

Career Guide

Decoding the Information
Security Profession



Published by

Sponsored by

Microsoft

(ISC)²
PRESS

(ISC)² SECURITY TRANSCENDS TECHNOLOGY[®]



The Year of the Information Security Professional

This publication, the first Career Guide to the Information Security Profession, is part of the Year of the Information Security Professional program, an initiative created by the International Information Systems Security Certification Consortium [(ISC)²] in conjunction with dozens of other major organizations worldwide, to:

- Spotlight information security professionals and attract high-quality candidates to the profession
- Highlight the increasingly significant role information security professionals play in the global economy
- Encourage organizations to meet the challenges of information security by increasing investment in their information security people

The Year of the Information Security Professional initiative was motivated by the conclusions of the first comprehensive study of the global information security workforce, commissioned by (ISC)² and conducted by IDC, a global industry analyst firm. The study reveals the increasingly vital role and growing stature of information security professionals across a multitude of industries. It showed that the need for new professionals would nearly double worldwide by 2008 to 2.1 million people.

For more information about the Year of the Information Security Professional, visit www.isc2.org/yisp.



SECURITY TRANSCENDS TECHNOLOGY®

About (ISC)²

(ISC)² is the premier non-profit organization dedicated to certifying information security professionals around the world. Founded in 1989, (ISC)² has certified over 33,000 information security professionals in more than 100 countries. Based in Palm Harbor, Florida, USA with offices in Vienna, Virginia, USA, London, Hong Kong and Tokyo, (ISC)² issues the Certified Information Systems Security Professional (CISSP®) and Systems Security Certified Practitioner (SSCP®) credentials and related concentrations to those meeting necessary competency requirements. The CISSP, the *Gold Standard* in information security certifications, is the first information technology credential to meet the stringent requirements of ANSI under ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)² also offers educational products and services based upon (ISC)²'s CBK®, a compendium of industry best practices for information security professionals, and is responsible for the annual (ISC)² Global Information Security Workforce Study. For more information, visit www.isc2.org.

About Microsoft and its Security Efforts

Founded in 1975, Microsoft is the worldwide leader in software services and solutions that help people and businesses realize their full potential.

Microsoft is committed to working with the industry to build trust in computing and to building software and services that will help better protect customers and the industry. Microsoft's approach to security requires continued technology investment from the industry and customers, prescriptive guidance, industry leadership through partnership, policy and initiatives.

Security is a critical issue for customers, and Microsoft recognizes that they depend on qualified information security professionals to help maintain the security of their networks. Microsoft applauds (ISC)² for spearheading this guide that spotlights the information security professional career as well as the important efforts of current security professionals in their ongoing work to protect networks and, by extension, the industry at large.

Table of Contents

Information security description.....	6
Jobs, industries and organizations.....	8
Profession requirements.....	12
Certifications	14
Typical salaries.....	17
Career outlook.....	18
Schools, education facilities, certification organizations	22
Additional resources and associations	33

Introduction

Welcome to the rapidly growing field of information security! Twenty-five years ago, the information security profession was new and obscure. Many of us fell into information security jobs when our employers realized their business was at risk and they needed to protect their networks and assets. The catch is they weren't sure how – in terms of technology or people – to make that happen.

We gathered in small groups and at conferences and tried to figure out how to tackle this job that no one had done before us. We had sketchy job descriptions and IT-oriented titles that didn't reflect business requirements, our company's environment or the actual jobs we were doing. There were also few standards and guidelines.

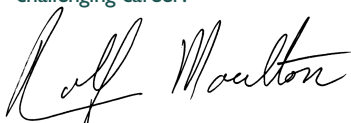
Today, things are different. Hackers have evolved from a small group of highly specialized guys writing malicious code to widespread professional thieves actively stealing identities and assets, destroying individuals' lives and ruining businesses.

As a result, society has come to rely on information security professionals. Businesses recognize that information and information security are critical to delivering their products and services, and they protect us all personally and nearly everything we use in our daily lives, from phones to electricity to home computers.

Information security has become a real profession driven by common standards and supported by education opportunities and certifications like the CISSP® that empower professionals throughout their careers.

Being an information security professional is a tough job. You need technical skills and the ability to understand how to protect information and information services in a business context. But it can also be an immensely rewarding career with thrilling prospects.

I hope this guide helps you understand the opportunities before you and prepare yourself for this exciting and challenging career!



– Rolf Moulton, CISSP-ISSMP, President & CEO, (ISC)²

What is Information Security?



Definition of Information Systems, according to Barron's Dictionary of Business Terms, Third Edition:

Information Systems is any written, electronic or graphical method of communicating information. The basis of an information system is the sharing and processing of information and ideas. Computers and telecommunication technologies have become essential information system components. The scope of information systems includes people, processes, infrastructures, architecture, and technical implementations.

