

This guide offers in-depth coverage of security certifications in the IT industry as well as resources for further study.

## IT Influencer Series

# Security Certification Resource Guide

Essential information on security certifications for IT professionals and managers.

## Contents

Introduction	3	EC-Council: Know Your Enemy	14
(ISC) <sup>2</sup> : Experience Counts	4	Blueprint for a Career in Security	15
SANS: A Practical Approach	6	Guide to Security Job Titles	19
Microsoft: Locking Windows	7	Q&A: Can Security Certifications Help Your Career?	22
CompTIA: Security for the Masses	8	Salary Data for IT Professionals	23
Cisco: Hardware Lockdown	9	About Those U.S. Government Security Clearances	24
Check Point: Enterprise Certified	10	15 Best Web Sites for Security	25
CWNP: Wireless Pro	10	5 Must-Read Security Newsletters	26
ISACA: Audit Secure	12	5 Web Picks for Security Certification	26
TruSecure: TISCA Experience	12	Security Bookshelf	28
Symantec: Sleeper Hit	13	Advertiser Index	30
SCP: Security Certified Pro	13		
SCSA: Seeking the Sun	14		



Knowledge.

# INTENSE SCHOOL

The IT & Security Training Experts

**Security. 04**

Microsoft - Cisco® - CISSP® - Professional Hacking - Computer Forensics - and more.

Choosing the right IT training school can spell the difference between failure and success. If you've been looking for a training and certification school that offers you the best return on your training investment, your search is over. Intense School has recently been voted the 2003 Windows & .Net Magazine Readers' Choice winner as **Best Boot Camps** and **Best Instructor-Led Training** in the category of Training and Certification!



# Introduction

**S**ecurity is one of the hottest areas in IT certification today. It can also be the most confusing.

As little as two years ago, IT professionals wanting to certify their security-related knowledge and expertise had only a handful of credentials to choose from, most of which were reserved for the most experienced professionals.

Since then, several vendors have added security-related titles and options, and those specializing in security are offering more credentials than ever. This boom has created a mix of titles that, while serving a wider cross-section of the IT community, also make understanding and evaluating security certifications an arduous endeavor.

We've created this guide to help IT professionals and managers sort out the many options available. On its pages you'll find profiles of almost every major security-related certification available today. For each, we explain the audience they're aimed for, the requirements for obtaining the titles, and what separates each from the other credentials.

But we also know that becoming an IT security professional takes more than just certification. That's why you'll also find advice on developing an IT security career, including frank words from security maven and author Roberta Bragg on what it takes to excel in this field, as well as



an honest perspective from an industry insider on exactly what certification can (and can't) do for your career. We also share the real way those all-too-elusive U.S. security clearances are obtained.

To help in the learning process, we've included our top picks for security Web sites and newsletters, as well as certification preparation resources.

Whether you're an IT professional considering a career in security or a manager who needs to guide your security staff's professional development, we hope the following information will offer you the comprehensive overview of security certification you've been searching for. Enjoy.

—The Editors

All content was written and/or developed by Keith Ward, senior editor, *Microsoft Certified Professional Magazine*; Becky Nagel, editor, *CertCities.com*; Michael Domingo, editor, *MCPmag.com* and Dian Schaffhauser, editorial director, *Microsoft Certified Professional Magazine*.

# Experience Counts

It takes more than just knowledge to earn (ISC)<sup>2</sup>'s CISSP and SSCP titles.

The International Information Systems Security Certification Consortium, (ISC)<sup>2</sup>, formed in 1989 to create an industry standard for information security best practices. Since that time, the organization has released several vendor-neutral certifications that combine testing candidates' knowledge of these practices along with experience, ethical and ongoing education requirements.

The organization's flagship title, the Certified Information Systems Security Professional (CISSP), focuses on 10 common bodies of knowledge (CBKs) based on the above-mentioned standards:

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

The resulting exam is a six-hour, 250-question affair, for which most candidates study months to prepare. Because of the broad depth of knowledge covered on the exam, most students prefer not to go it alone, joining study groups or attending instructor-led training courses.

However, simply passing the exam won't earn you the CISSP. (ISC)<sup>2</sup> cites its mission to create a "gold standard" certification as the reason it requires all candidates to have at least four years of "direct full-time security professional work experience" in one or more of the test domains listed above. A college

degree can substitute for one year. This experience must be documented by an independent third-party and submitted to the (ISC)<sup>2</sup> for audit, along with a signed document stating that the candidate will subscribe to the organization's code of ethics. Only then will the title of CISSP be granted. But that's not the end of it—all CISSPs must complete 120 units of continuing education per year to keep their title active.

If you don't quite have four years of direct work experience, you may want

to attempt the organization's Systems Security Certified Practitioner (SSCP) title. This three-hour, 125-question exam focuses on seven of the above domains and requires only one year of direct work experience. Like the CISSP, you must subscribe to the organization's code of ethics and earn continuing education units to maintain the title.

If you don't have enough experience to earn either title but you still want to take the above exams, you can become an Associate of (ISC)<sup>2</sup>. This new program from the organization allows candidates without the required experience to take the exams and then earn the certifications once they obtain the needed experience.

If you're already a CISSP and want to distinguish yourself further, the organization recently announced several "concentrations" that candidates can add on to their CISSP: CISSP Management and CISSP Architecture. There's also the Information System Security Engineering Professional (ISSEP), a concentration formed in conjunction with the United States National Security Agency that focuses on the information security needs of federal government employees.

Note that because the organization's exams are paper-based, candidates must sign up through (ISC)<sup>2</sup> and travel to an official testing location. Prices for the organization's exams currently range from \$350 to \$550, but will rise as much as \$100 beginning January 1, 2004.

More information on all of the above titles can be found on (ISC)<sup>2</sup>'s Web site at <http://www.isc2.org>.

— *Becky Nagel*

## (ISC)<sup>2</sup>

**Vendor:** The International Information Systems Security Certification Consortium (ISC)<sup>2</sup>

**Certifications:** CISSP, SSCP, related concentrations

**Certification Type/Focus:** Vendor-neutral titles focusing on best practices for information security professionals. Candidates must meet experience requirements and sign an ethics pledge.

**Exam Prices:** \$350 to \$550 (U.S.)

**Training Required?:** No

**Testing Centers:** Available only through vendor

**More information:**  
<http://www.isc2.org>



## STAY ON TOP OF THE LATEST SECURITY TRAINING...

...or your replacement will be happy to do it for you.

With 28 hands-on Security Training courses, Global Knowledge offers the industry's most comprehensive collection of Network Security courses delivered by real-world, expert instructors. Visit our web site now for more information: [www.globalknowledge.com](http://www.globalknowledge.com) Keyword: MCPSECURE or call 1-800-COURSES.



**GET A FREE T-SHIRT**  
When you take our 1-minute IT survey at  
[www.globalknowledge.com/securitytee](http://www.globalknowledge.com/securitytee)

# A Practical Approach

The SANS Institute's GIAC certifications combine testing with practical assignments.

Like (ISC)<sup>2</sup>, the SANS Institute's Global Information Assurance Certification (GIAC) takes a vendor-neutral approach. However, this organization's titles focus on the practical more than the theoretical, testing candidates' skills in a wide variety of areas through online or in-person testing as well as practical assignments.

Those interested in GIAC testing have a wide variety of titles to choose from:

- GIAC Security Essentials Certification (GSEC)
- GIAC Certified Firewall Analyst (GCFW)
- GIAC Certified Security Leadership (GSLC)
- GIAC Certified Intrusion Analyst (GCI A)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Windows Security Administrator (GCWN)
- GIAC Certified Unix Security Administrator (GCUX)
- GIAC Information Security Officer (GISO)
- GIAC Systems and Network Auditor (GSNA)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC IT Security Audit Essentials (GSAE)

Those who earn five of the above titles—GIAC Certified Firewall Analyst; GIAC Certified Intrusion Analyst; GIAC Certified Incident Handler; GIAC Certified Windows Security

Administrator; and GIAC Certified Unix Security Administrator—can earn the organization's highest certification, the GIAC Security Engineer. According to the organization, only two GIAC Security Engineers exist in the world today.

Before being allowed to take any

## SANS/GIAC

**Vendor:** The SANS Institute

**Certifications:** 12 Global Information Security Certification (GIAC) titles

**Certification Type/Focus:** Skills testing in a variety of security areas, such as firewalls, intrusion analysis and forensics. Candidates must pass an exam along with a practical assignment.

**Exam Prices:** \$250 (U.S.) with training, \$450 (U.S.) without

**Training Required?:** Yes, for select titles

**Testing Centers:** Available only through vendor

**More information:**  
<http://www.giac.org/>



GIAC exam, candidates must complete a “practical assignment”—an original research paper that demonstrates the candidate's knowledge of the material being tested. These assignments are reviewed and graded by the organization, and those who pass are then allowed to sit the related exam.

GIAC exams are delivered online and at SANS conferences. Because of the program's tie-in with SANS' educational offerings, some GIAC certifications require that candidates take the related SANS training course either at a conference or online. When taken along with a training course, the price of the exam is \$250. Exams cost \$450 when not accompanied by training.

All GIAC professionals must recertify every two years by passing a “refresher” exam. The price of renewal is \$120, which includes free access to SANS courseware online.

More information on GIAC's certification program can be found at: <http://www.giac.org>.

— *Becky Nagel*

# Locking Windows

Microsoft debuts MCSA: Security and MCSE: Security specializations.

If you're a Microsoft networking professional, you no longer need to seek titles from outside vendors to certify your Windows security expertise. That's because in June Microsoft announced new security specializations for its Microsoft Certified Systems Engineer (MCSE) and Microsoft Certified Systems Administrator (MCSA) titles.

"We put together these certification specializations to allow IT professionals a way to demonstrate a specific technical focus in the area of security within their job roles," David Lowe, product manager for security with Microsoft's Training and Certification group, said in an interview with *MCP Magazine* when the exams debuted. "The new specializations are directly analogous to the existing base credentials, but with a 'prescribed path' of specialization exams rather than electives." And that's the key to these specializations: To become an MCSE: Security or MCSA: Security, you don't have to take any more exams than would be required to earn the standard MCSA or MCSE. It's determined by *which* exams you take.

