities within the organization. The organization chart for information security/IT security may vary from organization to organization depending on the size, complexity of the organization and nature of business handled by each organization. See Fig. 12.3 as a sample organization chart based on ISO 27001 certification.[4] It is important to note that this may not be exactly how the security function is structured in each organization.

12.2.1 Roles and Responsibilities

Figure 12.3 displays various titles and before discussing about the skills and/or relevant certifications, let us understand the role of these titles.

Senior Level/Executive Level

Those appointed in this level are also called as C-Executives (CEO/CFO/CIO), who have overall respon- sibility of information security within the organization and provide the directives about overall busi- ness objectives to enable the middle-level management to chalk out IT Plan, aligned with business requirements.

Chief Executive Officer (CEO)

CEO's primary focus is on the business, in turn, generating the revenue for the organization and increasing the profits. Hence, CEO[5] sets the directives and strategy for the organization to follow. Being at the senior

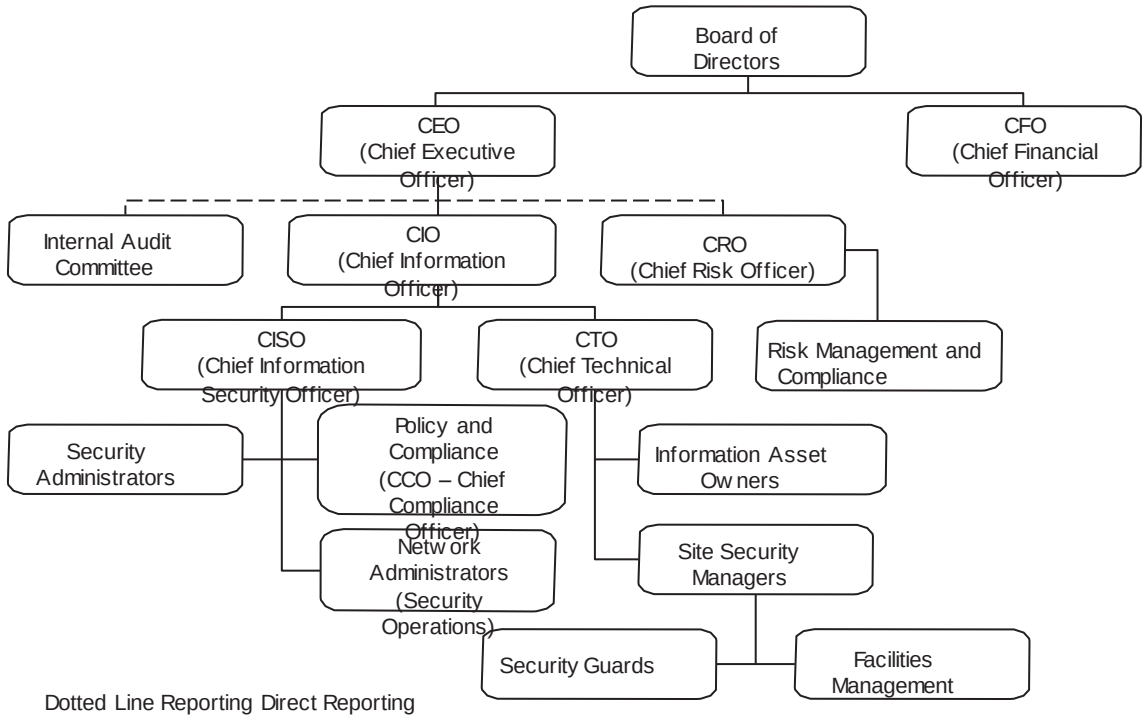


Figure 12.3 | IT security organization chart.

most position in the organization, the CEO is liable to government prosecutors and has signing authority which binds the CEO with the organization.

Chief Financial Officer (CFO)

The CFO[6] is in charge of controls over capital and other areas, including financial accounting, human resources and information security. Subordinates such as the CIO usually report to the CFO. As an organization officer, the CFO is liable to government prosecutors.

Chief Information Officer (CIO)

The CIO[7] is subordinate to the CEO. The CEO is still considered to be the primary person responsible for internal control. A CIO might not be a true Organization officer. An exception may be the CIO in the corporate

headquarters. The CIO title may bear more honor than actual authority, depending on the organization. The CIO has mixed liability depending on the issue and their actual position in the organization.

Middle Level

These executives are responsible to oversee the day-to-day operations as per the guidelines/strategies laid down by Senior Executives. In large organizations (i.e., MNCs) CIO may get counted into middle-level management.

Chief Technical Officer (CTO)

More commonly Chief Technology Officer[8] is an executive-level position in an organization, whose occupant is focused on scientific and technological issues within an organization. It typically involves overseeing Research and Development (R&D) activities, and formulating long-term visions and strategies at the officer level. Essentially, a CTO is responsible for the transformation of capital – be it monetary, intellectual or political – into technology in furtherance of the Organization's objectives. They must typically combine a strong technical or scientific background with business development skills.