Information Security, on the other hand, is assuring the correctness, reliability, availability, safety and security for all aspects of information and information systems.

Information Security is crucial for the economic well-being of commercial enterprises and national security, as well as for the integrity of the global economy. Major businesses and government departments using the Internet are deploying more and more complex inter-networked information systems. It is the job of information security professionals to ensure that these networks and computer systems are properly and adequately secure by protecting information assets, such as customer data, financial information and critical infrastructures.

“Quotes”

Job Challenges

“One challenge I face is explaining to top-level executives why security needs to be in place, the aftermath if the security is breached, and how to lock down the right control to make sure that the security risk is mitigated. You could lock the front door, only to find out that the garage door is left wide open.”

– **Troy J. Leach, CISSP, CSA**, Technology Risk Management Consultant with American Express

“Being responsible for information security at an institution of higher education, I was asked to handle many challenging situations, probably the most significant of which was the illegal use and distribution of copyrighted products (software, music, film clips, etc.). I worked with the Legal Department and the system administrators to develop a process for responding to complaints that not only reduced the risk to the institution for copyright infringement, but also maintained the open environment of an educational institution. Communication was key to this process – notifying the complaining organization that the request had been received, contacting the people who had the illegal materials on their machines, removing the offending materials or shutting them down from the network, and responding back to the complaining organization to verify that the problem had been resolved.”

– **Anne Oribello, CISSP, CISM**, Senior Information Security Analyst

What types of jobs are available? In what types of industries and organizations?

Areas of expertise within information security:

- Access control systems and methodology (how people enter and leave the system)
- Applications and systems development security (creating new computer programs to protect an organization)
- Auditing and monitoring (collecting information for identification and response to security breaches)
- Business continuity planning (BCP) and disaster recovery planning (DRP) (uninterrupted access to critical data systems)
- Cryptography (the coding and decoding of data and messages)
- Data communications (what is necessary to operate communications networks)
- Law investigation and ethics (computer crime laws and regulations)
- Malicious code (counter measures and prevention techniques for dealing with viruses, worms and other forms of deviant code)
- Operations security (setting identity controls; auditing and monitor the mechanisms and tools)
- Physical security (giving physical access to systems solely to those who need it)
- Risk, response and recovery (processes to identify, measure and control loss)
- Security architecture and models (building the security infrastructure for a complex organization)
- Security management (identification of information assets and development of policies and procedures)
- Telecommunications and network security (ensure security through remote access management, network availability, firewall architectures, VPNs, Data Networking, LAN Devices, etc.)

Typical job titles: Typical industries:

- | | |
|--|---|
| ■ Security auditor | ■ Professional services (real estate, legal, engineering) |
| ■ Security specialist | ■ Government (national, state, and local) |
| ■ Security consultant | ■ Telecommunications |
| ■ Security administrator | ■ Banking and other financial-related industries |
| ■ Security analyst/engineer | ■ Manufacturing |
| ■ Director/manager of security | ■ Healthcare |
| ■ Chief security officer (CSO)/chief information security officer (CISO) | ■ Education |
| | ■ Insurance |

“Quotes”

My Responsibilities

“I assess the risk and regulatory compliance of technology solutions within an enterprise environment and review current security policies and implementation to assure that controls operate as intended to mitigate internal and external threats. My work ranges from penetration testing of network infrastructure to assurance of confidentiality of electronic Personal History Interviews (ePHI) for Health Insurance Portability and Accountability (HIPAA).”

– **Troy J. Leach, CISSP, CSA**, Technology Risk Management Consultant with American Express



Typical organizations that hire information security professionals:

Although the majority of the organizations that hire information security professionals are in professional services, government, telecommunications, and banking, organizations of all kind and sizes, including a growing number of smaller businesses, need and are hiring information security staff.

“Quotes”

My Responsibilities

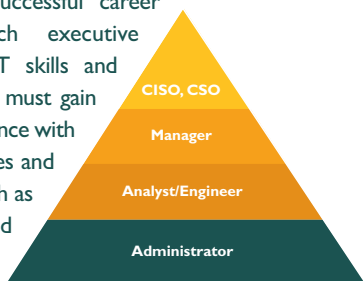
“As the United States Postal Service IT governance executive since October 2004, I am responsible for identifying, publicizing, monitoring and enforcing the organizational structures, policies and processes required to manage and control the use of information technology to create value, manage risk, and achieve the Postal Service’s business goals. The initial focus areas are the IT services metrics and value, information systems methodology (life cycle management), project planning and management, and standards compliance for the distributed infrastructure, including security.”

