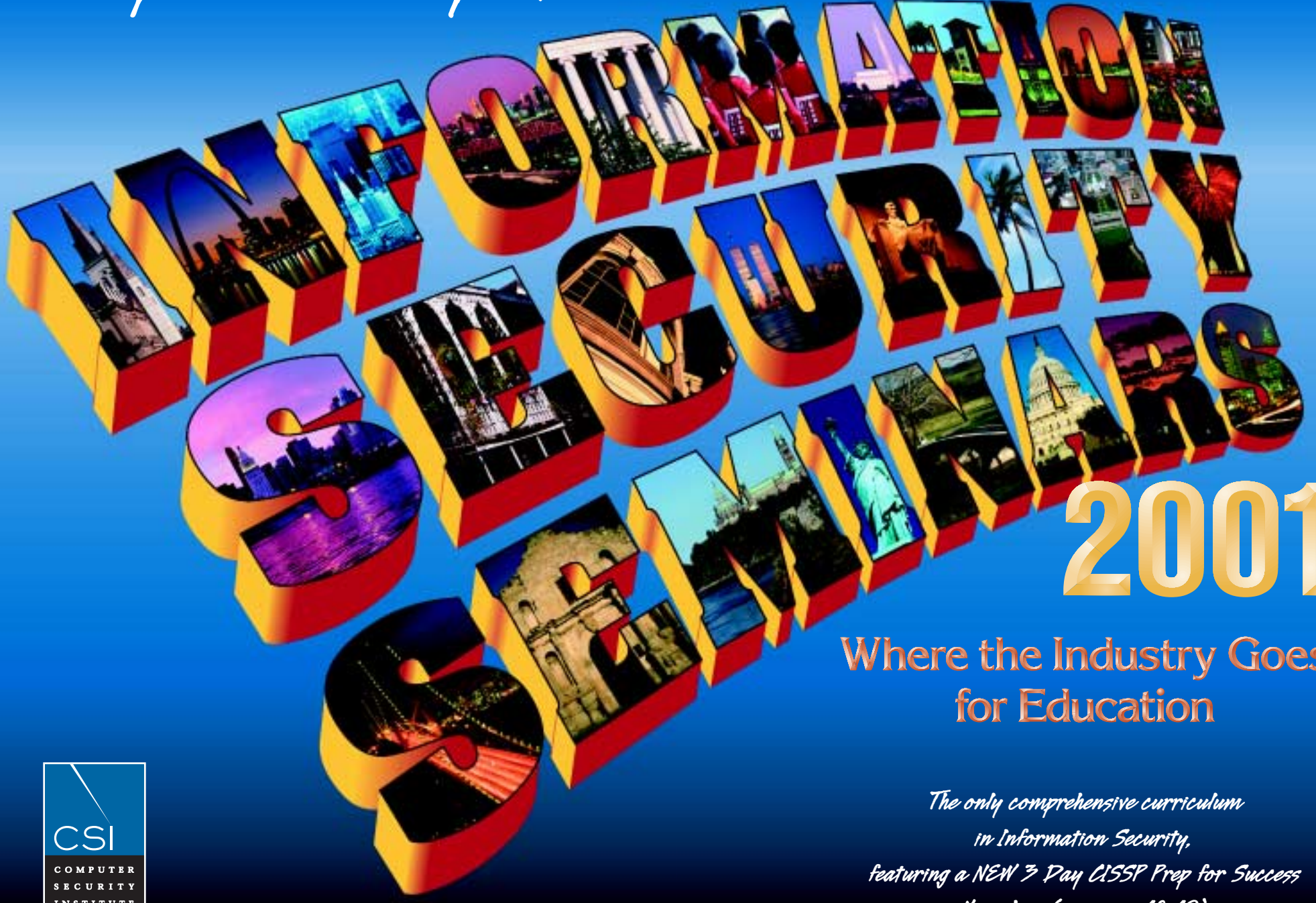
Computer Security Institute



2001

Where the Industry Goes for Education

The only comprehensive curriculum in Information Security, featuring a NEW 3 Day CISSP Prep for Success Workshop (see pages 18-19).