**For MCSA: Security 2000**, your elective exams must include:

- 70-214: Implementing and Administering Security in a Microsoft Windows 2000 Network
- 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition *OR* CompTIA's Security+

**For MCSE: Security 2000**, you must also take the elective:

- 70-220: Designing Security for a Microsoft Windows 2000 Network

**For MCSA: Security 2003**, you must take the following electives:

- 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network
- 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition *OR* CompTIA's Security+

**MCSE: Security 2003** requires the above plus:

- 70-298: Designing Security for a Microsoft Windows Server 2003 Network

If you've already earned your MCSA or MCSE, you can simply take any additional exams required to add the desired specialization.

Lowe explained that Microsoft created the specializations because, "We recognize that in IT job roles, like systems administrator and systems engineer, there are a number of individuals who have a very specific concentration on a particular area and, obviously, in an important area as security. So that's what these specializations will



## Microsoft

**Vendor:** Microsoft Corp.

**Certification:** MCSE: Security, MCSA: Security

**Certification Type/Focus:** Windows-specific specializations that show a candidate's security focus within the company's MCSA and MCSE titles.

**Exam Price:** \$125 (U.S.)

**Training Required?:** No

**Testing Centers:** Pearson Vue and Prometric

**More information:**

<http://www.microsoft.com/mcp>

allow individuals to demonstrate; they'll get to highlight their focus on platform-specific security and design skills."

Microsoft exams consist of standard, multiple-choice questions as well as more in-depth scenario-based questions. The company doesn't place training or experience requirements on its certifications, but hands-on experience with the products is highly recommended. Microsoft exams cost \$125 (U.S.) and are available worldwide through Pearson Vue and Prometric testing centers.

More information on these certifications can be found at <http://www.microsoft.com/mcp>.

— *Becky Nagel*

# Security for the Masses

CompTIA's Security+ aims to bring baseline security knowledge to all IT professionals.

The Computing Technology Industry Association is well known for its entry-level, vendor-neutral certifications such as A+, Network+ and Linux+. Therefore, it wasn't surprising when late last year the organization added Security+ to its roster.

Security+ is a one-exam certification covering a wide-range of top-level security knowledge. Topics covered on this exam include:

- Communication security
- Infrastructure security
- Cryptography
- Access control
- Authentication
- External attacks
- Operational security

The exam itself consists of 100 questions with a 90-minute time limit. The minimum passing score is 764, graded on a scale of 100 to 900. One focus of the exam is terminology, making sure candidates understand the many threats out there. Candidates are also tested on the best ways to tackle those threats. CompTIA recommends that all candidates have at least two years of general networking experience before taking the exam, but the experience level isn't required.

Many CompTIA corporate mem-

bers, such as Microsoft, IBM and Sun, helped create the title, participating in development meetings and deciding the certification's focus. As such, several certification programs either recommend Security+ as a prerequisite for their titles

## CompTIA

**Vendor:** Computing Technology Industry Association

**Certification:** Security+

**Certification Type/Focus:** Vendor-neutral security title that focuses on baseline security knowledge and skills.

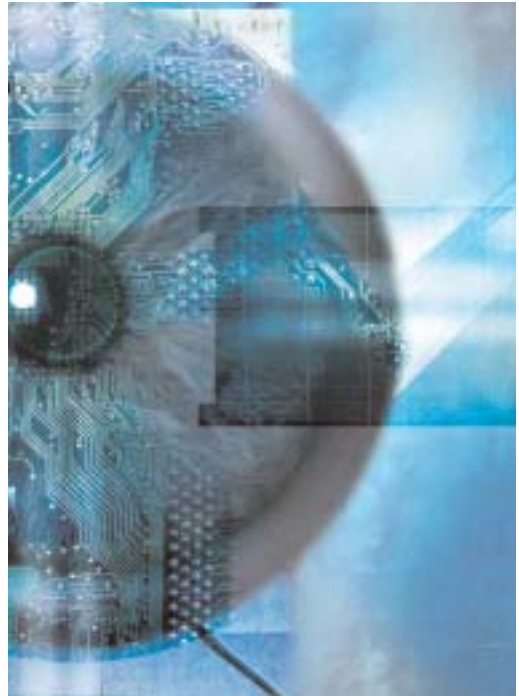
**Exam Price:** \$225 (U.S.)

**Training Required?:** No

**Testing Centers:** Pearson Vue and Prometric

**More information:**

<http://www.comptia.org/certification/security/default.asp>



or allow it as an alternative requirement. For example, Security+ counts as an elective toward MCSE 2000 as well as its new MCSA: Security and MCSE: Security specializations.

These tie-ins may be one reason this title has resonated so well with the IT community. Even before its official release, Security+ landed at #2 on CertCities.com's list of Top 10 IT Certifications for 2003. And according to Gene Salois, CompTIA's vice president of certification, Security+ is the organization's fastest-growing title ever.

The Security+ exam costs \$225 (U.S.), with a discount given to employees of corporate members. The certification is good for life, so there are no extra costs associated with renewing the title.

More information about Security+ can be found at <http://www.comptia.org/certification/security/default.asp>.

— *Becky Nagel*

# Hardware Lockdown

## Cisco offers a variety of ways to certify your expertise in securing its essential internetworking devices.

For the past 10 years Cisco Systems has been offering IT professionals working with its products ways to certify their expertise, but only recently has a suite of options emerged for those wishing to prove their security skills.

For the most experienced candidates, Cisco offers a security track for its expert-level Cisco Certified Internetwork Engineer (CCIE) title. The CCIE is known world-wide as one of the hardest certifications to obtain because candidates must pass an in-person, proctored troubleshooting lab exam.

Typical study methods won't get you a CCIE. As Cisco states on its Web site, "Training is not the CCIE program objective. Rather, the focus is on identifying those experts capable of understanding and navigating the subtleties, intricacies and potential pitfalls inherent to end-to-end networking." As such, the company recommends that all candidates have at least three to five years of hands-on experience working directly with the technology in a real-world environment.

CCIE exams are not only grueling, they're expensive: \$1,250 (U.S.) plus expenses to travel to one of five locations worldwide where lab exams are offered. To make sure that only those who have a chance of passing attempt the exam, all CCIE candidates must first pass a \$300, standard-format "qualification" exam, available through local Pearson Vue and Prometric testing centers. There are no other requirements or prerequisites to earn the title.

If you're not yet ready to tackle

CCIE Security, you may be interested in Cisco's newest security offering, the Cisco Certified Security Professional (CCSP).

The CCSP is a professional-level title, on the same level as its Cisco Certified Network Professional (CCNP) and Cisco Certified Design Professional (CCDP) certifications.

To become a CCSP, candidates must obtain a Cisco Certified Network Associate (CCNA) or Cisco Certified Internetwork Professional (CCIP) credential, then pass the following five exams:

- 642-501 SECUR: Securing Cisco IOS Networks
- 642-511 CSVPN: Cisco Secure VPN
- 642-521 CSPFA: Cisco Secure PIX Firewall Advanced
- 643-531 CSIDS (beta): Cisco Secure Intrusion Detection System
- 642-541 CSI: Cisco SAFE Implementation

As you can see from the above, this certification is so new that one of the required exams is still in beta format—it is expected to be released in its final version by the end of 2003.

These tests are standard-format exams featuring multiple-choice questions. Some also include simulation questions that require hands-on skills. All are available at Prometric and Pearson Vue testing centers worldwide. The beta is priced at \$50 and the live exams are \$125 (U.S.).

If you're not looking for a stand-alone title, you might want to augment

### Cisco

**Vendor:** Cisco Systems

**Certifications:** CCIE Security, CCSP, Qualified Specialist

**Certification Type/Focus:**

Product-specific titles for a variety of experience levels.

**Exam Prices:** \$125 to \$1,250 (lab exam) (U.S.)

**Training Required?:** No

**Testing Centers:** All but lab available through Pearson Vue and Prometric.

**More information:**

<http://www.cisco.com/en/US/learning/>

your existing CCNA certification with one of Cisco's security-related concentrations available through its Qualified Specialist program.

The company currently offers three security-related Qualified Specialist titles for the IT community at large:

- Cisco Firewall Specialist
- Cisco IDS Specialist
- Cisco VPN Specialist

As mentioned above, candidates must first obtain a CCNA. From there, each title requires passing two exams: 642-501 SECUR, plus one focused on the chosen specialty from the above list of CCSP exams. Because the exams are the same, candidates can apply their Qualified Specialist title toward future pursuit of the CCSP.

All Cisco certifications require recertification through passing update exams. Recertification for Cisco titles takes place every two to three years.

More information on all of Cisco certification offerings can be found at the following URL on Cisco's Web site: <http://www.cisco.com/en/US/learning/>.

— *Becky Nagel*

# Enterprise Certified

Check Point’s certifications test users’ skills with the company’s Firewall-1 NG product and more.

Mid-size and enterprise networks across the globe use Check Point Software Technologies’ Firewall-1 and VPN-1 products to keep their environments secure. If you are looking for a way to certify your skills on these products, Check Point offers several options.

Check Point separates its certifications into two tracks: Security and Management. Within the Security track, there are three titles, each of which requires one exam. The certifications are tiered, meaning that each higher level requires the previous certification. They are:

- Check Point Certified Security Administrator (CCSA), which focuses on Firewall-1.
- Check Point Certified Security Expert (CCSE), which adds VPN-1.
- CCSE Plus Enterprise Integration and Troubleshooting, which adds integration and troubleshooting for both products.

Also within this track is a new

title: Check Point Certified Security Principles Associate (CCSPA), “an entry-level certification that validates a student’s proficiency in security fundamentals, concepts and best practices”—much like CompTIA’s Security+ exam. The CCSPA isn’t required

## Check Point

**Vendor:** Check Point Software Technologies

**Certifications:** CCSPA, CCSA, CCSE, CCSE Plus, CCMSE, CCMSE Plus VSX

**Certification Type/Focus:** Product-specific titles focusing on Check Point security solutions for mid-size to enterprise networks.

**Exam Price:** \$125 (U.S.)

**Training Required?:** No

**Testing Centers:** Pearson Vue

**More information:** <http://www.checkpoint.com/services/education/certification/index.html>

to earn any other Check Point certification but is recommended for those new to security.

Check Point’s Management track offers two titles:

- Check Point Certified Managed Security Expert (CCMSE)
- CCMSE Plus VPX

Check Point describes the CCMSE as its premier-level title for those using the company’s Firewall-1, VPN-1 and Provider-1 products in a “Network Operating Center” environment. It requires passing three exams. The CCMSE Plus option allows CCMSEs add to their credential by showing their expertise with the company’s VSX security solution, as managed by Provider-1.