– **James. L. Golden, CISSP, CISM**, IT Governance Executive with the United States Postal Service

Typical job path:

- 2+ Years Experience – Information security administrator, eligible for SCCP certification
- 5+ Years Experience – Information security analyst/engineer, eligible for CISSP certification
- 7+ Years Experience – Information security manager
- 9+ Years Experience – Director of IT or information security, chief security officer (CSO) or chief information security officer (CISO)

If you wish to have successful career progression and reach executive status, in addition to IT skills and technical knowledge, you must gain knowledge of and experience with management best practices and business-related skills, such as communications skills and an understanding of policy, processes and personnel.





“Quotes” Most Rewarding

“I have a direct affect on changing security practices within an organization and making sure that it is prepared for whatever is going to come its way. That by itself, knowing that the overall goal of security is to be able to maintain a business’s status quo, is satisfying. A security breach affects much more than the actual assets that are compromised. A lot of families are affected when security breaches occur, especially within smaller companies. If you are in a smaller company of three to five hundred employees and a major security breach occurs, there is a good possibility that it could shut down the entire company. I think of not only of the lives of the employees but also of those of their husbands, wives and children.”

– **Troy J. Leach, CISSP, CSA**, Technology Risk Management Consultant with American Express

What's required to become an information security professional?

Education Options/Requirements

- Associate Degree for systems administrators
- B.A. in information technology or related field for analyst, engineer or manager
- B.S. in computer science or equivalent for analyst, engineer or manager
- M.S. or M.A. for director
- Ph.D. for professor, researcher, advanced developer

Technical Skills

- Knowledge of network systems and security protocols
- Knowledge of security software programs and implementation
- Knowledge of best practices in developing security procedures and infrastructure

General Skills and Aptitudes

- Excellent oral, written and presentation skills
- Solid leadership qualities
- Strong conceptual and analytical skills
- Ability to operate as an effective member of a team
- Ability to manage multiple diverse tasks simultaneously
- Strong project management skills (ability to manage the overall project while understanding subcomponents and how they relate to the total project)
- Demonstrate interpersonal and conflict management skills
- Ability to effectively relate security-related concepts to a broad range of technical and non-technical staff

“Quotes”

Skills/Aptitudes

“You need very strong analytical skills to work in information security. Security is all about problem-solving. You need to find out how the system can be broken, then after you break it, what to do to protect it and buffer it so it doesn’t happen again.”

– **Troy J. Leach, CISSP, CSA**, Technology Risk Management Consultant with American Express

“Quotes”

My Responsibilities

“As Director of Security Engineering Strategy for Microsoft’s Security Business and Technology Unit, my primary responsibility is for the Security Development Lifecycle, or SDL, Microsoft’s ongoing program to modify its software development processes to better accommodate security best practices and achieve measurably improved security. I lead a small team that does process development, training, and works with the internal stakeholder groups to identify ways in which we can build more secure software. In addition to my core role, I also lead a small team of Microsoft program managers (CISSPs) that work directly to address issues facing CISO’s and to gather input from some of Microsoft’s largest customers. This is a pretty different role from my engineering responsibilities, but because of my background as a CISO, CISSP and consultant, it’s something I enjoy and continue to do.

In my work for Microsoft, I get the opportunity to make security better for hundreds of millions of customers. I can’t imagine a more rewarding way to spend my working hours.”

– **Steven B. Lipner, CISSP**, Director of Security Engineering Strategy for Microsoft’s Security Business and Technology Unit

Certifications

Technology solutions alone cannot protect an organization's critical information assets. People are the key to a secure organization, and employers demand qualified information security staff to provide the highest standard of security for their customers, employees, stakeholders and partners. There are two categories of information security certifications: vendor-neutral and vendor-specific. A vendor-neutral certification, such as Certified Information Systems Security Professional (CISSP) or Certified Information Systems Auditor (CISA), encompasses a broad scope of knowledge and is not tied to any specific technology vendor or product. Vendor-specific certifications, such as Cisco Certified Security Professional (CCSP) or Microsoft Certified Systems Engineer: Security (MCSE), are offered by technology vendors covering knowledge and content about their products, solutions, and best practices. Both kinds of certifications play an extremely important role in the market, fulfilling specific knowledge and learning requirements of information security professionals, and demonstrating predetermined acceptable levels of competency and experience. (ISC)², the only non-profit body charged with maintaining, administering and certifying information security professionals via the compendium of industry best practices, the (ISC)² CBK, is the premier resource for information security professionals worldwide.

Benefits of Certification to the Professional:

- Demonstrates a working knowledge of information security
- Confirms the person's commitment to the profession
- Offers a career differentiator, enhanced credibility and marketability
- Provides access to valuable resources, such as peer networking and idea exchange

Benefits of Certification to the Organization:

- Establishes a standard of best practices for the organization
- Provides organization with staff that have demonstrated a broad knowledge in information security and professional judgement
- Provides access to a network of global industry and subject matter/domain experts
- Provides comfort to employer as to the individual's competency/knowledge of information security



(ISC)² Certifications

Associate of (ISC)² – Recognition for students or those at the beginning of their careers who have acquired knowledge of key information security concepts but do not yet have the work experience required for full accreditation. Gives them access to a vast network of professionals and various security-related resources.