The role became prominent with the ascent of the IT industry, but has since become prevalent in technology-based industries of all types (e.g., biotechnology, energy, etc.). As a corporate officer position, the CTO typically reports directly to the CEO and is primarily concerned with long-term and "big picture" issues (while still having deep technical knowledge of the relevant field). Depending on an organization structure and hierarchy, there may also be positions such as Director of R&D and VP of Engineering whom the CTO interacts with and/or oversees. The CTO also needs a working familiarity with Regulatory and Intellectual Property (IP) issues (e.g., patents, trade secrets, license contracts), and has an ability to interface with legal counsel to incorporate those considerations into strategic planning and inter-organization negotiations.

Chief Information Security Officer (CISO)/Chief Security and Privacy Officer (CSPO)

CISO[9] is responsible for establishing and maintaining the organization vision, strategy and program to ensure information assets are adequately protected. The CISO provides directions to IT staff in identifying, developing, implementing and maintaining processes across the organization to reduce information and IT risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of policies and procedures. The CISO is also usually responsible for information-related compliance. The CISO reaches the entire organization and responsibilities include:

1. Information security and assurance.
2. Information risk management and IT controls for financial and other systems.
3. Information privacy.
4. Computer Emergency Response Team/Computer Security Incident Response Team.
5. Identity and access management.
6. IT security architecture.
7. IT investigations, digital forensics, E-Discovery.
8. Disaster recovery and business continuity management.
9. Information Security Operations Center (ISOC).
10. Information regulatory compliance (e.g., PCI-DSS, HIPAA).
11. Management self-compliance (e.g., ISO 27001, ISO 20000).

Box 12.1 CSO Magazine

CSO magazine is published by CXO Media Inc., which is an IDG organization (International Data Group, USA). CSO provides news, analysis and research on a broad range of security and risk management topics. CSO focuses on areas such as information security, business continuity, identity and access management, physical security, etc.

Source: http://www.csoonline.com (30 October 2010).

Having a CISO or the equivalent function in the organization has become a standard in most business, both in government and non-profit sectors. Throughout the world, a growing number of organizations have a CISO [also called as CSO – Chief Security Officer (see Box 12.1)]. By 2009, approximately 85% of large organizations had a security executive, up from 43% in 2006 to 56% in 2008. About one-third of these security chiefs reports to a Chief Information Officer (CIO), 35% to Chief Executive Officer (CEO) and 28% to the Boards of Directors.

In the large Global IT organizations, the roles of CISO and CSPO (Chief Security and Privacy Officer) may be handled by different persons. This role is typically an executive role wherein CSPO is expected to play a strategic role for the organization and to provide vision for Data Privacy Information Security and Broad Guidelines.

1. Create and chair security and privacy team.
2. Lead the security and privacy team and build data privacy competence team.
3. Liaise with cross-functional teams (contracts, legal, IT security, etc.)
4. Act as a single point of focus on regulatory compliance matter queries relating to data privacy and information security.
5. Address clients' concerns on data security and privacy (protection measures, assessment programs, etc.).
6. Address business implications of privacy and security challenges.
7. Conduct privacy assessment of organization's internal tools.
8. Address data privacy concerns with external vendors, contractors and other third-party service providers.
9. Align the data security and privacy (DS&P) agenda with the other global teams of the organization.
10. Represent the organization externally as needed on these topics with clients, government officials and others.

Chief Risk Officer (CRO)

Chief Risk Officer (CRO)[10] of a corporation is the executive accountable for enabling the efficient and effective governance of significant risks, and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, operational, financial, compliance-related or reputational. CRO's are accountable to the Executive Committee and the Board for enabling the business to balance risk and reward. In more complex organizations, they are generally responsible for coordinating the organization's Enterprise Risk Management (ERM) approach. The position became more common after the Basel Accord, the Sarbanes-Oxley Act and the Turnbull Report.

A main priority for the CRO is to ensure that the organization is in full compliance with applicable regulations. They may also deal with topics regarding insurance, internal auditing, corporate investigations, fraud and information security. CRO's serving in the large and complex organizations, typically have post-graduate education and 20+ years of business experience, with actuarial, accounting, economics and legal backgrounds common.

Chief Compliance Officer (CCO)

CCO [11] of an organization is the officer primarily responsible for overseeing and managing compliance issues within an organization. CCO ensures that an organization is in compliance with regulatory require- ments, and that the organization and its employees are complying with internal policies and procedures. h e role has long existed at companies that operate in heavily regulated industries such as financial services and healthcare. For other companies, the rash of recent accounting scandals, the Sarbanes-Oxley Act and the recommendations of the US Federal Sentencing Guidelines have led to additional CCO appointments. Scott Cohen, editor and publisher of Compliance Week, dates the proliferation of CCOs to a 2002 speech by SEC (Securities and Exchange Commission, US) commissioner Cynthia Glassman, in which she called on companies to designate a "corporate responsibility officer." h e responsibilities of the position often include leading enterprise compliance efforts, designing and implementing internal controls, policies and procedures to assure compliance with applicable local, state and federal laws and regulations and third-party guidelines; managing audits and investigations into regulatory and compliance issues and responding to requests for information from regulatory bodies.

Technical Operations Level

System Administrator

Systems administrator,[12] or sysadmin, is a person employed to maintain and operate a computer system and/or network. System administrators may be members of an IT or Electronics and Communication Engineering department.

h e duties of system administrator are wide-ranging, and vary widely from one organization to another. Sysadmins are usually charged with installing, supporting and maintaining servers or other computer systems, and planning for and responding to service outages and other problems. O ther duties may include scripting or light programming, project management for systems-related projects, supervising or training computer opera- tors and being the consultant for computer problems beyond the knowledge of technical support staff. To per- form their job well, a system administrator must demonstrate a blend of technical skills and responsibility.