All of Check Point’s exams are standard-format multiple choice tests, available for \$150 (U.S.) through Pearson Vue testing centers worldwide. Check Point recommends that all candidates have six months to one year of hands-on experience with the products they want to certify on.

More information on Check Point’s certification program can be found at: <http://www.checkpoint.com/services/education/certification/index.html>.

— *Becky Nagel*

# Wireless Pro

Certify your wireless security expertise with Planet3’s CWSP.

There are plenty of security issues surrounding wireless networking. The Certified Wireless Networking Program (CWNP) from Planet3 Wireless is a certification option that allows wireless professionals to test their security knowledge and skills.

According to Planet3, CWNP’s Certified Wireless Security Professional (CWSP) title is vendor-neutral, focusing on 802.11 wireless technology rather than specific vendors’ products. As the second tier of the program’s four levels of certification, candidates must

first obtain the program’s Certified Wireless Networking Associate (CWSA) before pursuing the CWSP.

According to Planet3 Wireless, the CWSP exam focuses on three areas:

- Wireless LAN intrusion
- Wireless LAN security policy
- Wireless LAN security solutions

The exam itself is a standard-format, multiple-choice test with 60 questions. It’s available through Prometric testing centers worldwide for \$175, although candidates must purchase the exam voucher directly from Planet3.

## CWNP

**Vendor:** Planet3 Wireless

**Certification:** CWSP

**Certification Type/Focus:** Vendor-neutral wireless security title.

**Exam Price:** \$175 (U.S.)

**Training Required?:** No

**Testing Center:** Prometric

**More information:** <http://www.cwne.com>

For more information on this certification, visit <http://www.cwne.com>.

— *Becky Nagel*

MCP MAGAZINE'S  
**TECH MENTOR**

Network  
and certification  
training for  
Windows®  
professionals.

# 2004 EVENTS

**NEW ORLEANS, LA**  
**APRIL 4 – 8**

**SAN JOSE, CA**  
**SEPTEMBER 28 – OCTOBER 1**

Join network managers and administrators for a new lineup of technical training sessions by networking, messaging and security experts. Take control. Get solutions, not theories, to your everyday networking problems.

Registration opens mid-November.



presented by:

**MICROSOFT**  
Certified Professional Magazine

[TechMentorEvents.com](http://TechMentorEvents.com)

**101**communications  
Enabling Technology Professionals to Succeed

## Audit Secure

The Independent Systems Audit and Control Association offers two certification options for IS auditing and security professionals.

The Information Systems Audit and Control Association (ISACA) has been offering its flagship Certified Information Systems Auditor (CISA) title since 1978. The title, which focuses on IS auditing and control as well as systems security, is now held by more than 30,000 professionals worldwide.

While this title does cover security, the organization recently decided to create another credential specifically for security professionals: the Certified Information Security Manager (CISM).

ISACA describes the CISM as its “next generation credential...specifically geared toward experienced information security managers and those who have information security management

responsibilities,” the Web site states. “It is business-oriented and focuses on information risk management while addressing management, design and technical security issues at a conceptual level.”

Both ISACA exams are offered once a year at a variety of locations worldwide. Candidates don't have to be members to take an exam, but they do need to agree to adhere to the organization's code of ethics. Both titles must be maintained through continuing education requirements.

The exams range in cost from \$325 to \$495 (U.S.) depending on membership status, registration date and method of registration. Through Dec. 31, 2004, candidates with eight

## ISACA

**Vendor:** Information Systems Audit and Control Association

**Certifications:** CISA, CISM

**Certification Type/Focus:** High-level certifications for information security and auditing professionals.

**Exam Price:** \$325 to \$495 (U.S.)

**Training Required?:** No

**Testing Centers:** Available through vendor only

**More information:**  
<http://www.isaca.org>

years of information security experience can grandfather directly into the CISM title without taking the exam. Various degrees and certifications count toward the grandfathering process.

More information on ISACA certifications can be found at <http://www.isaca.org>.

— *Becky Nagel*

## TISCA Experience

TruSecure moves into certifying individuals with its TISCA program.

You may know TruSecure as the company that owns the ISCA labs, which tests and certifies security products. What you might not know is that TruSecure also offers certifications for IT security professionals.

The company has turned its certification experience into the vendor-neutral TruSecure ICSA Certified Security Associate (TISCA) title. To achieve it, candidates must first prove they have least two years of hands-on experience or attend 48 hours of computer security training within a two-year period. Only then are candidates allowed to sit the TISCA exam, which features 70 questions covering TruSecure's 14 “essential” bodies of knowledge:

- Essential security practices vs. “best” security practices

- Risk management fundamentals
- TCP/IP networking basics
- Firewall fundamentals
- Incident response and recovery practices
- Administration maintenance procedures
- Design and configuration fundamentals
- Malicious code mechanisms
- Law, ethics, and policy issues
- Authentication techniques
- Cryptography basics
- Host- vs. network-based security
- PKI and digital certificates basics
- Operating system security fundamentals

Six areas of risk are also covered: electronic, malicious code, physical threat, human, privacy and downtime.

## TruSecure

**Vendor:** TruSecure

**Certification:** TISCA

**Certification Type/Focus:** Vendor-neutral title that also requires experience.

**Exam Price:** \$295 (U.S.)

**Training Required?:** No

**Testing Center:** Prometric (U.S. and Canada Only)

**More information:**  
<https://ticsa.trusecure.com/>

The \$295 (U.S.) exam is available through Prometric testing centers in the U.S. and Canada only. In addition to passing the exam, candidates are required to sign an ethics statement before the credential will be awarded. For more information on the TISCA, go to: <https://ticsa.trusecure.com/>.

— *Becky Nagel*

## Sleeper Hit

### Symantec jumps to second on CRN's 2003 list of most valuable certifications for resellers.

If you're looking for a security certification that resonates with solution providers, then a title from Symantec may be right for you.

Earlier this year, *Computer Reseller News* released the results of its third annual certification study, which rates the importance of various IT certifications for small and large solution providers. Symantec's Certified Security Practitioner (SCSP) jumped up the list to become the second most important certification for small solution providers (revenue under \$5 million) and the fastest-growing title in importance for large service providers (revenue more than \$5 million).

Even if you're not working for a solution provider or reseller, Symantec may still offer the certification you're

looking for. Symantec's program features four tiers of certification focusing on its products along with general security knowledge and strategies. Following is the listing of these titles and their description as provided by Symantec:

- **Symantec Product Specialist (SPS):** One exam on a single security product and its functionality in an overall security system.
- **Symantec Technology Architect (STA):** one-exam title focusing on vendor-neutral security knowledge of how to design, plan, deploy and manage effective security solutions.
- **Symantec Certified Security Engineer (SCSE):** covers a high-level understanding of a broad range of security solutions plus in-depth knowledge and skills within a specific security focus. These titles require passing two to three SPS and/or STA exams.
- **Symantec Certified Security Practitioner (SCSP):** senior security title. Achieved by earning all four of the SCSE certifications.

Within these tiers, there are four areas of product focus: Firewall &

### Symantec

**Vendor:** Symantec

**Certifications:** SPS, STA, SCSE, SCSP

**Certification Type/Focus:** Tiered program focusing four Symantec product areas.

**Exam Price:** \$125 to \$150 (U.S.)

**Training Required?:** No

**Testing Centers:** Prometric

**More information:**

<http://www.symantec.com/education/certification/>

VPN, Vulnerability Management, Intrusion Detection and Virus Protection & Content Filtering.

Symantec exams cost between \$125 and \$150 (U.S.) and are available at Prometric testing centers worldwide.

More information on Symantec certification can be found at <http://www.symantec.com/education/certification/>.

— *Becky Nagel*

## Security Certified Pro

### Ascendant Learning offers a vendor-neutral alternative.

Ascendant Learning bills its Security Certified Professional as an advanced, vendor-neutral IT security certification program. "The Security Certified Program is proud to offer intense certification exams," the program's Web site reads. "Whereas most certifications test on rote memorization-level details... SCP exams are designed to test a candidate's knowledge of working security issues, programs and utilities."

Currently, the program offers two titles: Security Certified Network Professional (SCNP) and the Security Certified Network Architect (SCNA). The SCNP focuses on defensive securi-

ty technologies, such as firewalls and intrusion detection. The SCNA focuses on the next level of technology, such as enterprise security solutions, forensics and biometrics.

Both titles require passing two exams each. The exams feature scenario-based questions. Although training is highly emphasized on the program Web site, it doesn't say that it's required before taking the exams.

SCNP exams cost \$150. SCNA exams cost \$180 (U.S.). All are available at Pearson Vue and Prometric testing centers worldwide.

The program requires all title

### SCP

**Vendor:** Ascendant Learning

**Certifications:** SCNP, SCNA

**Certification Type/Focus:** Mid- to high-level vendor-neutral security certifications.

**Exam Price:** \$150 to \$180 (U.S.)

**Training Required?:** No

**Testing Centers:** Pearson Vue and Prometric

**More information:** <http://www.securitycertified.net>

holders to recertify every two years.

For more information about these certifications, visit <http://www.securitycertified.net>.

— *Becky Nagel*

## Seeking the Sun

Solaris administrators worldwide now have a way to certify their expertise on this Unix-based operating system.

While there's still a dearth of Unix-specific security certifications available, at least one vendor has stepped up to the plate. In April 2003, Sun Microsystems debuted the Sun Certified Security Administrator (SCSA) for Solaris 9 OS.

This one-exam title is, in fact, the first security-specific certification to be offered by Sun. The objectives for the exam break down into six main areas:

- General security concepts
- Detection and device management
- Security attacks
- File and system resources protection
- Host and network prevention
- Network connection access, authentication and encryption

Although there are no prerequisites for this title, Sun recommends that all candidates hold either its Sun

Certified Network Administrator (SCNA) or Sun Certified Systems Administrator (SCSA) certification before attempting the exam. Six to 12 months of hands-on experience is also recommended.

Like other Sun tests, the Sun Certified Security Administrator exam contains multiple choice, scenario-based, matching, drag and drop and free-response questions. There are 60 questions, with 60 percent needed to pass. Candidates are given 90 minutes. The exam is available for \$150 (U.S.) at Prometric testing centers worldwide.

To give candidates an idea of what to expect, Sun offers 10 free sample questions for the SCSA on its Web site.

Because the certification is so new, it's only available for Solaris version 9.