Systems Security Certified Practitioner (SSCP) – This credential offers information security tacticians the opportunity to demonstrate their level of competence with the seven domains of the compendium of best practices for information security, the (ISC)² SSCP CBK.

The SSCP credential is ideal for those working toward or who have already attained positions as Senior Network Security Engineers, Senior Security Systems Analysts or Senior Security Administrators.

Certified Information Systems Security Professional (CISSP) – As the first and only ANSI-accredited information security credential under ISO/IEC Standard 17024, the CISSP certification provides information security professionals with not only an objective measure of competence but a globally recognized standard of achievement. The CISSP credential demonstrates competence in the 10 domains of the (ISC)² CISSP CBK, a compendium of industry best practices.

The CISSP credential is ideal for mid- and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.

Jim Wade



“Quotes” **Education**

“At the time I began my career in information security, there were few, if any, formal organizations (private or public) or educational institutions that were addressing information security except the U.S. Army. Therefore, I received almost all of my information security education while serving in the U.S. Army. Today, there are many sources of education in information security, beginning with undergraduate studies and progressing all the way to the doctoral level. Information security has progressed from being a specialty to a life-long profession.”

– **James R. Wade**, CISSP-ISSAP, ISSMP, CHS-III,
(ISC)² Past President & Director, Former
Chief Security Officer for the
U.S. Federal Reserve

(ISC)² certification services and programs include:

- Ongoing education
- Concentrations for proven subject matter expertise
- Peer networking/online discussion forums
- Constituent briefings/receptions
- Job postings
- Industry communications
- Speaking and volunteer opportunities
- Advocacy for your career and the information security profession

IDC surveyed information security professionals worldwide who are actively involved in making hiring decisions about the importance of security certifications, and 93% of them believe security certifications are either somewhat or very important when making hiring decisions.

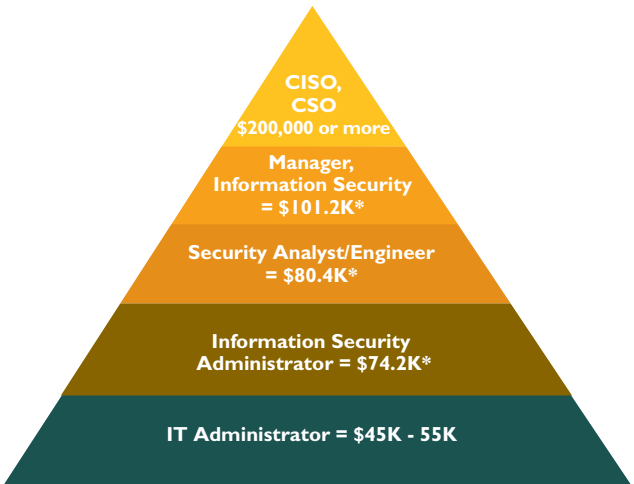
“Quotes”

Salaries

“Salaries were discussed at my high school reunion, and my salary was head and shoulders above most of the people my age.”

– **Jared R. Greene, CISSP-ISSAP, ISSMP, CCNA, CCDP**, Sr. Systems Engineer,
Security Assessment Team

What are Salaries?



Average Base Salary (U.S. National)

* Source: Foote Partners (www.footepartners.com), “IT Insider IT Professional Salary Survey: 1st Quarter, 2005”. Survey of 48,000 IT professionals.

What is the career outlook?

According to the 2004 (ISC)² Global Information Security Workforce Study, the outlook is optimistic. IDC estimates the number of information security professionals worldwide in 2004 to be 1.3 million, a 14.5% increase over 2003. The number of professionals is expected to increase to 2.1 million by 2008 at a compounded annual growth rate (CAGR) of 13.7 % from 2003.

Also according to the study, over 97% of respondents had moderate to very high expectations for career growth. Security professionals are experiencing growth in job prospects, career advancement, higher base salaries and salary premiums at faster rates than other areas of information technology.