A system administrator's responsibilities might include:

1. Analyzing system logs and identifying potential issues with computer systems.
2. Introducing and integrating new technologies into existing data center environments.
3. Performing routine audits of systems and software.
4. Performing backups.
5. Applying operating system updates, patches and configuration changes.
6. Installing and configuring new hardware and software.
7. Adding, removing or updating user account information, resetting passwords, etc.
8. Answering technical queries.
9. Responsibility for security.
10. Responsibility for documenting the configuration of the system.
11. Troubleshooting any reported problems.
12. System performance tuning.
13. Ensuring that the network infrastructure is up and running.

Network Administrator

Network Administrator[13] is a modern professional responsible for the maintenance of computer hardware and software that comprises a computer network. h is normally includes deploying, configuring, maintaining

and monitoring active network equipment. A related role is that of the network specialist, or network analyst, who concentrates on network design and security.

The Network Administrator or Network Admin is usually the level of technical/network staff in an organization and will rarely be involved with direct user support. The Network Administrator will concentrate on the overall integrity of the network, server deployment, security and ensuring that the network connectivity throughout an organization's LAN/WAN infrastructure is on par with technical considerations at the network level of an organization's hierarchy. Network Administrators are considered as Tier 3 support personnel that only work on break/fix issues that could not be resolved at the Tier 1 (i.e., helpdesk) or Tier 2 (desktop/network technician) levels.

Depending on the organization, the Network Administrator may also design and deploy networks. However, these tasks may be assigned to a Network Engineer in the large organizations wherein Network Administrator has a focused role of managing and monitoring the organization's network.

The actual role of the Network Administrator will vary from organization to organization, but will com- monly include activities and tasks such as network address assignment, assignment of routing protocols and routing table configuration as well as configuration of authentication and authorization – directory services. It often includes maintenance of network facilities in individual machines, such as drives and settings of per- sonal computers as well as printers. It sometimes also includes maintenance of certain network servers: file servers, Virtual Private Network (VPN) gateways, intrusion detection system, etc.

Network specialists and analysts concentrate on the network design and security, particularly trouble- shooting and/or debugging network-related problems. Their work can also include the maintenance of the network's authorization infrastructure as well as network backup systems.

3. Career Paths in Cybersecurity

IT security is transforming from tactical strategies to information risk management. The traditional role of IT security was limited to managing organization's network, firewall configurations and antivirus updates, which beginners in any organization are exposed to. The role of the professionals has been evolved to protect the enterprise from information loss and outages. With maturity and experience, at Senior Management level, IT security official would have to justify the cost of ongoing and future investments to mitigate information risks. Aligning business objectives with a concise security strategy is a critical element in this role.

1. Assurance and Compliance Security Audit

Let us understand the two terms *Assurance* and *Compliance* before we get into the discussion upon types of Assurance and Compliance Security Audits.

1. **Assurance:** Assurance[14] refers to activities designed to reach a measure of confidence. Assurance is different from audit, which is more concerned with compliance to formal standards or requirements.
2. **Compliance:** Compliance[14] is a discipline, set of practices and/or organizational group that deal with adhering to laws, regulations, standards and contractual arrangements. It is also the adher- ence to requirements. Data Governance programs often support many types of compliance require- ments: regulatory compliance, contractual compliance, adherence to internal standards, policies and architectures, and conformance to rules for data management, project management and other disciplines.

2 Types of Assurance and Compliance

Legal Compliance

Organization requires to comply with certain laws, regulations and business rules, which is a MANDATORY compliance. Any failure toward regulatory compliance leads either heavy penalties or may result into wind- ing up the business. For example, Sarbanes-Oxley Act. (see Chapter 6 to understand legal perspectives of cybercrime.)

Contractual Obligation

Organizations have certain security-related requirements enforced by the customers and stated in the engage- ment contract to which organization has to abide and demonstrate the compliance. For example, Data Security Audits, SAS70 Assessments.

Self-Initiative (Self-Compliance)

Management decides and committed to obtain certain certifications like ISO 9000 that is related with Quality Management System (QMS), which may help to build customer's confidence about the processes established into an organizations and may result the business growth. Similarly, certifications related with IT security also has a vital importance nowadays and Internal Security Team is responsible for implementation and ongoing compliance of these ISO standards.

1. **ISO/IEC 27001:** Information Security Standard is published jointly by ISO (the International Organization for Standardization) and IEC (the International Electro technical Commission). the ISO/IEC 27000-series (ISO27k) provides best practice recommendations on overall informa- tion security management, risks and controls and hence also known as ISMS (Information Security Management System) Family of Standards. ISO 27002 has been evolved from BS 7788 and incor- porates both parts of BS 7799. BS 7799 (Part I) provides an outline for information security policy whereas BS 7799 (Part II) provides a certification.
2. **ISO/IEC 20000:** his is the first international standard for IT Service Management. It has been evolved from BS 15000 Standard, which in turn is based on ITIL (Information Technology Infrastructure Library) framework. ISO/IEC 20000-1 describes the best practices for service man- agement whereas ISO/IEC 20000-2 states code of practice.
3. **BS 25999:** his is published by BSI (the British Standards Institution), BS 25999 is a BCM (Business Continuity Management) standard. BS 25999-1:2006 (Part I) states code of practice and BS 25999-2:2007 (Part II) specifies requirements for implementing, operating and improving BCMS (Busi

Many Institutions/Certifying Bodies conduct the courses on "Lead Auditor," "Auditor" and "Implementer" on these ISO/BS Standards. Aspirants should ensure that such courses are authorized by IRCA, without which these certifications do not have any global recognition in the industry.