### Sun

**Vendor:** Sun Microsystems

**Certification:** SCSA for Solaris 9

**Certification Type/Focus:** One-exam title testing security expertise in Solaris 9.

**Exam Price:** \$150 (U.S.)

**Training Required?:** No

**Testing Center:** Prometric

**More information:**

<http://suned.sun.com/US/catalog/courses/CX-310-301.html>

Sun has made no indication of creating exams for earlier versions, despite the continued popularity of its SCSA and SCSA for Solaris 8 exams.

More information about this certification can be found at: <http://suned.sun.com/US/catalog/courses/CX-310-301.html>.

— *Becky Nagel*

## Know Your Enemy

EC-Council offers white hats a chance to shine with its Ethical Hacker certification.

What exactly is an ethical hacker? The International Council of E-Commerce Consultants (EC-Council) states on its Web site: "The Ethical Hacker is an individual who is employed and can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods as a Hacker... The key difference is that the Ethical Hacker has authorization to probe the target."

Although passing the title's one exam does grant one the title of Ethical Hacker, the credential appears to really be aimed at systems administrators and

### EC-Council

**Vendor:** International Council of E-Commerce Consultants

**Certification:** Ethical Hacker

**Certification Type/Focus:** Tests knowledge of hacking terminology and techniques.

**Exam Price:** \$125 (U.S.)

**Training Required?:** No

**Testing Center:** Prometric

**More information:**

<http://www.cwne.com>

other security professionals who are interested in exactly what the other side is doing and how to prevent it.

The exam itself consists of 50 questions covering 22 domain areas, such as footprinting, system hijacking, hacking Web servers, SQL injection, password cracking techniques and ethics. It's available for \$125 at Prometric testing centers worldwide. EC-Council offers optional training for the title.

More information about this certification can be found at: <http://www.eccouncil.org/CEH.htm>.

— *Becky Nagel*

# Blueprint for a Career in Security

By Roberta Bragg

If you want to do IT security because it's "hot" right now, or because you think that's where the money is, forget it. If you truly love the field, read on.

What do I mean? Perhaps you're one of the many who have written for my help in "getting into security" or pursuing a security career. Perhaps you wonder if security is an area for you. Maybe you want the big bucks. Maybe you're out of a job, find your engagement calendar empty, or otherwise think it's time to change your game plan.

## You Missed the Wave, Dude

Security isn't the answer to your shrinking paycheck. It won't bring you fame and fortune; it won't even get you an interview. If you don't already have deep security knowledge, you don't have time to gain it in order to ride the current wave. The days of success are long past for those armed with minimal knowledge and a pre-programmed security vulnerability scanner. The word "Security" in your title or your company's name will get you no instant appreciation now. The market for security goods and services is more sophisticated than it was. To make your way, to survive, you have to be able to do more than know a few buzzwords.

This market isn't a Mecca for those who want to relax, either. Security is 10 percent pure panic and 90 percent drudgery. It's long hours with no reward. You'll generally only get recognition when you fail. For me, it's like I'm always hanging from a cliff by my

fingernails and struggling to keep up with the dual demands of rapidly changing information and rarely changing attitudes. Sure, it's fun to ramble about the foibles of most infrastructure gurus, but I can't even talk about my greatest jobs, those where my input or my design prevented the success of a very determined attacker.

## The Four-Step Program

Are you still reading, even after my attempts at dissuasion? You haven't given up in despair? You say you want to be a security expert, and you realize it's not an easy thing. Here, in my humble opinion, is how to fulfill that goal. Your program should include these four steps.

### Step One: Narrow Your Options

Your first step should be to determine exactly what you mean by "security." Do you want to specialize in some technical aspect of security, say establishing and configuring perimeter defenses such as firewalls? Do you absolutely love decoding packets to figure out what's happening on the wire? Are you obsessive-compulsive about the code you write? Does implementing technology excite you, or does the fact that your mistakes might provide a venue

for an attacker to steal credit card numbers off your servers grab your guts? Would you rather manage or do? Does creating policy float your boat? As you can see, there's a wide range of careers in security. I know security officers who have never touched a server, and systems admins who never should have.

To help you find your niche, consider attending a security conference. *Continued on next page*

## Hackers Need Not Apply

If you think that hacking into Web sites, writing and releasing malicious code or breaching security at Fortune 500 companies, government offices, utilities or other well-known entities is a precursor to or a guarantee of a security career, you're dead wrong. Doing these things is just plain stupid. You can disrupt business, shut down basic utilities and kill people. There's a new hardened attitude out there, and you may just find yourself doing time instead of working for the company of your choice.

—Roberta Bragg



You'll meet people who already work in the field, gain some security knowledge, and maybe make a few useful contacts. Check out the sites listed below and the conferences and seminars they offer. They represent many different sides of the security game. Just don't assume you'll see all security careers represented at any one event, or that you'll be accepted with open arms when you say the words "Microsoft" and "security."

- <http://www.rsasecurity.com>
- <http://www.sans.org>
- <http://www.gocsi.com/annual/index.html>
- <http://www.blackhat.com>
- <http://www.defcon.org>
- <http://www.issa.org>
- <http://www.misti.com>

### Step Two: Get Naked

Second, take a long look at yourself. Carefully review your background, successes and failures, dreams and reality. As they say in the weight-loss biz, stand in front of the mirror naked and take a good, long look. A clear understanding of your abilities, aptitudes and experience is the starting point. Having a clear goal will help you identify the path to take. Does something in your background fit your idea of this long-term goal? If your experience lies in networking or systems administration, you have a good foundation to build upon. Writing solid code and understanding good coding practices is paramount to many security careers. If you don't have either of these skill sets, why are you reading this article? Seriously, while many security jobs don't require you to code or to configure systems, they do require you to have knowledge in these areas. Get some. If you're struggling in IT because of a lack of ability to do a job for which you were trained, what makes you believe that you can enter the security arena without any experience or education at all?

Now the good news—maybe: If you stop and think about it, much of what you do in IT is security-related. Most systems administrators spend a fair amount of time granting or preventing resource access. Security is, in large part, about exercising controls in order to protect resources. If, however, you get your chuckles from making complex systems work, or writing elegant code, or getting the best performance or throughput, or the most "bang for the buck," then security may not be a wise choice for you.

On the other hand, if you feel that someone's always looking over your shoulder; if you have multiple online personalities; change out your hard drive when you go online; subscribe to multiple security newsletters (and actually read and follow their advice); have been to Defcon or a CSI conference; downloaded all the NSA guidelines; know who Stephen Northcutt, Bruce Schneier, Mudge and cDc are; purchased the SANS checklists; and have [www.microsoft.com/security](http://www.microsoft.com/security) as your default home page, you probably have the necessary makeup for the security field.

### Step Three: Get Trained

Now that you know where you are and what you want to do, determine what you need to do to get there. Each security opportunity may require a different skill set, a different level of education. Where not long ago there were no "security degrees" and only a smattering of certifications, both formal education and a plethora of certification programs now exist. The opportunities for education have multiplied like hack attacks on a new IIS server.

Are formal education programs the way to go? Remember: Security as a career has gone through its first two phases. In the first one, a need evolved as the natural result of the mainframe culture. Many people got trained on

the job, some were trained by the military, and others were gifted with deep talent and mathematical education. Few had formal training in computer security, per se. In the second phase, a large demand meant even inexperienced people could earn money peddling security advice, and many self-proclaimed hackers—the guys with the experience—were able to cut their hair and morph into security consultants.

Now we're in stage three. There's still a large demand, but buyers are more knowledgeable. To get hired, you need some proof of expertise. If you don't have experience, do you have certification or education? Employers today are certification-shy, and bad experiences with paper MCSEs have contributed to this. Several very good education alternatives exist, and you should start at <http://www.nsa.gov/isso/programs/nietp/newspg1.htm>. Among the offerings on the National INFOSEC Education & Training Program Web site are the 50 universities designated "Centers of Excellence in Information Assurance Education" by the National Security Agency. Take a look at these programs. You'll find that not one of them is a short-term answer to your goals. Most are traditional four-year undergraduate programs, or master's and doctorate programs. Some of the more well-known of these schools include:

- **Carnegie Mellon University:** (<http://www.heinz.cmu.edu/infosecurity/>), well-known as the host location for the Computer Emergency Response Team (CERT), as well as many fine programs that offer education in information security.
- **George Mason University:** (<http://www.isse.gmu.edu/~csis/index.html>)
- **Janes Madiscon University:** (<http://www.infosec.jmu.edu/program/html/classroom.htm>) offers a

*Continued on next page*

**"This is the way to learn!"**



 LearnKey 2003 Winner  
Best Computer Application Training  
Best Online Certification Training  
- Training Magazine 2003 APX awards

**First 20 Callers**  
**SAVE \$100!**  
on LearnKey Security Training

**Security is not an option!** LearnKey Security Training

<b>CISSP Series</b> ( Domains also sold separately) .....	11 Sessions.....C#150168.....	<b>\$2,995</b>
<b>Cisco® Certified Security Professional Series</b> (Prep for SECUR, CSPFA, CSVPN, CSI, & CSIDS Exams) .....	24 Sessions.....C#562198.....	<b>\$3,265</b>
<b>CompTIA® Security+</b> .....	4 Sessions.....C#101078.....	<b>\$355</b>
<b>Hacking Revealed</b> .....	5 Sessions.....C#150108.....	<b>\$425</b>
<b>Windows® 2000 Network Security Design</b> .....	3 Sessions.....C#601098.....	<b>\$265</b>
<b>ISA Server 2000</b> .....	4 Sessions.....C#601958.....	<b>\$355</b>

**FREE Security Training CD!**

*Choose from these popular titles:*  
**CompTIA® Security+ • CISSP • Cisco® SECUR**

 **Click Here**  
and register to get yours!

**HURRY!**  
First 50 Only!

- Training Features:**
- Dynamic instructor-led video
  - Powerful animations & graphics
  - Testing, labs and eSupport
  - 99% pass-rate

**www.learnkey.com/mcpsecurity / 1.800.865.0165 ext. 5256**

**LearnKey™**

© 2003 LearnKey, Inc. LK112503 Source Code #5256 Prices listed are for Single-Users. Please call for Multi-User pricing and Corporate solutions.

master's degree program with a concentration in information security, taught entirely online.

- **North Carolina State University:** (<http://ecommerce.ncsu.edu/infosec/courses.html>), offers undergraduate, masters and doctorate programs in information assurance.
- **University of Idaho:** (<http://www.csds.uidaho.edu/>), has the Center for Secure and Dependable Software (CSDS).