CSI
COMPUTER SECURITY INSTITUTE

www.gocsi.com

Information Security Seminars 2001

Training Schedule

register online at
www.gocsi.com

Phone 415.947.6320
Fax 415.947.6023
Email csi@cmp.com

Date	Course Title	City	Instructor
January			
22-23	Practical Forensics: How to Manage IT Investigations	Ontario, Calif.	Peter Garza
24-26	Technical Recovery of Electronic Evidence *(Hands-on)*	Ontario, Calif.	Peter Garza
30-31	Management Skills for a Superior Information Security Program	Phoenix, AZ	John O'Leary
February			
1-2	Firewalls and VPNs	Phoenix, AZ	Fred Avolio
6-7	Introduction to Computer and Network Security	Gaithersburg, MD	John O'Leary
8-9	How to Manage a Network Vulnerability Assessment	Gaithersburg, MD	John O'Leary
13-14	A 6-Step Framework for Incident Response	Marietta, GA	Gene Schultz
13-14	Internet Security Tools and Techniques	Marietta, GA	Fred Avolio
15-16	Practical Forensics: How to Manage IT Investigations	Marietta, GA	Peter Garza
15-16	Intrusion Techniques and Countermeasures	Marietta, GA	Rik Farrow
March			
13-14	Securing E-Business: A Technical Guide to Implementing PKI	New York City	Anish Bhimani
14-16	3-Day CISSP Prep for Success	Phoenix, AZ	Team
15-16	How to Design a Security Architecture for eBusiness	New York City	David Lynas
27-28	Windows 2000 Security	St. Louis, MO	Joel Scambray
29-30	How to Manage a Network Vulnerability Assessment	St. Louis, MO	John O'Leary
April			
3-4	How to Create & Sustain a Quality Info Security Awareness Program	Phoenix, AZ	John O'Leary
3-4	How to Develop Information Security Policies	Gaithersburg, MD	Tom Peltier
5-6	How to Develop Information Security Standards and Procedures	Gaithersburg, MD	Tom Peltier
5-6	Intrusion Techniques and Countermeasures	Phoenix, AZ	Rik Farrow
16-17	Practical Forensics: How to Manage IT Investigations	Ontario, Calif.	Peter Garza
18-20	Technical Recovery of Electronic Evidence *(Hands-on)*	Ontario, Calif.	Peter Garza
24-25	Management Skills for a Superior Information Security Program	Cincinnati, OH	John O'Leary
26-27	A Practical Guide to Encryption and Certificate Authorities	Cincinnati, OH	John O'Leary
May			
7-8	Introduction to Computer and Network Security	Orlando, FL	John O'Leary
8-9	Firewalls and VPNs	Valley Forge, PA	Fred Avolio
9-10	How to Manage a Network Vulnerability Assessment	Orlando, FL	John O'Leary
10-11	How to Develop a Winning Security Architecture	Valley Forge, PA	David Lynas
15-16	Windows 2000 Security	Ottawa, Canada	Joel Scambray
17-18	Management Essentials for E-Business Security and Continuity	Ottawa, Canada	John O'Leary
22-23	Management Skills for a Superior Information Security Program	Rockville, MD	John O'Leary
24-25	Facilitated Risk Analysis for Business and Security	Rockville, MD	Tom Peltier
June			
5-6	A 6-Step Framework for Incident Response	Madison, WI	Gene Schultz
7-8	Practical Forensics: How to Manage IT Investigations	Madison, WI	Peter Garza
16-17	Introduction to Computer and Network Security	New Orleans, LA	John O'Leary
16-17	How to Develop Information Security Policies	New Orleans, LA	Tom Peltier
16-17	How to Develop a Winning Security Architecture	New Orleans, LA	David Lynas
16-17	How to Perform a Technical Network Vulnerability Assessment	New Orleans, LA	Justin Peltier
16-17	A 6-Step Framework for Incident Response	New Orleans, LA	Gene Schultz
16-17	Securing E-Business: A Technical Guide to Implementing PKI	New Orleans, LA	Anish Bhimani
18-20	**NetSec 2001**	**New Orleans, LA**	
20-22	3-Day CISSP Prep for Success	New Orleans, LA	Team
21-22	Management Essentials for E-Business Security and Continuity	New Orleans, LA	John O'Leary