4. **COBIT:** Information security has been spread and given prime importance by the Senior Management, which leads to many organizations implement their processes based on some estab- lished framework and/or guideline. COBIT (Control Objectives for Information Technology) is an IT

control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. Management may engage the external consultant to conduct the assessment on their IT Processes based on COBIT framework that may help the management to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework and/or any other ISO Certification requirements.

The Assurance and Compliance team assists management to establish the compliance and sustain it throughout the lifecycle. The compliance team becomes a liaison between the management and external agencies such as client and/or assessors (auditors).

3. Network Security

Besides the role of System Administrator and Network Administrator, which we have discussed in the earlier section, Vulnerability Assessment and Penetration Testing (VAPT) is another niche field (see Appendix E in CD) which requires fundamental knowledge of networking. One may target his move toward ethical hacking or forensics investigator, after gaining significant amount of experience into VAPT and/or network security.

4. Cybercrime Investigation and Litigation

Increased number of cybercrime within last few years, created the need for cybercrime legal professionals. Many universities and institutions have "cybercrime and cyberlaw" as a separate subject under the curriculum of lawyers' stream of education. Besides university courses, Asian School of Cyber Laws also has recognition within India and the institute conducts the courses on Cybercrime Investigator. (www.asianlaws.org).

5. Computer Forensics

Computer forensics involves conducting investigations, data recovery and E-Discovery (see Chapters 7 and 8). One needs to have a solid foundation of technical experience and expertise as well as possess strong communication skills.

Forensics Auditing

Forensics Auditing[15] is also called Forensics Accounting that includes the steps needed to detect and deter fraud. Forensics auditors must have a bachelor's degree either from Commerce/Law stream or from Foresenics field and can work in industries such as law and financial services. Few universities segregate the area of "litigation support" and "investigative accounting." According to the Association of Chartered Certified Accountants, Forensics auditors help investigate how long the fraud occurred and how the perpetrator carried it out. Forensics auditors can also act as expert witnesses in court proceedings.

The job scope is very wide. Let's look at the key responsibilities as mentioned below:

1. Plan, organize, conduct and manage a variety of computer forensics examination activities such as conducting live analysis on networks and multiple platforms.
2. Provide advices on related technical issues to enhance forensics engagements.
3. Provide computer forensics services such as digital evidence preservation, analysis, data recovery, tape recovery, E-mail extraction, database examination, etc.
4. Manage and perform comprehensive technical analyses and interpretation of computer-related evidence such as E-Mail, accounting software, various

5. Ensure that evidence collection methods are conducted, managed and archived in a manner consistent to maintain preservation and protection of data and evidence.
6. Ensure that all laboratory hardware and software are verified and validated as required by the State Law.
7. Evaluate and troubleshoot a variety of technical issues including hardware and software troubleshooting.
8. Conduct security assessments, penetration testing, and ethical hacking and conduct exams on compro- mised computers and servers.
9. Work according to budget by completing it within the timeframe.
10. Perform other job-related duties as necessary such as demonstrating effective communication and work closely with partners, managers, staff and clients.

Cybersecurity Certifications

Security certifications are accreditation programs organized by institutes and/or governing bodies to endorse the candidates skill set and core knowledge of information security. h e importance of grabbing these certi- fications is becoming a vital step to beat the competitive edge. A dedicated magazine has been published for all types of certifications to build awareness among professionals (see Box 12.2).

Acquiring these security certifications is a two step process:

1. **Successfully scoring the minimum passing score in the examination:** h e candidate is assessed on the "Common Body of Knowledge" designed for respective certification.
2. **Awarding the Certification:** Awarded after completion upon certain criteria such as qualifications specified by a certifying authority, proof of professional accomplishments, achieving a specified grade in an examination or some combination thereof. h e intention is to establish that the candidate holding a certification is technically qualified to hold certain types of position within the field.

Certifications, usually, need to be renewed periodically, or may be valid for a specific period of time (i.e., the lifetime of the product upon which the individual is certified). As a part of a complete renewal of an individual's certification, it is common for an individual to show evidence of continual learning – often termed as CPE (Continuing Professional Education) to be demonstrated by earning continuing education units (CEU).

12.4.1 Classification of Certifications

Information Security Certifications can be classified as "vendor-specific" and "vendor-neutral" certifications. Table 12.1 lists the numerous certifications that have global recognition.