Jared
Greene

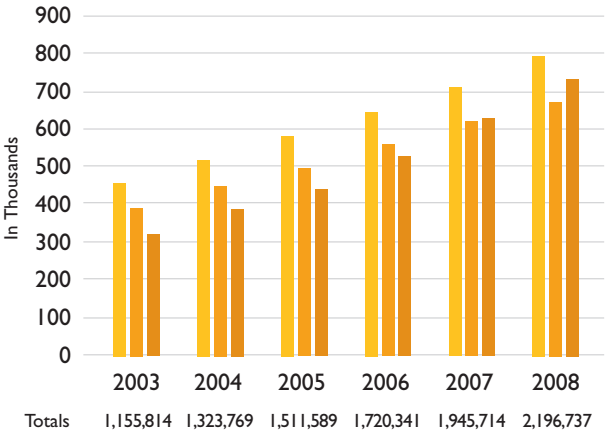


“Quotes” How I Started

“I perform vulnerability risk assessments in the banking and financial industry. I got started when I was sent by my employer to cover for someone doing security assessments for the company. I was able to hack a bank wide open in 28 minutes. From there, the company decided that they needed to send me to get CISSP education and obtain the certification through (ISC)².”

– **Jared R. Greene, CISSP-ISSAP, ISSMP, CCNA, CCDP,**
Sr. Systems Engineer, Security Assessment Team

Worldwide Information Security Professionals by Region, 2003-2008



	2003-2004 Growth (%)	2003-2008 CAGR (%)
Americas	13.1	12.0
EMEA	12.7	11.4
Asia/Pacific	18.9	18.3
Total	14.5	13.7

EMEA = Europe, Middle East, Africa

“Quotes” The Future

“Given the continued trend toward connected businesses and pressure for faster decisions and response, I believe that information security will continue to be both a very exciting profession and one of growing importance. I believe information security professionals will need to grow both by being more connected to business and strategy and by being better able to evaluate and/or recommend technical tradeoffs.”

– **Steven B. Lipner, CISSP**, Director of Security Engineering Strategy for Microsoft’s Security Business and Technology Unit

**Anne
Oribello**



“Quotes” **The Future**

“I expect to see more legislation and regulations surrounding the management of data, which will continue to push organizations to improve their security. Companies will be required to have their security more in line with generally accepted standards and these standards, will continue to evolve as new threats are identified and new tools are available.”

– **Anne Oribello, CISSP, CISM**, Senior Information Security Analyst

“Quotes” **Words of Wisdom**

“The information security profession is rapidly becoming both a management and a technical profession. Earlier, information security professionals were very much considered technicians. There is room and demand for both, and rarely do you find a person with strong skills in both areas. Professionalization is becoming more and more critical. A person may generally be good in one or the other skills and have to work very hard and gain skills in both to reach the top.”

– **James. L. Golden, CISSP, CISM**, IT Governance Executive with the United States Postal Service

Words of Wisdom

“My advice to someone interested in starting in the profession is to get a good foundation in some of the fundamentals. A degree in IT or computer science and an M.B.A. are ideal, although you don’t have to do all this at one time. Read some books and Websites about information security. Plan to pass the CISSP exam as soon as your skills and experience allow you to. Finally – this may go without saying – remember that a lot of security is about trust, and that your personal integrity and reputation are super-important to your ability to function effectively in this or any other field.”

– **Steven B. Lipner, CISSP**, Director of Security Engineering Strategy for Microsoft’s Security Business and Technology Unit

“I recommend anyone wanting to get into information security to spend the grunt work years developing various platforms that will be used in assessing security. Like with most things, you can’t start to fix it unless you know how it works.”

– **Troy J. Leach, CISSP, CSA**, Technology Risk Management Consultant with American Express

“For high schoolers, my advice is to beat down the door of the network administrators at the county offices or somebody in network support and tell them that they have an interest and want to volunteer their time. After working in the network department for two to three years, then they could walk out the door of high school at age 18 and already have two years of network experience. That is powerful. I also recommend that they get a CompTIA Network Plus certification as a starter because it covers all the basics of networking and gives them an idea of what area of specialization to get into. From there, I recommend they pursue a CISSP for security or take the Cisco route for systems administration.”

– **Jared R. Greene, CISSP-ISSAP, ISSMP, CCNA, CCDP**, Sr. Systems Engineer, Security Assessment Team

Schools, Education Facilities and Certification Companies, Additional Resources and Associations

Multiple Locations

(ISC)² Institute
Vienna, VA
(888) 333-4458
e-mail institute@isc2.org
www.isc2.org

* Scholarships are available through (ISC)². Visit:
www.isc2.org or call (727) 785-0189 for more details.