Be sure to check out the new Federal Cyber Service: Scholarship for Service programs if you're studying information security in college. U.S. citizens can get two years of their information security education paid for in return for two years of government information security work. Pay attention to the qualifications: Not every program—nor every candidate—qualifies. You must be enrolled in an info sec curriculum in one of several qualifying colleges before you can apply. Several of the programs referenced above participate in the program. Your best source of information is their Web sites.

And don't forget that good old practice of studying on your own or with your buds. I don't have to tell you that many of your peers in IT run extensive home test networks. If you're thinking of hitting the consultant career path, this is essential. It's my belief that you can earn the equivalent of a master's degree if you're willing to invest in a subscription to MSDN and TechNet, cobble together a few boxes in your basement and spend hours and hours with them. Note that it's my belief: I know of no college that will give you credit for your wee-hour explorations of PKI, Insect, Kerberos, group policy or other security-related items.

Many vendors have certifications, too. If you work extensively with their products or wish to, these certs—many

of which are profiled in the first part of this report—may help. Experience is more important, but studying for certification isn't a bad way to develop well-rounded product knowledge.

#### Step Four: Market Research

Research the job market. IT security employment is currently suffering a softening of the market. Visit IT recruiter L.J. Kushner (<http://www.ljkushner.com/>) to get the skinny on where they think it's headed; if you're qualified, post a resume.

Visit popular headhunter sites and do a search on information security. At Career Builder (<http://www.headhunter.net>) I found more than 371 jobs from the keywords "information security." Granted, a lot of jobs didn't fit my definition of info sec, but many did. Poring over the possibilities might just reveal some ideas you hadn't considered. How about being a senior fraud examiner, security manager, risk management-security and regulatory manager, security engineer, IT auditor, security engineering specialist, IT risk management specialist, policy maintenance senior specialist, acquisition security specialist, network security integrator, chief information privacy officer, security analyst, security system installer, director of IT security or HIPAA information security officer? Job listing sites are an excellent way to learn about the various security job categories and required experience level. You may be startled to learn that many pay less than a good network administrator job.

Graze through popular security product sites. Many of them have employment sections. Working for a security consulting firm or product company can boost your career. A word to the wise: Research the financial stability of these companies before you join. Many security startups got their funding during the high-tech expansion wars, when the word "Internet" was synonymous with "Cha-ching!" and

adding the word "security" was a double guarantee. Many of these companies are just treading water now; make your own inquiries before diving in.

Think outside the box. Did you notice the acronym "HIPAA" in the job list above? It stands for Health Insurance Portability and Accountability Act of 1996. Some of the regulations of this act mean radical changes in the way hospitals, doctor offices, insurance companies and anyone who handles patient information must do their job. While many institutions have a strategy in place, others are still trying to understand what they need to do. In either case, there will be a continued demand for IT security people in the health care industry.

#### If You're Still Interested...

By now you should have an idea that being a security professional is not donning a 10-year-old's T-shirt or doing the rock star strut across a stage. There's no surgical security implant or Viagra for the brain. You've found there's a crying need for those who know IT security, but no money to pay them; hordes of security babe-wannabes; and an immature industry where even the definition of "security professional" is undecided. If somehow you've made it to this point, you probably still want to pursue the dream, so go for it.

A version of this article was first printed in *Microsoft Certified Professional Magazine*.

---

*Roberta Bragg, MCSE: Security, CISSP, Security+ and contributing editor for MCP Magazine, runs Have Computer Will Travel Inc., an independent firm specializing in security, operating systems and databases. She's a frequent speaker and trainer for TechMentor. She's currently completing two books on network security for Microsoft Press. Contact her at [Roberta.bragg@mcpmag.com](mailto:Roberta.bragg@mcpmag.com).*

# Guide to Security Job Titles

Does adding “security” to already-existing IT job titles mean a new job for you? In some cases, yes.

A search of popular job search engines like Dice.com or ITjobs.com on the keywords “IT,” “network” and “security” will produce titles such as systems administrator and security administrator, network analyst and security analyst, or IS manager and IS security manager. Are these new jobs or the same jobs you’re familiar with, with security sneaking onto the list of responsibilities? Purely based on a random survey of jobs that are available out there, it’s a mixture of both.

The need for specialists pervades any profession and often produces new job titles—the IT profession is no different. New security titles have cropped up out of necessity and these types of jobs can be found primarily in medium to large organizations where security has to be controlled on a large scale. (That’s not to say that small companies don’t have their fair share of security jobs; you might find the odd need for a security analyst at a consulting or outsourcing firm.) Imagine, for example, having to manage and troubleshoot regularly scheduled password changes for an accounting firm, where data access is critical and can’t be interrupted.

Security encompasses issues beyond the traditional IT scope; for example, as with the Health Insurance Portability and Accountability Act of 1996. HIPAA is a recurring criteria for security-related jobs in healthcare and banking. Likewise, federal positions having to do with security may require you to possess a

security clearance—which isn’t something you can simply pick up when you need it, making that a factor beyond the usual IT job descriptions. (For more on this topic, read “About Those U.S. Government Security Clearances” later in this guide.)

In this article, we share various security-related job titles and what kind of work they entail. It isn’t meant to be a comprehensive list, but it covers the major ones you’ll run across in the course of scanning employment opportunities.

## Security Administrator

Security administrators typically are tasked with implementing security measures on a network. This may include: administering passwords, monitoring system or data security practices based on established company guidelines and monitoring and thwarting internal and external incidents (worms, viruses, Trojans and external or internal system abuses). They also might be in charge of disaster recovery efforts and typical network administrator duties.

Security administrators may have a hand in maintaining or recommending changes in established security policies and procedures.

Security administrators report to a project lead or manager.



## Security Engineer

Security engineers are typically involved in planning, managing and implementing higher-level security issues as they relate to systems and networks and are often tasked with evaluating security software and the impact that third-party software may have as it’s installed on a network. Security engineers usually have significant input on setting up security policies during the planning phase. The security engineer may fill roles as project leads and may even be a manager.

You’ll find security engineers among any type of IT engineer who performs a specialty. One interesting form of the security engineer on an ITjobs.com listing is the information assurance security engineer. This job’s differentiating factor was the concentration on certification and accreditation of systems/sites. For this job title, the company required someone with some form of government security clearance, since the job involved writing up information assurance activities on federal government customer systems and networks.

You might find jobs with specialties in database security and firewalls. Here’s an interesting twist on the secu-

rity engineer title: Enterprise Security Engineer, Ethical Hacker, for a Fortune 500 company in Chicago. The company requires “ethical hacking skills,” which often means programming expertise with a strength in developing exploits.

### Security Architect

Similar to security engineer in expertise, security architects are primarily responsible for establishing a framework for a comprehensive security strategy. The framework might involve drilling down to specific policies and procedures. Rarely is the security architect involved in implementation, unless providing hands-on support to a security team. Architects usually have a thorough understanding of network, application and database security.

Security architects can be highly specialized, such as one Dice.com listing for a “single sign-on architect.” It’s a highly specialized security architect whose sole responsibility is to design a single sign-on standard, often done for disparate network systems that need to be wholly secure across architectures.

The security architect might be interchangeable with the security manager at some companies or may report to a security manager.

### Security Consultant

Often someone whose breadth of experience encompasses security administrator to architect to director, security analysts or consultants often work in an outsource capacity to test and recommend security solutions or strategies. Security consultants and analysts should have extensive knowledge of network access, authentication, development of security policies and procedures and conducting vulnerability assessments. They may also be involved in security pre-sales engagements. The security analyst title may be interchangeable with the security consultant title.

One company on ITjobs.com posted a job for a “senior consultant, HIPAA security,” who would primarily play advisor and coordinator for pre-sales engagements to companies that required HIPAA compliance before forming partnerships.

Another listing called for a Security Analyst, Intrusion Detection/Forensics, a job whose defining characteristic was the ability to respond quickly to security incidents that can affect mission-critical production systems. Response had to be quick and thorough, particularly in assessing, documenting and offering solutions to thwart attacks. Another duty: That person would be tasked with developing new ways to harden systems.

Another job listing asked for a cyber security analyst. Based on the description, job duties matched up with a typical security consultant.

### Security Monitoring/Compliance Officer

This person implements and supports information security to maintain compliance with applicable laws. He or she acts as a resource on matters relating to information security and will investigate and recommend secure solutions for implementing IS security policy and standards. In some companies, the security monitoring/compliance officer might report directly to an enterprise security director or chief security officer, perhaps even to the CIO or CEO.

A Dice.com job listing asked for a specialized business information security officer (BISO) who would be responsible for IS audits and advising other groups of security requirements for line of business applications and concoct compliance reports in terms of business risk. The BISO would report to the officers of various groups, such as engineering directors and data center managers.

Another job was listed as fraud investigator, a highly specialized skill

that encompassed the same as a security monitoring/compliance officer, but also required some experience in legal evidence-gathering techniques.

### Security Director

Security directors are often the line between staff and executive management, usually leaning over to the latter. Security directors, though, make rare appearances on job search engines, because the responsibilities can be an amalgamation of higher-level duties taken on by a team of security managers, engineers and administrators. If such a job listing appears, it’s rarely for a small company. Typical responsibilities for security directors include: overseeing and coordinating security policies for IT and company-wide for departments like engineering, operations, legal and so on; developing and standardizing the communication of security, privacy policies and disaster recovery initiatives, often in accordance with industry regulations; and developing or driving security awareness training. Security directors typically report to a chief information officer or chief security officer.

### Chief Security Officer

At or near the top of a company hierarchy (CSO would report directly to the CTO or CEO), the chief security officer often dictates the companywide security mission or strategy. One high profile member of this elite corps is Howard Schmidt, previously the CSO for Microsoft, then pegged as cybersecurity advisor to the White House, and more recently vice president and chief information security officer for eBay. While it’s a mystery how CSOs differ from CIOs, many of the Fortune 500 companies like Microsoft and General Electric have them.

Consider these positions to be a rare breed, indeed.

—*Michael Domingo*



Knowledge.