Box 12.2 Certification Magazine

Certification magazine is a publication dedicated to information about technical certification and technology education. They cover specific technical certifications as well as soft skills training, such as communication and presentation skill development. Certification magazine also includes links to information about technology education and trends in the technology job market. Certification Magazine can be found online at www.certMag.com

Table 12.1 | Information security-related certifications

Certification Body	*Certifications*
I Vendor-specific certifications	
Microsoft	MCSE • MCSA RHCSA •
Red Hat (Linux) Cisco	RHCSS
Systems Checkpoint	CCNA • CCNP • CCSP • CCWP
	CCSPA • CCSA • CCSE • CCMSE • CPCS
II Vendor-neutral Certifications	
CompTIA SCP	Security+
(ISC)² ISACA BCM	SCNS • SCNP • SCNA
ITIL	SSCP • CAP • CSSLP • CISSP • ISSAP • ISSEP • ISSMP CISA • CISM •
EC-Council	CGEIT • CRISC
	BCCP • BCCS • BCCE • DRCS • DRCE • BCCA • BCCLA
	ITIL–Foundation • ITIL–Practitioner • ITIL–Manager
CWNP	ENSA • CEH • CHFI • ECSA • LPT • CNDA • ECIH • ECSS • ECVP • EDRP •
IAPP	ECSP • ECSO
GIAC	CWTS • CWNA • CWSP • CWDP • CWAP • CWNE CIPP • CIPP/G •
	CIPP/C • CIPP/IT
ISECOM	GSIF • GSEC • GCFW • GCIA • GCIH • GCUX • GCWN • GCED
Offensive Security	• GPEN • GWAPT • GAWN • GISP • GLSC • GCPM • GLEG
Mile2	• G7799 • GSSP-NET • GSSP-JAVA • GCFE • GCFA • GREM • GSE
CREST	OPST • OPSA • OPSE • OWSE • CTA OSCP • OSCE •
IACRB	OSWP
eLearnSecurity	CPT Engineer (CPTE) • CPT Consultant CREST Consultant
CERT	CPT • CEPT eCPPT CSIH
CSA CSI	CCSK CSFA

Vendor-specific certifications cover the security aspects related with proprietary technology and/or system. h ese certifications are valid to the specific version of the system or model of the device. In-depth knowledge of operation and configuration settings for the respective product can be gained by acquiring these certifications. Vendor-neutral certifications focus on security strategies and conceptual understanding about IT and different components for information security architecture. h ese certifications are not based on any, one technology platform but cover the universe of IT from the perspective of IT Process Controls. Table 12.2 lists important certifications, which are popular among the IT security professionals and are subset of the certifications mentioned in Table 12.1.

Table 12.2 | List of important certifications

Sr. No.	Certification	Certification Description	Website	Certification Details
1	MCSA	*M*icrosoft *C*ertified *S*ystems *A*dministrator	http://www.microsoft.com/learning/en/us/certification/mcsa.aspx	MCSA certification enables to manage and troubleshoot network environments based on the Windows Server 2003 operating system. It reflects a unique set of skills required to succeed in a variety of job roles, such as systems administrator, network administrator, information systems administrator, network operations analyst, network technician and technical support specialist.
2	MCSE	*M*icrosoft *C*ertified *S*ystems *E*ngineer	http://www.microsoft.com/learning/en/us/certification/mcse.aspx	MCSE certification helps in designing, implementing and administering infrastructures for business solutions based on Windows Server 2003 and Microsoft Windows 2000 Server. Implementation responsibilities include installing, configuring and troubleshooting network systems.
3	CCNA	*C*isco *C*ertified *N*etwork *A*ssociate	http://www.cisco.com/web/learning/le3/le2/le0/le9/learning_certification_type_home.html	CCNA certification enables to install, configure, operate and troubleshoot medium-size route and switched networks, including implementation and verification of connections to remote sites in a WAN. CCNA curriculum also includes basic mitigation of security threats, introduction to wireless networking concepts and terminology, and performance-based skills.
4	CCNP	*C*isco *C*ertified *N*etwork *P*rofessional	http://www.cisco.com/web/learning/le3/le2/le37/le10/learning_certification_type_home.html	CCNP enables to plan, implement, verify and troubleshoot local and wide-area enterprise networks and work collaboratively with specialists on advanced security, voice, wireless and video solutions. he CCNP certification is appropriate for those with at least 1 year of networking experience who are ready to advance their skills and work independently on complex network solutions.
5	SCNS	*S*ecurity *C*ertified *N*etwork *S*pecialist	http://www.securitycertified.net/Certifications/SCNS.aspx	SCNS curriculum provides the knowledge about Network Defense Fundamentals, Hardening Routers and Access Control Lists, Implementing IPSec and Virtual Private Networks, Securing Wireless Networks, Designing and Configuring Intrusion Detection System, Designing and Configuring Firewall Systems.