Keller Graduate School of Management of DeVry University
MBA with Concentrations in Security Management or
Information Security; Graduate Cert. in Information Security
(404) 292-7900
www.keller.edu

Security University
Stamford, CT
(203) 357.7744
e-mail: info@SecurityUniversity.net
<http://www.securityuniversity.net/>

Locations by State

Alabama

Auburn University
Information Assurance Laboratory
Department of Computer Science
and Software Engineering
Auburn, AL
(334) 844-6360
www.eng.auburn.edu/users/hamilton/security/

California

Naval Postgraduate School
Center for Information Systems
Security Studies and Research
Monterey, CA
(831) 656-3758
<http://cisr.nps.navy.mil>

Stanford University
Computer Science Department
Stanford, CA
(650) 723-2273
www.cs.stanford.edu

California

University of California at Davis
Computer Security Laboratory
Department of Computer Science
Davis, CA
(530) 752-7004
<http://seclab.cs.ucdavis.edu/>

Vista Community College
AA in Computer and Information Systems Security
Berkeley, CA
(510) 981-2800
www.vistacollege.edu/default.htm

Colorado

Colorado Technical University
Masters in Management w/ Information
Systems Security Concentration
Colorado Springs, CO
(866) 591-1987

District of Columbia

George Washington University
School of Engineering and Applied
Science
Washington, DC
(800) 537-SEAS
www.seas.gwu.edu

National Defense University
Information Resources Management, College
Washington, DC
(202) 685-6300
www.ndu.edu/irmc

Florida

Florida State University
Department of Computer Science
Tallahassee, FL
(850) 644-4029
www.cs.fsu.edu/infosec/

Seminole Community College
AA in Computer and Information Systems Security
Sanford, FL
(407) 328-4722
www.scc-fl.com

Georgia

Albany State University
BS in Security Management
Albany, GA
(229) 430-4646
www.asurams.edu

Georgia Institute of Technology
College of Computing
Atlanta, GA
(404) 894-3152
www.cc.gatech.edu

Kennesaw State University
Center for Information Security
Education and Awareness
Kennesaw, GA
(770) 499-3568
<http://infosec.kennesaw.edu>

Idaho

Idaho State University
Informatics Research Institute and the National
Information Assurance Training and Education Center
BBA and MBA with Emphasis In Computer Security
and Information Assurance
(208) 282-3194
www.Security.isu.edu and www.niatec.info

University of Idaho
Center for Secure and Dependable Systems
Moscow, ID
(208) 885-4114
www.csds.uidaho.edu

Illinois

University of Illinois at Urbana-Champaign
Department of Computer Science
Urbana, IL
(217) 333-3426
www.cs.uiuc.edu

Indiana

Purdue University
The Center for Education and
Research in Information Assurance
and Security (CERIAS)
West Lafayette, ID
(765) 494-7841
www.cerias.purdue.edu

Iowa

Iowa State University
MS in Information Assurance
Ames, IA
(515) 294-4111
www.iastate.edu

Maryland

Capitol College
MS in Network Security
Laurel, MD
(301) 369-2800
www.capitol-college.edu

Johns Hopkins University
Information Security Institute
Baltimore, MD
(410) 516-4250
www.jhuisi.jhu.edu

Towson University
Center for Applied Information
Technology
Towson, MD
(410) 704-4909
www.towson.edu/CAIT/

University of Maryland
University College
Adelphi, MD
(800) 888-UMUC
www.umuc.edu

University of Maryland,
Baltimore County
Center for Information Security and
Assurance
Baltimore, MD
(410) 455-3500
www.cisa.umbc.edu

University of Maryland
MS in Computer Systems Management
University of Maryland, College Park
College Park, MD
(301) 405-6330
www.vprgs.umd.edu

Massachusetts

Boston University
Department of Computer Science,
Metropolitan College
Boston, MA
(617) 353-2566
www.bu.edu/met/departments/computer/

Northeastern University
College of Computer and Information Science
Boston, MA
(617) 373-2462
www.ccs.neu.edu

University of Massachusetts, Amherst
Department of Computer Science
Amherst, MA
(413) 545-2744
www.cs.umass.edu

University of Massachusetts Lowell
Certificate Program in Security Management
Lowell, MA
(978) 934-3931
www.uml.edu

Michigan

Eastern Michigan University
Graduate Certificate in Information Security
Master of Library Science with Information Security
Concentration
College of Technology
BTE Office
Ypsilanti, MI
(734) 487-4330
www.bte.emich.edu/infosec.html

University of Detroit, Mercy
Centre for Assurance Studies
Detroit, MI
(313) 993-3337
http://business.udmercy.edu/center_assurance.htm

Walsh College
Information Assurance Center
Troy, MI
(248) 823-1369
www.walshcollege.edu/pages/432.asp

Minnesota

Rasmussen College Eagan
AA in Computer and Information Systems Security
Eagan, MN
(800) 852-6367
www.rasmussen.edu

Mississippi

Center for Computer Security Research
Department of Computer Science
and Engineering
Mississippi State, MO
(662) 325-7450
www.cse.msstate.edu/

Nebraska

University of Nebraska at Omaha
Nebraska University Consortium on
Information Assurance, College of
Information Science and Technology
Omaha, NB
(402) 554-2380
<http://nucia.ist.unomaha.edu/>

New Jersey

New Jersey Institute of Technology
College of Computing Sciences
University Heights
Newark, NJ
(973) 596-3366
www.ccs.njit.edu