21-22	How to Develop Information Security Standards and Procedures	New Orleans, LA	Tom Peltier
June, continued			
21-22	Intrusion Techniques and Countermeasures	New Orleans, LA	Rik Farrow
21-22	Technical Recovery of Electronic Evidence	New Orleans, LA	Peter Garza
21-22	How to Design a Security Architecture for eBusiness	New Orleans, LA	David Lynas
21-22	Windows 2000 Security	New Orleans, LA	Joel Scambray
July			
16-17	Practical Forensics: How to Manage IT Investigations	Ontario, Calif.	Peter Garza
18-20	Technical Recovery of Electronic Evidence *(Hands-on)*	Ontario, Calif.	Peter Garza
August			
7-8	Management Skills for a Superior Information Security Program	Gaithersburg, MD	John O'Leary
9-10	Securing E-Business: A Technical Guide to Implementing PKI	Gaithersburg, MD	Anish Bhimani
27-28	Firewalls and VPNs	Ottawa, Canada	Fred Avolio
29-30	Internet Security Tools and Techniques	Ottawa, Canada	Fred Avolio
September			
17-18	How to Perform a Technical Network Vulnerability Assessment	San Antonio, TX	Justin Peltier
17-18	Facilitated Risk Analysis for Business and Security	San Antonio, TX	Tom Peltier
17-18	Windows 2000 Security	San Antonio, TX	Joel Scambray
19-20	A Practical Guide to Encryption and Certificate Authorities	San Antonio, TX	John O'Leary
19-20	Technical Recovery of Electronic Evidence	San Antonio, TX	Peter Garza
19-20	How to Design a Security Architecture for eBusiness	San Antonio, TX	David Lynas
19-21	3-Day CISSP Prep for Success	San Antonio, TX	Team
25-26	How to Manage a Network Vulnerability Assessment	New York City	John O'Leary
27-28	Management Essentials for E-Business Security and Continuity	New York City	John O'Leary
October			
2-3	Intrusion Techniques and Countermeasures	Phoenix, AZ	Rik Farrow
4-5	Practical Forensics: How to Manage IT Investigations	Phoenix, AZ	Peter Garza
27-28	Introduction to Computer and Network Security	Washington, D.C.	John O'Leary
27-28	Facilitated Risk Analysis for Business and Security	Washington, D.C.	Tom Peltier
27-28	Practical Forensics: How to Manage IT Investigations	Washington, D.C.	Peter Garza
27-28	How to Design a Security Architecture for eBusiness	Washington, D.C.	David Lynas
27-28	How to Perform a Technical Network Vulnerability Assessment	Washington, D.C.	Justin Peltier
27-28	A 6-Step Framework for Incident Response	Washington, D.C.	Gene Schultz
29-31	**28th Annual Computer Security Conference and Exhibition**	**Washington, D.C.**	
31-Nov. 2	3-Day CISSP Prep for Success	Washington, D.C.	Team
November			
1-2	How to Develop Information Security Standards and Procedures	Washington, D.C.	Tom Peltier
1-2	Intrusion Techniques and Countermeasures	Washington, D.C.	Rik Farrow
1-2	Technical Recovery of Electronic Evidence	Washington, D.C.	Peter Garza
1-2	How to Develop a Winning Security Architecture	Washington, D.C.	David Lynas
1-2	Internet Security Tools and Techniques	Washington, D.C.	Fred Avolio
1-2	Windows 2000 Security	Washington, D.C.	Joel Scambray
1-2	Securing E-Business: A Technical Guide to Implementing PKI	Washington, D.C.	Anish Bhimani
12-13	How to Develop Information Security Policies	San Francisco, CA	Tom Peltier
14-15	How to Develop Information Security Standards and Procedures	San Francisco, CA	Tom Peltier
27-28	How to Create & Sustain a Quality Info Security Awareness Program	Gaithersburg, MD	John O'Leary
29-30	A Practical Guide to Encryption and Certificate Authorities	Gaithersburg, MD	John O'Leary
December			
3-4	Practical Forensics: How to Manage IT Investigations	Ontario, Calif.	Peter Garza
5-7	Technical Recovery of Electronic Evidence *(Hands-on)*	Ontario, Calif.	Peter Garza