(*Continued*)

Table 12.2 (*Continued*)

Sr. No.	Certification	Certification Details		
			Website	Description
6	SCNP	*S*ecurity *C*ertified *N*etwork *P*rofessional	http://www.securitycertified.net/Certifications/SCNP.aspx	SCNP curriculum provides the knowledge about analyzing Network Packet Structures, Creating Security Policies, Performing Risk Analysis, Internet and WWW Security, Cryptography, Hardening Linux Computers, and Windows Server 2003.
7	SSCP	*S*ystems *S*ecurity *C*ertified *P*ractitioner	www.isc2.org	SSCP is designed for the professionals who implement the plans and policies designed by Information Security Managers and equip with technical implementation side of information security systems and the ability to collaborate with those that write policy.
8	CISSP	*C*ertified *I*nformation *S*ystems *S*ecurity *P*rofessional	www.isc2.org	CISSP covers variety of information security topics. CISSP establishes a common framework of information security terms and principles that allow information security professionals to understand and resolve matters pertaining to information security profession with a common understanding.
9	CSSLP	*C*ertified *S*ecure *S*oftware *L*ifecycle *P*rofessional	www.isc2.org	CSSLP is designed to provide an ability to mitigate the security concerns and risks that surround application development throughout the SDLC (i.e., from the original specification and design through implementation, maintenance and disposal).
10	CISA	*C*ertified *I*nformation *S*ystems *A*uditor	www.isaca.org	CISA covers the entire gamut of information security and IT security. CISA equips the professional with an approach to conduct information system audits.
11	CISM	*C*ertified *I*nformation *S*ecurity *M*anager	www.isaca.org	he objective of CISM is to provide a common body of knowledge for Information Security Managers (ISM) to focus upon information risk management and to govern information security as well as on practical matters such as developing and managing an information security program along with managing incidents.
12	CEH	*C*ertified *E*thical *H*acker	www.eccouncil.org	he ethical hacker is employed by the organization, which trusts him/her to attempt to penetrate networks and/or computer systems, using the same methods as a cracker, for the purpose of finding and fixing computer security vulnerabilities.

Table 12.2 (*Continued*)

Sr. No.	Certification	Certification Description	Website	Certification Details
13	CHFI	*C*omputer *H*acking *F*orensics *I*nvestigator	www.eccouncil.org	Tools and techniques used for conducting Computer Investigations, be it computer crime, digital forensics, computer investigations or even standard computer data recovery, are covered under CHFI and prepare the aspirants to conduct computer investigations using groundbreaking digital forensics technologies.
14	LPT	*L*icensed *P*enetration *T*ester	www.eccouncil.org	EC-Council's Certified Security Analyst (LPT) program is designed to deliver advanced uses of the LPT methodologies, tools and techniques required to perform comprehensive information security tests and design, secure and test networks to protect your organization from the threats hackers and crackers pose.
15	CWNP	*C*ertified *W*ireless *N*etwork *A*dministrator	www.cwnp.com/cwna	CWNA begins with wireless fundamentals to the unique security requirements of 802.11 networks, plus network and protocol analysis.
16	CWSP	*C*ertified *W*ireless *S*ecurity *P*rofessional	www.cwnp.com/cwsp	CWSP emphasizes security threats and weaknesses of wireless LANs, and covers hardware, software, protocols, procedures and design techniques used in reducing wireless LAN security risks.
17	CIIP/IT	*C*ertified *I*nformation *P*rivacy *P*rofessional/*I*nformation *T*echnology	www.privacyassociation.org/certification/cipp_it	CIPP/IT professional assesses understanding of privacy and data protection practices in the development, engineering, deployment and auditing of IT products and services.
18	BCCLA	*B*usiness *C*ontinuity *C*ertified *L*ead *A*uditor	www.bcm-institute.org/bcmi10/en/bccla	BCCLA certification is designed and developed to instill pertinent concepts and knowledge in BCM practitioners and Audit professionals which will enable them to certify organizational-wide Business Continuity Management System (BCMS)
19	CFE	*C*ertified *F*raud *E*xaminer	www.acfe.com	CFE provides an insight and expertise into fraud prevention, detection and deterrence. CFEs are trained to identify the warning signs and red flags that indicate evidence of fraud and fraud risk. he curriculum focuses upon four areas – Fraud prevention and deterrence, financial transactions, fraud investigation and legal elements of fraud.
20	CSFA	*C*yber *S*ecurity *F*orensics *A*nalyst	www.cybersecurityforensi-canalyst.com	CSFA professionals are capable of conducting a thorough forensics analysis using sound examination and

CSA Certificate of Cloud Security Knowledge (CCSK) is the first certification that has provided a consistent way of developing cloud security competency and has also provided both organizations and IT security professionals the confidence they need to adopt secure cloud solutions.

Aspirants would have to search for the availability of nearest local chapter of the respective certification body, in case of vendor-neutral certifications and in case of vendor-specific certifications, would have to search the nearest franchise of a private training institute, who can provide the guidance on these certifica- tions. Nowadays numerous private institutes offer such guidance through scheduled courses. Usually these certification examinations are based on Common Body of Knowledge (CBK) published by these certifica- tion bodies and the nature of these examinations is of Multiple Choice Questions (MCQs). Aspirants might have to enquire whether the certification examination would be a "paper-pencil" examination or would be "online (computer-based)" examination, which is conducted into prometric center. The private training institutes also called as "Accredited Training Center" have authorized prometric center. One has to book the date and time with these prometric centers to take up these certification examinations or else will have to plan for examinations in case it is "paper-pencil" examination, as it may be scheduled every quarter/every 6 months/every year.

5. Guide Path

One of the most frequently asked questions is, "Where and how should I start to be a cybersecurity expert?" and simple answer would be "For any profession one should follow 3D, that is, determination, dedication and devotion". However, still it does not provide any directives to aspirants and hence the objective of this section is to lay down a guide path that will provide a direction on which aspirants can think and get along. Any career has three steps to be an SME (subject matter expert) in the field.