Stevens Institute of Technology
Department of Computer Science
Hoboken, NJ
(201) 216-5328
www.cs.stevens-tech.edu

New Mexico

New Mexico Tech
Department of Computer Science
Socorro, NM
(505) 835-5126
www.cs.nmt.edu/page_home.html

New York

Pace University
School of Computer Science and
Information Systems
White Plains, NY
(914) 422-4191
www.csis.pace.edu/csis/

Polytechnic University
Brooklyn, NY
(718) 260-3600
www.poly.edu

State University of New York, Buffalo
Center of Excellence in Information
Systems Assurance Research and
Education, Department of Computer
Science and Engineering
Buffalo, NY
(716) 645-3180 x300
www.cse.buffalo.edu/caeiae/

State University of New York, Stony Brook
Computer Science Department
Stony Brook, NY
(631) 632-8470
www.cs.sunysb.edu

Syracuse University
Center for Systems Assurance
Syracuse, NY
(315) 443-2938
www.csa.syr.edu

United States Military
Academy, West Point
Information Technology and
Operations Center
Department of Electrical Engineering
and Computer Science
West Point, NY
(845) 938-2200
www.itoc.usma.edu

North Carolina

North Carolina State University
Computer Science Department
Raleigh, NC
(919) 515-5764
<http://ecommerce.ncsu.edu/infosec/>

University of North Carolina, Charlotte
The Laboratory of Information
Integration, Security and Privacy
Department of Software and
Information Systems
Charlotte, NC
(704) 687-4770
www.sis.uncc.edu/LIISP

Ohio

Air Force Institute of Technology
Center for Information Security
Education and Research (CISER)
Wright-Patterson Air Force Base, OH
(937) 255-3636 x4602
www.afit.edu

Oklahoma

University of Tulsa Center for Information Security
Tulsa, OK
(800) 331-3050
www.cis.utulsa.edu

Oregon

Portland State University
Maseeh College of Engineering and
Computer Science
Portland, OR
(503) 725-4036
www.cs.pdx.edu

Pennsylvania

Drexel University
Department of Electrical and
Computer Engineering
Philadelphia, PA
(215) 895-2241
www.ece.drexel.edu

Pennsylvania

East Stroudsburg University
Computer Science Department
East Stroudsburg, PA
(570) 422-3666
www.esu.edu/cpsc

Indiana University of Pennsylvania
Center of Academic Excellence in
Information Assurance
John P. Murtha Institute for
Homeland Security
Indiana, PA
(724) 357-2524
www.iup.edu/infosecurity

Pennsylvania State University
Center for Information Assurance
School of Information Sciences and
Technology
University Park, PA
(814) 865-3529
<http://netl.ist.psu.edu/cica/>

University of Pennsylvania
Department of Computer and
Information Science
Philadelphia, PA
(215) 898-8560
www.cis.upenn.edu

University of Pittsburgh
Laboratory of Education and
Research on Security Assured
Information Systems (LERSAIS)
Pittsburgh, PA
(412) 624-9405
www.sis.pitt.edu/~lersais/

Carnegie Mellon University
MS in Information Systems Management
Pittsburgh, PA
(888) 634-9604
www.mism.cmu.edu

Pennsylvania

ICM School of Business and Medical Careers
AA in Computer and Information Systems Security
Pittsburgh, PA
(800) 441-5222
www.icmschool.com

West Chester University of Pennsylvania
Information Assurance Center
Department of Computer Science
West Chester, PA
(610) 436-1000
www.cs.wcupa.edu/ia

South Dakota

Dakota State University
Center for Information Assurance
Madison, SD
(888) DSU-9988
www.ia.dsu.edu

Texas

Texas A&M University
Center for Information Assurance and Security
College Station, TX
(979) 845-8585
<http://cias.tamu.edu/>

University of Dallas
Center for Information Assurance
Graduate School of Management
Irving, TX
(972) 721-5174
http://gsmweb.udallas.edu/info_assurance/

University of Dallas
Irvine, TX
(972) 721-5000
<http://www.udallas.edu/>

University of North Texas
Center of Information and Computer Security
Denton, TX
(940) 565-2000

Texas

University of Texas, Dallas
Cybersecurity and Emergency
Preparedness Institute
Erik Jonsson School of Engineering
and Computer Science
Richardson, TX
(972) 883-2563
www.utdallas.edu/research/dfepi/

University of Texas, San Antonio
College of Business
San Antonio, TX
(210) 458-4313
<http://business.utsa.edu>

Utah

Weber State University
Certificate Program for Chief
Information Security Officer
Ogden, UT
(801) 626-6839
www.weber.edu

Vermont

Norwich University
Northfield, VT
(802) 485-2001
(800) 468-6679
www.norwich.edu/biz/cs