# INTENSE SCHOOL

The IT & Security Training Experts

Security. 04

## Accelerated Security Training:

CCSP®

ISSEP Boot Camp

Computer Forensics

CompTIA Security+

CISSP® Boot Camp

Professional Hacking

MCSA/MCSE: Security 2003

Wireless Network Security



Locations in: Ft. Lauderdale, FL | New York Metro | Columbus, OH | San Diego, CA | Quebec, QC | Las Vegas, NV  
Washington, DC Metro | Atlanta, GA | Dallas, TX | San Francisco, CA | Chicago, IL | Los Angeles, CA | Seattle, WA

INTENSE SCHOOL - 8211 W. BROWARD BLVD FORT LAUDERDALE, FL 33324 Ph.800-330-1446 [www.intenseschool.com](http://www.intenseschool.com)



# Q&A: Can Security Certifications Help Your Career?

We asked a security insider to share his honest take on exactly what security certifications can—and can't—do for your job prospects.

*Greg Owen is technical director for the Global Information Assurance Certification (GIAC), a vendor-neutral certification program sponsored by the SANS Institute. He holds three GIAC certifications:*

- *GIAC Certified Incident Handler (GCIH)*
- *GIAC Certified Windows Security Administrator (GCWN)*
- *GIAC Certified Forensic Analyst (GCFA)*

*Part of his duties with GIAC include exam preparation. Owen also does network security consulting for a consulting company in Boston, Massachusetts. He's been working in IT, including network security, for more than 10 years.*

## Are security certifications becoming more important or less so in the current market?

**Greg Owen:** It's becoming more important. The larger the company, the more reliant they are on the certification. The events of the last couple of years are starting to drive home to everybody the point that security is more important than it used to be. For a large company, it's hard for them to make a shift like that. Human resources needs to have something they can look for to differentiate that "this is a candidate who can do what we want; this [one isn't]." At one bank I've worked with, their security people almost universally hold the CISSP.

## Can you get a security-related job with certification and no experience?

I think the security certification helps a lot, in the situation where someone's been doing IT and has gotten certification and had to deal with corners of the

security problems from time to time. That cert makes it more official that they do know this area. They've probably had to deal with it, probably had to help out. I think that for a person with no IT experience, to go out and get a cert is not as useful, but that's not the case for the vast majority of people who are [pursuing security certification]. It can still be useful for someone without experience, but employers are looking for the combination of experience and testable proof.

## Should you wait until you've been in security for some years before getting certs?

I think a year or two is useful, but the thing about security is it's something people have to deal with all the time. Having a job on your resume that has to do with security [is helpful].

## Do security certifications help if you want to become a security consultant?

I think so. Whenever a consulting firm or independent consultant comes in to bid for a job, the good ones will have a page on the back which has a quick bio of the people they're proposing to send in on the job [and certifications show up well].

Consulting [for independent consultants] is as much a sales issue as anything else, and part of the sales issue is saying, "Yes, I know what I'm doing, and here's what I have to prove it." Certifications can be very helpful to prove that.

## Will there be further areas of security certification specialization?

It depends on the size of the company. In larger companies, I'm definitely seeing a trend toward specialization, simply

because they're so big that one person can't do all the jobs. Having said that, I don't think being fully specialized is a helpful thing, especially in security. I think knowing a little bit about everything helps you do one thing better. Broad experience and broad understanding of the entire problem area makes dealing with specific areas easier.

## Is there value in platform-specific certification, like Microsoft or Cisco?

There definitely is. With specific respect to security, I don't know how much the Microsoft [security specialization] will help. It's only recently that they've added the security specialization. I think the attitude is, "Why would you go to the vendor who shipped the broken software in the first place to tell you how to fix it?" There's a certain amount of hesitancy there, but specific training is definitely valuable if you're going to be working in that area. If you're looking for a Windows network administrator, you definitely want them to have their MCSE. If you have a large Cisco infrastructure and you need that supported, you're going to want Cisco certification.

## What would you tell someone who wanted a security certification because it's the "hot" field right now?

I wouldn't recommend that somebody go into it if they haven't had an interest in it, just because of that [*i.e.*, it's popular at the moment]. Like any profession, if you're just going into it for the money, if you're not truly interested in the challenges, it will show to employers. They'll see that. If you don't enjoy doing that kind of work, if you don't enjoy walking that walk, I'm not sure I'd recommend it.

— *Keith Ward*

# Salary Data for IT Security Professionals

“The true source of long-run wealth is for us to specialize in what we are best at,” writes Brad DeLong, economics professor at U.C. Berkeley. He may have been explaining 19th century economist David Ricardo’s principle of “comparative advantage” in simpler terms, but DeLong’s explanation has application with IT careers.

Becoming a specialist can be one way to make some personal improvements in your career and sustain your good fortune in these shaky times. Several current surveys of IT salaries among those who specialize in security skills show modest gains against contemporaries who don’t indicate a specialty.

Take Salary.com, which offers basic ongoing reporting of salaries within the U.S., compiling data from thousands of human resources departments. Based on its report for Nov. 11, median average salary for network administrators across the U.S. was \$54,458. Compare that to security administrators, whose median was \$62,074, a 12 percent increase.

*ComputerWorld’s* 2003 compensation survey backs up Salary.com’s data with a more pronounced increase. Network administrators earned \$51,265 on average, while IS security specialists said they earned \$70,780. Specialization here may account for a 26 percent increase.

Salaries qualified by certification show increases that are just as remarkable. The *Microsoft Certified Professional Magazine* 2003 Salary Survey (*MCP Magazine* and *CertCities.com* are both 101communications LLC companies) reports that the average base salary for MCPs was \$61,700. Respondants who held additional security-based certifications like Microsoft’s own ISA Server or CISSP,

Title	Salary
MCP*	\$61,700
ISA Server	\$65,100
(ISC) <sup>2</sup> Systems Security Certified Practitioner	\$77,500
Check Point Certified Security Expert	\$78,500
(ISC) <sup>2</sup> : Certified Information System Security Professional (CISSP)	\$78,800
Cisco Certified Security Professional	\$93,500

*Table 1. Comparing salaries of MCPs and those holding security-specific certifications.*

\* Average base salary of all MCPs; all other figures come from Chart 8, “Salary by Other Certifications,” from the 2003 *MCP Magazine* Salary Survey. More at <http://mcpmag.com>.

as well as the MCP, made at least \$4,000 more, and in some cases \$30,000 more (see Table 1).

While specializing may seem to be the next logical step, salary numbers like those shown on these reports aren’t guaranteed. Remember that salary surveys only provide a snapshot of salaries among the employed as those surveys were conducted. Obtaining a security specialty only means your breadth of expertise may give you an advantage over peers. Whether that translates to additional compensation is up to your employer and your powers of persuasion over the one who signs your check.

Looking into 2004, it’s tough to know how valuable the security focus in your portfolio will continue to be. What’s hot today can grow cold tomorrow in IT. We’d advise you to stay in touch with published information on compensation; but remember, those numbers can’t pinpoint what a particular individual should earn. Variables such as geographic location, years of experience, type and size of organization and negotiating skills come into play in any given scenario.

To find detailed salary survey information, check out these links:

- **Salary.com:**

(<http://www.salary.com>) Get daily salary reports just by clicking on the simple criteria. Data changes

because Salary.com gathers it on a continual basis.

- **ComputerWorld 2003 Salary Survey:**

(<http://www.computerworld.com/areertopics/careers/story/0,10801,86413,00.html>). Published in October 2003, data comes from more than 19,000 responses.

- **Microsoft Certified Professional Magazine 2003 Salary Survey:**

(<http://mcpmag.com/salarysurveys/>) *MCP Magazine* is known for its yearly survey of certified professionals working with Microsoft products. Data collected from more than 6,000 respondents.

- **Janco Associates:**

(<http://www.psrinc.com/salary.htm>) This technical outsourcing firm gathers compensation data from more than 400 mid- and large-sized companies twice a year. The most recent report was published in June.

- **Foote Partners LLC:**

(<http://www.footepartners.com/salaryresearch.htm>) Collects salary data from 35,000 IT workers on a quarterly basis. Reports are costly, but the sample versions have a significant amount of data.

More links to salary surveys can be found on CertCities.com at [http://certcities.com/editorial/salary\\_surveys/](http://certcities.com/editorial/salary_surveys/).

—*Michael Domingo*

# About Those U.S. Government Security Clearances

You've found a job whose description fits you perfectly except for one small matter: It requires a security clearance and you don't have one. As with many things in life, getting this particular position would be a long shot for you, but that doesn't mean you shouldn't try anyway.

The fact is that security clearance is something you can't obtain for yourself. Your current or prospective employer has to set the wheels in motion to get it for you. Since the process is costly and time-consuming, organizations won't do it unless it's absolutely essential. Let's review the basics.

You typically need a security clearance when you hold a sensitive position within the federal government or when you work for a government contractor or some other organization that has access to classified information or deal with other restricted information relating to national security. Clearances come in many different flavors, primarily confidential, secret, top secret, and sensitive compartmented information (SCI).

Once a person has been offered a position that requires a clearance, the employer opens up a request with the Office of Personnel Management through a federal security officer. The OPM gives the candidate undergoing the clearance check access to an online system called e-Qip, or Electronic Questionnaire for Investigations Processing, a digital version of Standard Form 86 ([http://www.usaid.gov/procurement\\_bus\\_opp/procurement/forms/SF-86/sf-86.pdf](http://www.usaid.gov/procurement_bus_opp/procurement/forms/SF-86/sf-86.pdf)).

SF 86 is a 13-page document that asks you to list your vitals—name, social security number, place of birth, etc.—and then drills down on your personal history going back at least seven years. You're expected to list where you've lived for the last seven years, where you went to school, your employment activities—

including titles, supervisor names and supervisor addresses—people who know you well aside from spouses and relatives, relatives and associates (along with their dates of birth, country of birth and current address), your military history and foreign activities (including travel for business and pleasure), police records, medical records, financial records and delinquencies, use of illegal drugs and alcohol, and groups you associate with that espouse the violent overthrow of the government.

Sound comprehensive? The idea is to weed out those who aren't (according to SF 86) "reliable, trustworthy, of good conduct and character, and loyal to the United States." The same form also warns that your current employer will be contacted and questioned, whether you want them to be or not.

Your form and your fingerprints go to the Federal Investigations Processing Center, which calls on investigators—both federal employees and contract—to start confirming what you've said on the form. During this phase of the process, investigators review available records (including your presence on the Internet), check with the police, run a credit check on you and talk to people who know you—those you've listed on the form as well as people in a position to observe you, such as neighbors. Plus, you'll be interviewed yourself.