1. Basic and fundamental Knowledge.
2. Advance knowledge and mastering skills.
3. Specialized skill set.

There could be a good debate on the guide path – which path and/or certifications, aspirants may have to follow/acquire to evolve as an SME in cybersecurity field. We have made an attempt to tie career paths discussed in Section 12.3 with certifications mentioned in Section 12.4, which could be used as a common guideline toward career in cybersecurity field and aspirants may plan their career depending upon their exist- ing competency level, educational background and career objectives.

1. **Assurance and Compliance Security Audit:** Most of the Assurance and Compliance Auditors have a bachelor's or master's degree either from Commerce stream or from Computing field. Vendor- specific certifications always help to understand the basics and fundamentals about various computer network operations and components. Vendor-neutral certifications such as "CISA (Certified Information Systems Auditor)" and "ISO Standard – Lead Auditor," provide an insight about "auditing methodology." Fundamental and advanced set of certifications provide a good head-start to sail into Information Systems Audit environment and subsequently the knowledge can be enriched by focusing upon specialized skill set and acquiring certifications such as BCCLA/CIPP (IT) (see Table 12.3).

Table 12.3 | Guide path: Assurance and compliance security audits

Facet	*Vendor-Specific Certifications*	*Vendor-Neutral Certifications*
Basic and fundamental knowledge	• Microsoft Certified Systems Administrator (MCSA) • Cisco Certified Network Associate (CCNA)	**SSCP/SCNP** • Systems Security Certified Practitioner (SSCP) • Security Certified Network Professional (SCNP)
Advance knowledge and mastering skills	**MCSE/CCNP** • Microsoft Certified Systems Engineer (MCSE) • Cisco Certified Network Professional (CCNP)	**CISA, ISO 27001 LA/ISO 20000 LA** • Certified Information Systems Auditor (CISA) • Lead Auditor (LA)
Specialized skill set		**CSSLP/BS 25999 LA/BCCLA/CIPP(IT)** • Certified Secure Software Lifecycle Professional (CSSLP) • Lead Auditor (LA) • Business Continuity Certified Lead Auditor (BCCLA) • Certified Information Privacy Professional/ Information Technology (CIIP/IT)

2. **Network Security:** Beginners may start with fundamental knowledge of networking by acquiring the combination of vendor-neutral and vendor-specific certifications. Mastering in networking field is gained through experience and subsequently may target advance level of certifications as described

Table 12.4 | Guide path: Network security

Facet	*Vendor-Specific Certifications*	*Vendor-Neutral Certifications*
Basic and fundamental knowledge	**MCSA/CCNA/RHCSA** • Microsoft Certified Systems Administrator (MCSA) • Cisco Certified Network Associate (CCNA) • Red Hat Certified System Administrator (RHCSA)	**SSCP/SCNP** • Systems Security Certified Practitioner (SSCP) • Security Certified Network Professional (SCNP)
Advance knowledge and mastering skills	**MCSE/CCNP/RHCSS** • Microsoft Certified Systems Engineer (MCSE) • Cisco Certified Network Professional (CCNP) • Red Hat Certified Security Specialist (RHCSS)	**CISSP/CISM/SSNP** • Certified Information Systems Security Professional (CISSP) • Certified Information Security Manager (CISM) • Security Certified Network Specialist (SCNS)

(*Continued*)

Table 12.4 | (*Continued*)

Facet	*Vendor-Specific Certifications*	*Vendor-Neutral Certifications*
Specialized skill set	**CCSA/CCSE** • Check Point Certified Security Administrator (CCSA) • Check Point Certified Security Expert (CCSE)	**CEH/CWNP/CWSP/LPT** • Certified Ethical Hacking (CEH) • Certified Wireless Network Professional (CWNP) • Certified Wireless Security Professional (CWSP) • Licensed Penetration Tester (LPT)

in Table 12.4. VAPT and ethical hacking are the specialized fields and aspirants are always fascinated about it. However, aspirants should note that, strong knowledge and experience about computer networks is very essential. To know more about VAPT, see Appendix E in CD.

3. **Cybercrime investigation and litigation:** Bachelor's or Master's degree from IT stream with gradu- ation/post-graduation in Law (e.g., LLB – *Legum Baccalaureus* in Latin language, i.e., Bachelor's Degree in Law and LLM – *Legum Magister* in Latin language, i.e., Masters Degree in Law) with specialization in cyberlaw along with IT security certifications could be the best option to start this field. Being a cybercrime lawyer, one may need to investigate online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, cyber sabotage, Phishing attacks, E-Mail hijacking, denial of service, hacking divorce cases, murder cases, organized crime, terrorist operations, defamation, pornography, extortion, smuggling, etc. To have an overview about all these attacks and types of frauds, one may plan and acquire certifications as displayed in Table 12.5 along with an understanding of IT Act (see Chapter 6).
4. **Computer forensics:** Most of the forensics professionals have a bachelor's or master's degree in forensics which is offered by most of the universities in India. Apart from universities affiliated courses, global certifications[16] listed below can add more value in the knowledge base. (Reader may visit the URL mentioned in Ref. #16, References to get an overview about each certification listed below.)