Welcome

to CSI's Information Security Seminars 2001

Where the industry goes for education

Computer Security Institute

Computer Security Institute is the leading international membership organization dedicated to assisting information security professionals in protecting the information assets of their organizations. Since 1974, CSI has been the world's leading proponent of information security—aggressively advocating the critical importance of protecting information assets. CSI serves thousands of practitioners internationally through seminars, conferences, peer groups, publications, and on-line services. For information on becoming a CSI member, see page 33 or call (415) 947-6320.

CSI has helped grow the careers of information security professionals for over 27 years, training close to 50,000 individuals from major multinational companies and government organizations. While other training organizations limit their training to a few security topics, only CSI offers a complete curriculum of seminars, covering a wide variety of topics and technical levels.

Whether you're new to security or a seasoned practitioner, Computer Security Institute seminars, developed and taught by instructors of unparalleled skill and expertise, provide the highest quality training you'll find anywhere.

CSI's Resources

Here is what we have put together to help you reach your 2001 goals:

- 21 seminars on topics ranging from Intro to PKI to Windows 2000, for a total of 80+ publicly offered seminars, including 8 brand new classes on Forensics, Incident Response, E-Business Security and more.
- **NEW!** Professional certification preparation class to help you become a CISSP.® See pages 18-19.
- On-site training and special projects—Every publicly held CSI seminar in this catalog may be brought on-site to your organization, as well as several additional courses especially popular as private classes. See pages 28-31.
- More from CSI—In addition to seminars, CSI offers a variety of publications, program assessment tools, awareness newsletter, membership benefits and two annual conferences. See pages 32-35.

Sign up now for the seminars that will keep your security program moving forward, using the registration form on page 36, or online at gocsi.com. We look forward to being a part of your success.

Need training for the entire team?

Every class listed in this catalog may be held at your site. Save travel dollars and get the entire team involved—all at the lowest possible cost. For more information, contact Pam Salaway, Manager of Special Projects at (631) 878-2205 or *psalaway@cmp.com*.

Training program assistance

Not sure where to begin or whether a specific class will meet your needs? Call Pam Salaway at (631) 878-2205.

CSI COMPUTER SECURITY INSTITUTE

www.gocsi.com

Graphic design by Coda Creative, Inc., Oakland, CA

Information Security Seminars 2001
Class Schedule by City

register online at www.gocsi.com

Phone 415.947.6320
Fax 415.947.6023
Email csi@cmp.com

Cincinnati, Ohio

April	24-25	Management Skills for a Superior Information Security Program	John O'Leary
April	26-27	A Practical Guide to Encryption and Certificate Authorities	John O'Leary

Gaithersburg, Maryland

February	6-7	Introduction to Computer and Network Security	John O'Leary
February	8-9	How to Manage a Network Vulnerability Assessment	John O'Leary
April	3-4	How to Develop Information Security Policies	Tom Peltier
April	5-6	How to Develop Information Security Standards and Procedures	Tom Peltier
August	7-8	Management Skills for a Superior Information Security Program	John O'Leary
August	9-10	Securing E-Business: A Technical Guide to Implementing PKI	Anish Bhimani
November	27-28	How to Create & Sustain a Quality Info Security Awareness Program	John O'Leary
November	29-30	A Practical Guide to Encryption and Certificate Authorities	John O'Leary

Madison, Wisconsin

June	5-6	A 6-Step Framework for Incident Response	Gene Schultz
June	7-8	Practical Forensics: How to Manage IT Investigations	Peter Garza

Marietta, Georgia

February	13-14	A 6-Step Framework for Incident Response	Gene Schultz
February	13-14	Internet Security Tools and Techniques	Fred Avolio
February	15-16	Practical Forensics: How to Manage IT Investigations	Peter Garza
February	15-16	Intrusion Techniques and Countermeasures	Rik Farrow

New Orleans, Louisiana

June	16-17	Introduction to Computer and Network Security	John O'Leary
June	16-17	How to Develop Information Security Policies	Tom Peltier
June	16-17	How to Develop a Winning Security Architecture	David Lynas
June	16-17	How to Perform a Technical Network Vulnerability Assessment	Justin Peltier
June	16-17	Securing E-Business: A Technical Guide to Implementing PKI	Anish Bhimani
June	16-17	A 6-Step Framework for Incident Response	Gene Schultz
June	**18-20**	**NetSec 2001**	
June	21-22	Management Essentials for E-Business Security and Continuity	John O'Leary
June	21-22	How to Develop Information Security Standards and Procedures	Tom Peltier
June	21-22	Intrusion Techniques and Countermeasures	Rik Farrow
June	21-22	Technical Recovery of Electronic Evidence	Peter Garza
June	21-22	How to Design a Security Architecture for eBusiness	David Lynas
June	21-22	Windows 2000 Security	Joel Scambray
June	20-22	3-Day CISSP Prep for Success	Team