All the data that's collected ends up in a single file, called "The Report of Investigation," which is sent to the federal agency that asked for the investigation in the first place. At that point, it's up to the federal security officer at the agency of hire to determine your eligibility to have a position with access to secure information. You may get the chance to explain or refute negative or unclear information during this "adjudication phase." Then your clearance is either

granted or denied.

If it's granted, the fun doesn't stop there. Depending on what level of clearance you have, you'll have to undergo reinvestigation every five, 10 or 15 years. If you leave that position, the clearance is still active, but it may not be usable by your next employer—depending on what type of security clearance the new job requires. Let enough time pass and the clearance will have no merit at all.

The whole process of obtaining a clearance can take many months—sometimes longer than a year—and cost several thousands (even tens of thousands) of dollars. The more sensitive the job, the deeper—and the costlier and more time-consuming—the investigation. You can't speed up the effort, nor can you offer to pay the cost. That's why so many jobs listing security clearance as a requirement are anxious to find candidates who already possess a clearance of the right type—the project may be over by the time somebody new to the process obtains his or her clearance. If you've noticed the propensity of government contractors to intensely recruit ex-military people for open positions, it's because vets frequently come with the security clearance that's needed as part of their portfolio.

If you don't already have a security clearance but there's a particular organization you're determined to work for, your best approach is to obtain employment that doesn't require the clearance with the agency or firm. Then put in your time and make it clear to your manager that should the right opportunity present itself, you'd be willing to undergo the investigation. But temper your enthusiasm: Too much eagerness to undergo this in-depth exploration into your personal and professional life might be viewed as suspicious behavior.

— *Dian Schaffhauser*

# 15 Best Web Sites for Security

## 1. Microsoft TechNet IT Pro Security Zone

<http://www.microsoft.com/technet/security/community/default.msp>

The IT Pro Security Zone is Microsoft's newest security portal. It's your one-stop shop for Microsoft-related security newsgroups, latest patches, chats and special events, security articles, FAQs and lots more.

## 2. CERT Coordination Center

<http://www.cert.org/>

The Computer Emergency Response Team helps protect the Internet through various means. It constantly monitors public networks for attacks, and normally knows one is coming before it hits. A treasure trove of great information.

## 3. NTBugtraq

<http://www.ntbugtraq.com>

Everyone in the security community knows Russ Cooper, TruSecure's Surgeon General. This is his Web site, which offers one of the most active security newsgroups on the Net.

## 4. InfoSec Reading Room

<http://www.sans.org/rr/>

SANS is well-known for its security training. Its InfoSec Reading Room has more than 1,200 security white papers in 70 different categories. All the major platforms are covered, including mainframes, Unix, Linux, Mac/Apple and Windows.

## 5. WildList Organization International

<http://www.wildlist.org/>

The best source of information on what viruses are currently out there "in the wild." Serious security people check this list constantly.

## 6. LinuxSecurity.com

<http://linuxsecurity.com>

This is an excellent site for Linux security administrators. Contains Linux security-specific news, advisories, tools and research.

## 7. Windows 2000 Security Operations Guide

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=f0b7b4ee-201a-4b40-a0d2-cdd9775aef8>

This guide is a must-have document for anyone with Windows 2000 servers on their network. Following the step-by-step instructions can drastically reduce successful attacks on your network.

## 8. Common Criteria

<http://www.commoncriteria.org/>

Common Criteria provides a set of standards for information security. Products are submitted to CC for testing and then given a rating based on their overall level of security. The higher the number, the better.

## 9. InfoSec News

<http://www.infosecnews.com/>

One of the few sites that specializes in computer security news. It's updated daily and contains a broad range of content.

## 10. SecurityStats.com

<http://www.securitystats.com/>

Want to follow the legal trials and tribulations of your favorite hackers? Find out how much the MS Blaster Worm cost companies? Keep up on Web defacements? Security Stats is the place to do that and get lots of other good security information.

## 11. Hacker Wacker

<http://www.hackerwhacker.com/>

One of the best features of this security-packed Web site is the ability to do free remote security scans of your network and firewall. See what the hackers are seeing.

## 12. InfoSysSec

<http://www.infosyssec.org/>

Like many of the sites listed here, this one offers a wealth of security-related information. However, this site also lists the Top 10 IP addresses from which Internet attacks are being launched and the Top 10 ports that are being attacked.

## 13. HIPAA.org

<http://www.hipaa.org/>

Are you unsure of how the Health Insurance Portability and Accountability Act (HIPAA) works? If you're a security consultant, you should know, since there's a lot of money to be made by ensuring HIPAA compliance. This site is a good starting point.

## 14. CSRC NIST PKI Program

<http://csrc.nist.gov/pki/>

Thinking about instituting a Public Key Infrastructure? If so, this site from the National Institute of Standards and Technology is the best place to begin your research.

## 15. 2600

<http://www.2600.com/>

Why is the most famous hacker Web site of all on this list? Because to fight hackers, it's important to understand their mindset.

— Keith Ward

# 5 Must-Read Security Newsletters

## 1. TechNet Flash

<http://www.microsoft.com/technet/subscriptions/current/suboserv.asp>

TechNet Flash is Microsoft's bi-weekly newsletter covering all things TechNet. Of course, one of its main purposes is to alert you of the newest security vulnerabilities, patches, hotfixes and procedures for securing your network.

## 2. Security Watch

<http://lists.101com.com/nl/main.asp?NL=mcpmag>

Security Watch, published by the same folks who produce *Microsoft Certified Professional Magazine*, provides lots of original content (something often difficult to find in newsletters). Included in each issue is a commentary by Windows security expert Roberta Bragg and a roundup of top security stories by ENTMag.com editor Scott Bekker. If you have security responsibilities on a Windows network, this newsletter is a must-read.

## 3. Crypto-Gram

<http://www.counterpane.com/crypto-gram.html>

Crypto-Gram is a free monthly newsletter from Bruce Schneier, the field's foremost expert in cryptography. Schneier comments on a host of security topics, covering a broad range of issues. He's never at a loss for a strong opinion on any security-related topic.

## 4. SANS Critical Vulnerability Analysis Report

<http://www.sans.org/newsletters/cva>

The SANS Critical Vulnerability Analysis Report is a weekly bulletin of top vulnerabilities. SANS, a security training company, lists the risk levels with each vulnerability, potential damage of each and links to learn more about them.

## 5. Asian School of Cyber Laws

<http://www.asianlaws.org/infosec/newsletter/index.htm>

The first reaction to the "Asian School of Cyber Laws" is usually, "What the heck is that?" It's a public organization

based in India that, among other activities, publishes a bi-weekly security newsletter that's mostly news, but also has sprinklings of opinion scattered throughout. Solid coverage of security news throughout the world, not just the United States.

— Keith Ward

*Note: Only free newsletters were considered for this list. Most of us have enough things to pay for without shelling out for electronic newsletters.*

## 5 Web Picks for Security Certification

### 1. CCCure.org

<http://www.cccure.org>

This top-notch site for CISSP candidates is packed with useful preparation tools, including exam reviews, news, research and an expansive collection of practice questions. A similar site worthy of prospective CISSP candidates can be found at <http://www.cissps.com/>.

### 2. Rtek2000 Security Links

<http://www.rtek2000.com/Tech/InternetSecureLinks.html>

This page from training company Rtek2000 hosts one of the most comprehensive security link collections available, covering just about every baseline topic tested on security certification exams (and then some). The perfect place to begin your online studies.

### 3. CertCities.com Security Exam Reviews

<http://www.certcities.com/certs/security/exams/>

Go here to read CertCities.com's collection of security-related exam reviews, including Microsoft's 70-214, CompTIA's Security+ and (ISC)<sup>2</sup>'s CISSP.

### 4. Certification-Crazy's Security+ Resources

<http://www.certification-crazy.net/security+.htm>

Scroll down to view a nice list of online Security+ resources from a fellow candidate.

### 5. GetCertified4Less.com

<http://www.getcertified4less.com/testvoucher.asp>

Offers discounted vouchers for Microsoft, Cisco, Check Point and CompTIA exams.

— Becky Nagel



# THE ANTI-SPAM SUMMIT

**MARCH 17-19, 2004**  
THE PALACE SAN FRANCISCO, CA

**You know** what e-mail abuse costs your business.

**You've tried** to stop it.

**Now attend** the only industry summit  
focused solely on the technical and  
business issues surrounding spam.

## COME LEARN ABOUT:

- The best-of-breed tool overviews
- The latest technologies
- Case studies straight from your peers
- Legislation and regulation
- What the major ISPs are doing

## PRESENTERS:

Hear from top names fighting the spam problem today: Experts from AOL, Yahoo, Microsoft, the FTC, California's Office of Privacy Protection, and many more.

- **Ryan Hamlin**  
General Manager,  
Microsoft's Anti-Spam  
Technology and Strategy Group
- **Jon Praed**  
Founding Partner,  
Internet Law Group

## WHAT THE SUMMIT OFFERS:

- A technical track will focus on tools and technical solutions for **systems administrators, network managers, analysts, IT managers and administrators** – anyone fighting spam in the trenches.
- A business track will focus on legislation, regulation, costs, and other business issues for **IT managers, vice presidents, technical developers, and chief privacy officers, chief security officers, and other C-level executives.**

Sponsored by 101communications and *Microsoft Certified Professional Magazine*

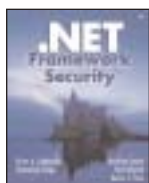


# Security Bookshelf

Popular print resources for security technology and certification.