Table 12.5 | Guide path: Cybercrime investigation and litigation

Fact	*Vendor-Specific Certifications*	*Vendor-Neutral Certifications*
Basic and fundamental knowledge	**MCSA/CCNA** Microsoft Certified Systems Administrator (MCSA) • Cisco Certified Network Associate (CCNA)	**SSCP/SCNP** • Systems Security Certified Practitioner (SSCP) • Security Certified Network Professional (SCNP)
Advance knowledge and mastering skills		Certified Information Systems Auditor **(CISA)**
Specialized skill set		Certified Fraud Examiner **(CFE)**

- *Vendor-neutral forensics certifications*
  (a) CCE: Certified Computer Examiner.
  (b) CCFE: Certified Computer Forensics Examiner.
  (c) CDFE: Certified Digital Forensics Examiner.
  (d) CEDS: Certified E-Discovery Specialist.
  (e) CHFI: Computer Hacking Forensics Investigator.
  (f) CSFA: Cyber Security Forensics Analyst.
  (g) GCFA: GIAC Certified Forensics Analyst.
  (h) GCFE: GIAC Certified Forensics Examiner.
  (i) CFCE: IACIS Certified Forensics Computer Examiner.
- *Vendor-specific forensics certifications*
  (a) ACE: AccessData Certified Examiner.
  (b) CFIP: Certified Forensics Investigation Practitioner.
  (c) CMFS: Certified Mac Forensics Specialist.
  (d) CMI: Certified Malware Investigator.
  (e) EnCE: EnCase Certified Examiner.
  (f) EnCEP: EnCase Certified E-Discovery Practitioner.

Aspirants those who have not completed university programs in forensics can also plan to complete the certifications as displayed in Table 12.6 to get into this field. Aspirants should note that one has to build

Table 12.6 | Guide path: Computer forensics

Facet	*Vendor-Specific Certifications*	*Vendor-Neutral Certifications*
Basic and fundamental knowledge	**MCSE/CCNA** • Microsoft Certified Systems Administrator (MCSA) • Cisco Certified Network Associate (CCNA)	**Security+, SCNS/SCNP, CCE** • Systems Security Certified Practitioner (SSCP) • Security Certified Network Professional (SCNP) • Certified Computer Examiner (CCE)
Advance knowledge and mastering skills	**ACE/CFIP/CMI** • AccessData Certified Examiner (ACE) • Certified Forensics Investigation Practitioner (CFIP) • Certified Malware Investigator (CMI)	**CCFE/CDFE/CHFI/GCFE** • Certified Computer Forensics Examiner (CCFE) • Certified Digital Forensics Examiner (CDFE) • Computer Hacking Forensics Investigator (CHFI) • GIAC Certified Forensics Examiner (GCFE)
Specialized skill set	**CFIP/CMFS/EnCE/EnCEP** • Certified Forensics Investigation Practitioner (CFIP) • Certified Mac Forensics Specialist (CMFS) • EnCase Certified Examiner (EnCE) • EnCase Certified E-Discovery Practitioner (EnCEP)	**CSFA/GCFA/GCFE** • Cyber Security Forensics Analyst (CSFA) • GIAC Certified Forensics Analyst (GCFA)

Aspirants should note that vendor-specific certifications are required and necessary to excel in "network security" and "computer forensics" field. Fundamental and advanced level of vendor-specific certifications always provide good understanding about the technology and gaining knowledge is resourceful while conducting Information Security Audit assignments effectively, in "compliance and assurance" field as well as conducting investigations in "cybercrime litigations" field.

in-depth knowledge base about IT as well as should master into one of the forensics tools, to be an expert into this field.
To become a skilled and effective security professional expert, followseven E's[17]:

1. **Exploration:** Research and read extensively about cybersecurity.
2. **Education:** Global certifications are becoming necessary along with college degree.
3. **Experimentation:** Experimentation with systems, applications, utilities and tools is very essential to gain hands on experience of how they work and what they do.
4. **Experience:** Working on real cases by utilizing each opportunity to have the opinions tested by experienced cross-examiners.
5. **Exchange:** Sharing the knowledge by networking with other practitioners helps to maintain the knowledge-base among all the practitioners.
6. **Equipment:** Investing efforts and time at least into one tool (i.e., security utility) has been indispens- able for Information Security Professional to know how they work and where they can be used.
7. **Earning:** Satisfying the requirements and needs of the client are the ultimate earning reason which will generate good business in near future.

Aspirants/readers may visit the URL http://www.intelligentedu.com/itcerts.html to explore the cer- tifications based on various facets such as domain, level to be mastered, vendor-specific, etc.

SUMMARY

As cybersecurity threats continues to grow and the importance toward awareness of cybersecurity to corporations, government and private individuals continues to increase. Privacy is an important con- cern across the globe and the protection of data has become a key issue. With concerns over identity theft and other cybercrimes, intense public focus remains intense on the cybersecurity field.

The ongoing struggle against cyberterrorism and the quest for emergency preparedness as well as disaster preparedness puts a continued urgency into the cybersecurity field. Organizations are also facing new challenges about how to handle the data in the wake of corporate scandals. In short, cybersecurity field is growing and those with the proper training and experience will find plenty of opportunities.

Aspirants should focus on any of their interest of domains and should acquire relevant certification(s) to fetch the right opportunity. However, the focus should be more on building knowledge base rather than only scoring marks to succeed to sail through certification examination. The practitioners who are already in the