Virginia

ECPI College of Technology
AA in Computer and Information Systems Security
Hampton, VA
(757) 838-9191
www.ecpi.edu

George Mason University
Center for Secure Information Systems
Fairfax, VA
(703) 993-1653
<http://isse.gmu.edu/~csis/>

James Madison University
Harrisonburg, VA
(540) 568-8772
www.infosec.jmu.edu

Virginia

University of Virginia
School of Engineering and Applied
Science
Charlottesville, VA
(434) 924-3072
www.seas.virginia.edu

Washington

University of Washington
Center for Information Assurance and Cybersecurity
Institute of Technology
Tacoma, WA
(253) 692-5860
<http://depts.washington.edu/uwciac/>

Additional Resources

(ISC)²'s Resource Guide for Today's Information
Security Professional – Americas Edition
www.isc2.org/resourceguide

Professional Associations

AFCEA International
www.afcea.org
(800) 336-4583

American Council for Technology (ACT) and Industry
Advisory Council
www.actgov.org
(703) 218-1955

ASIS International
www.asisonline.org
(703) 519-6200

Association for Computer Security Day
www.computersecurityday.org

Association for Computing Machinery (ACM)
www.acm.org
(800) 342-6626

Computer Security Institute
www.gocsi.com
(866) 271-8529

The Computing Technology Association (CompTIA)
www.comptia.org
(630) 678-8300

Cyber Security Industry Alliance (CSIA)
www.csialliance.org
(202) 204-0838

The Federation for Identity and Cross-Credentialing
Systems (FiXs)
www.fixs.org
(703) 730-3556

Government Electronics and Information Technology
www.geia.org
(703) 907-7566

Homeland Security Institute
www.homelandsecurity.org
(703) 416-3134

Information Assurance Professionals Association
(IAPA)
www.iapa-glc.org
(248) 396-6649

Information Systems Audit and Control Association
(ISACA)
www.isaca.org
(847) 253-1545

Information Systems Security Association (ISSA)
www.issa.org
(800) 370-ISSA

Information Technology Association of America
(ITAA)
www.itaa.org
(703) 522-5055

Institute of Electrical Electronics Engineers (IEEE)
www.ieee.org
(202) 785-0017

Institute of Electrical and Electronics Engineers
Computer Society
www.computer.org
(202) 371-0101

International Information Systems Forensics
Association (IIFSA)
www.infoforensics.org
(678) 835-5267

International Information Systems Security
Certification Consortium, Inc. (ISC)²
www.isc2.org
(727) 785-0189

International Security, Trust, and Privacy Alliance
(ISTPA)
www.istpa.org
(703) 478-7615

Latin American Security Association (ALAS)
www.alas-la.org
(305) 592-1119

Liberty Alliance Project
www.projectliberty.org
(732) 465-6475

NACHA, The Electronic Payments Association
www.nacha.org
(703) 561-1100

National Defense Industrial Association (NDIA)
www.ndia.org
(703) 522-1820

National Standard Registry Board (NSRB)
www.nsrp.us
(313) 537-0613

OASIS (Organization for the Advancement of
Structured Information Standards)
www.oasis-open.org
(978) 667-5115

SANS Institute
www.sans.org
(301) 654-7267

USENIX
www.usenix.org
(510) 528-8649

(ISC)²[®]
INSTITUTE

1964 Gallows Road, Suite 210
Vienna, Virginia 22182
United States of America
Ph: +1.866.462.4777 or
+1.703.891.6781
Fx: +1.703.356.7977

(ISC)²[®]
SERVICES

2494 Bayshore Boulevard, Suite 201
Dunedin, Florida 34697
United States of America
Ph: +1.888.333.4458 or
+1.727.738.8657
Fx: +1.727.738.8522



(ISC)²[®]

(ISC)² Headquarters
33920 US 19 North, Suite 205
Palm Harbor, Florida 34684
United States of America
Ph: +1.727.785.0189
Fx: +1.727.786.2989

(ISC)² EMEA
Winchester House
Old Marylebone Road
London, NW1 5RA
United Kingdom
Ph: +44 (0)207.170.4141
Fx: +44 (0)207.170.4139

(ISC)² Asia-Pacific
Level 30, Bank of China Tower
1 Garden Road
Central, Hong Kong
Ph: +852.8226.7798
Fx: +852.8226.7723

(ISC)² Japan
Yanagi Bldg., 4 FL 3-1-26 Roppongi
Minato-ku, Tokyo 106-0032
Japan
Ph: +813.3583.8460
Fx: +813.3583.8669

© Copyright 2005 (ISC)², Inc.

All rights reserved. All contents of this brochure constitute the property of (ISC)², Inc. All marks are the property of the International Information Systems Security Certification Consortium, Inc.