## .NET Framework Security

Brian A. LaMacchia, Sebastian Lange, Matthew Lyons, Rudi Martin, Kevin T. Price  
Addison-Wesley  
067232184X  
April 24, 2002  
\$57.99

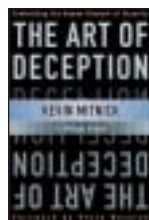


## Anti-Hacker Tool Kit

Keith J. Jones, Mike Shema, Bradley C. Johnson  
McGraw-Hill Osborne Media  
0072222824  
June 25, 2002  
\$59.99

## The Art of Deception : Controlling the Human Element of Security

Kevin D. Mitnick, William L. Simon  
Hungry Minds  
076454280X  
October 2003  
\$16.95



## Authentication: From Passwords to Public Keys

Richard E. Smith  
Addison-Wesley  
0201615991  
October 1, 2001  
\$44.99

## Beyond Fear: Thinking Sensibly About Security in an Uncertain World

Bruce Schneier  
Copernicus Books  
0387026207  
September 2003  
\$25

## Building Secure Software: How to Avoid Security Problems the Right Way

John Viega, Gary McGraw  
Addison-Wesley  
020172152X  
September 24, 2001  
\$54.99

## Building an Information Security Awareness Program

Mark B. Desman  
Auerbach  
0849301165  
October 30, 2001  
\$49.95

## Building Internet Firewalls (2nd Edition)

Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman  
O'Reilly & Associates  
1565928717  
January 15, 2000  
\$49.95

## The CERT Guide to System and Network Security Practices

Julia H. Allen  
Addison-Wesley  
020173723X  
June 7, 2001  
\$39.99



## Computer Forensics: Incident Response Essentials

Warren G. Kruse II, Jay G. Heiser  
Addison-Wesley  
0201707195  
September 26, 2001  
\$44.99

## Computer Security Incident Handling: Step-by-Step (Version 2.3.1)

Stephen Northcutt  
SANS Institute  
0972427376  
March 2003  
\$29.99

## Counter Hack: A Step-by- Step Guide to Computer Attacks and Effective Defenses

Ed Skoudis  
Prentice Hall  
PTR  
0130332739  
July 23, 2001  
\$49.99



## Computer Security Handbook

Seymour Bosworth and Michel E. Kabay, Editors  
John Wiley & Sons  
0471412589  
April 2002  
\$80

## Designing Security Architecture Solutions

Jay Ramachandran  
John Wiley & Sons  
0471206024  
March 1, 2002  
\$55

## The E-Policy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies

Nancy L. Flynn  
AMACOM  
0814470912  
November 2000  
\$19.95

## The Effective Incident Response Team

Julie Lucas, Brian Moeller  
Addison-Wesley  
0201761750  
September 26, 2003  
\$39.99



## Firewall Architecture for the Enterprise

Norbert Pohlmann, Tim Crothers  
John Wiley & Sons  
July 8, 2002  
076454926X  
\$49.99

## Firewalls: The Complete Reference

by Keith Strassberg, Gary Rollie, Richard Gondek  
McGraw-Hill Osborne Media  
0072195673  
May 28, 2002  
\$59.99

## Firewalls and Internet Security: Repelling the Wily Hacker, Second Edition

William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin  
Addison-Wesley  
020163466X  
February 24, 2003  
\$49.99

## The Hack Counter-Hack Training Course: A Desktop Seminar

Edward Skoudis  
Prentice Hall PTR  
013047729X  
June 14, 2002  
\$69.99

## Hacker's Challenge 2: Test Your Network Security & Forensic Skills

Mike Schiffman, Bill Pennington, David Pollino, Adam J. O'Donnell  
McGraw-Hill Osborne Media  
0072226307  
December 18, 2002  
\$39.99



Continued on next page

**Hacking Exposed: Network Security Secrets & Solutions, Fourth Edition**

Stuart McClure, Joel Scambray, George Kurtz  
McGraw-Hill Osborne Media



0072227427  
February 25, 2003  
\$49.99

**Hacking Exposed Web Applications**

Joel Scambray, Mike Shema  
McGraw-Hill Osborne Media  
007222438X  
June 19, 2002  
\$49.99

**Hacking Exposed Windows 2000**

Joel Scambray, Stuart McClure  
McClure  
0072192623  
August 29, 2001  
\$49.99



**Hacking Exposed Windows Server 2003**

Joel Scambray, Stuart McClure  
McGraw-Hill Osborne Media  
0072230614  
October 27, 2003  
\$49.99

**Hacking Linux Exposed**

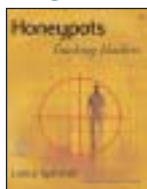
Brian Hatch, James B. Lee, George Kurtz  
0072127732  
March 27, 2001  
\$39.99

**HackNotes Web Security Pocket Reference**

Mike Shema  
McGraw-Hill Osborne Media  
0072227842  
June 30, 2003  
\$29.99

**Honeypots: Tracking Hackers**

Lance Spitzner  
Addison-Wesley  
0321108957  
September 10, 2002  
\$44.99



**Incident Response: Investigating Computer Crime**

Chris Prorise, Kevin Mandia  
McGraw-Hill Osborne Media  
0072131829  
June 21, 2001  
\$39.99

**Information Security Architecture, Second Edition**

Jan Killmeyer Tudor  
CRC Press  
0849315492  
June 28, 2003  
\$79.95

**Information Security Architecture: An Integrated Approach to Security in the Organization**

Jan Killmeyer Tudor  
CRC Press  
0849399882  
September 25, 2000  
\$69.95

**Information Security Management Handbook, Fourth Edition, Volume 4**

Micki Krause and Harold F. Tipton, Editors  
Auerbach  
0849315182  
November 26, 2002  
\$69.95



**Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management**

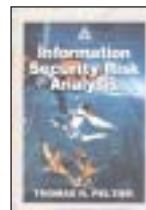
Thomas R. Peltier  
CRC Press  
0849311373  
December 20, 2001  
\$69.95

**Information Security Policy Manual**

Edmond D. Jones  
Rothstein Associates  
1931332096  
February 23, 2001  
\$89

**Information Security Risk Analysis**

Thomas R. Peltier  
Auerbach  
0849308801  
January 23, 2001  
\$69.95



**The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program**

Gerald L. Kovacich  
Butterworth-Heinemann  
0750698969  
May 1998  
\$41.95

**Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems**

Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Fredrick, Ronald W. Ritchey  
Que  
0735712328  
June 28, 2002  
\$49.99

**Intrusion Detection with Snort**

Jack Koziol  
SAMS  
157870281X  
May 20, 2003  
\$45

**Intrusion Signatures and Analysis**

Mark Cooper, Stephen Northcutt, Matt Fearnow, Karen Frederick  
Que  
0735710635  
January 29, 2001  
\$39.99

**Kerberos: A Network Authentication System**

Brian Tung  
Addison-Wesley  
0201379244  
May 4, 1999  
\$19.95

**Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community**

The HoneyNet Project  
Addison-Wesley  
0201746131  
August 31, 2001  
\$39.99



**Linux Security Cookbook**

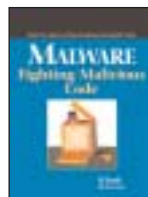
Daniel J. Barrett, Richard E. Silverman, Robert G. Byrnes  
O'Reilly & Associates  
0596003919  
June 2003  
\$39.95

**Linux Server Hacks**

Rob Flickenger, Editor  
O'Reilly & Associates  
0596004613  
January 2003  
\$24.95

**Malware: Fighting Malicious Code**

Ed Skoudis, Lenny Zeltser  
Prentice Hall PTR  
0131014056  
November 9, 2003  
\$44.99



**Managing A Network Vulnerability Assessment**

Justin Peltier, John A. Blackley, Thomas R. Peltier  
Auerbach  
0849312701  
May 30, 2003  
\$59.95

*Continued on next page*

### Network Intrusion Detection, Third Edition

Stephen Northcutt, Judy Novak  
Que  
0735712654  
August 27, 2002  
\$49.99

### Network Security: Private Communication in a Public World

Charlie Kaufman, Radia Perlman, Mike Speciner  
Prentice Hall PTR  
0130460192  
April 15, 2002  
\$54.99

### PKI: Implementing & Managing E-Security

Andrew Nash, Bill Duane, Derek Brink, Celia Joseph  
McGraw-Hill Osborne Media  
0072131233  
March 27, 2001  
\$49.99



### Practical Unix & Internet Security, 3rd Edition

Simson Garfinkel, Gene Spafford, Alan Schwartz  
O'Reilly & Associates  
0596003234  
February 2003  
\$54.95

### Real World Linux Security: Intrusion Prevention, Detection and Recovery

Bob Toxen  
Prentice Hall PTR  
November 2000  
0130281875  
\$44.99

### Secrets and Lies: Digital Security in a Networked World

Bruce Schneier  
John Wiley & Sons  
0471453803  
January 2004  
\$17.95

### Security Architecture: Design, Deployment and Operations

Christopher King, Ertem Osmanoglu (Editor), Curtis Dalton  
McGraw-Hill Osborne Media  
0072133856  
July 30, 2001  
\$49.99

### The Shellcoder's Handbook : Discovering and Exploiting Security Holes

Jack Koziol, David Litchfield, Dave Aitel, Chris Anley, Sinan Eren, Neel Mehta, Riley Hassell  
John Wiley & Sons  
0764544683  
March 2004  
\$50

### Snort 2.0 Intrusion Detection

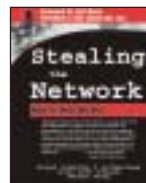
Brian Caswell, Jay Beale, James C. Foster (Editor), Jeremy Faircloth (Editor)  
McGraw-Hill Osborne Media  
0072226307  
December 18, 2002  
\$39.99

### Special Ops: Host and Network Security for Microsoft, UNIX, and Oracle

Erik Pace Birkholz, Stuart McClure  
Syngress  
1931836698  
February 17, 2003  
\$69.95

### Stealing the Network: How to Own the Box

Ryan Russell (Editor), Ido Dubrawsky, FX  
Syngress  
1931836876  
June 2003  
\$49.95



### SQL Server Security

Chip Andrews, David Litchfield, Bill Grindlay  
McGraw-Hill Osborne Media  
0072225157  
August 27, 2003  
\$49.99

### SQL Server Security Distilled

Morris Lewis  
APress  
1590591925  
July 1, 2003  
\$39.99

### Web Hacking: Attacks and Defense

Stuart McClure, Saamil Shah, Shreeraj Shah  
Addison-Wesley  
0201761769  
August 8, 2002  
\$49.99



### Writing Information Security Policies

by Scott Barman  
Que  
157870264X  
November 9, 2001  
\$34.99

### Writing Secure Code

Michael Howard and David LeBl, David LeBlanc  
Microsoft Press  
0735615888  
December 15, 2001  
\$39.99

—*Michael Domingo*

## Advertiser Index

### Global Knowledge

[www.globalknowledge.com](http://www.globalknowledge.com)

Global Knowledge is a worldwide leader in IT education and offers over 31 hands-on security training courses.

### Intense School

[www.intenseschool.com](http://www.intenseschool.com)

The Security Training Experts. 2003 Award Winners.

### LearnKey, Inc.

[www.learnkey.com/mcpsecurity](http://www.learnkey.com/mcpsecurity)

Free Security Training CD. Sec+, CISSP, SECUR. Hurry 50 only!