New York City

March	13-14	Securing E-Business: A Technical Guide to Implementing PKI	Anish Bhimani
March	15-16	How to Design a Security Architecture for eBusiness	David Lynas
September	25-26	How to Manage a Network Vulnerability Assessment	John O'Leary
September	27-28	Management Essentials for E-Business Security and Continuity	John O'Leary

Ontario, California

January	22-23	Practical Forensics: How to Manage IT Investigations	Peter Garza
January	24-26	Technical Recovery of Electronic Evidence *(Hands-on)*	Peter Garza
April	16-17	Practical Forensics: How to Manage IT Investigations	Peter Garza
April	18-20	Technical Recovery of Electronic Evidence *(Hands-on)*	Peter Garza
July	16-17	Practical Forensics: How to Manage IT Investigations	Peter Garza
July	18-20	Technical Recovery of Electronic Evidence *(Hands-on)*	Peter Garza
December	3-4	Practical Forensics: How to Manage IT Investigations	Peter Garza
December	5-7	Technical Recovery of Electronic Evidence *(Hands-on)*	Peter Garza

Orlando, Florida

May	7-8	Introduction to Computer and Network Security	John O'Leary
May	9-10	How to Manage a Network Vulnerability Assessment	John O'Leary

Ottawa, Canada

May	15-16	Windows 2000 Security	Joel Scambray
May	17-18	Management Essentials for E-Business Security and Continuity	John O'Leary
August	27-28	Firewalls and VPNs	Fred Avolio
August	29-30	Internet Security Tools and Techniques	Fred Avolio

Phoenix, Arizona

January	30-31	Management Skills for a Superior Information Security Program	John O'Leary
February	1-2	Firewalls and VPNs	Fred Avolio
March	14-16	3-Day CISSP Prep for Success	Team
April	3-4	How to Create & Sustain a Quality Info Security Awareness Program	John O'Leary
April	5-6	Intrusion Techniques and Countermeasures	Rik Farrow
October	2-3	Intrusion Techniques and Countermeasures	Rik Farrow
October	4-5	Practical Forensics: How to Manage IT Investigations	Peter Garza

Rockville, Maryland

May	22-23	Management Skills for a Superior Information Security Program	John O'Leary
May	24-25	Facilitated Risk Analysis for Business and Security	Tom Peltier

San Antonio, Texas

September	17-18	How to Perform a Technical Network Vulnerability Assessment	Justin Peltier
September	17-18	Facilitated Risk Analysis for Business and Security	Tom Peltier
September	17-18	Windows 2000 Security	Joel Scambray
September	19-20	A Practical Guide to Encryption and Certificate Authorities	John O'Leary
September	19-20	Technical Recovery of Electronic Evidence	Peter Garza
September	19-20	How to Design a Security Architecture for eBusiness	David Lynas
September	19-21	3-Day CISSP Prep for Success	Team

San Francisco, California

November	12-13	How to Develop Information Security Policies	Tom Peltier
November	14-15	How to Develop Information Security Standards and Procedures	Tom Peltier

St. Louis, Missouri

March	27-28	Windows 2000 Security	Joel Scambray
March	29-30	How to Manage a Network Vulnerability Assessment	John O'Leary

Valley Forge, Pennsylvania

May	8-9	Firewalls and VPNs	Fred Avolio
May	10-11	How to Develop a Winning Security Architecture	David Lynas

Washington, D.C.

October	27-28	Introduction to Computer and Network Security	John O'Leary
October	27-28	Facilitated Risk Analysis for Business and Security	Tom Peltier
October	27-28	Practical Forensics: How to Manage IT Investigations	Peter Garza
October	27-28	How to Design a Security Architecture for eBusiness	David Lynas
October	27-28	How to Perform a Technical Network Vulnerability Assessment	Justin Peltier
October	27-28	A 6-Step Framework for Incident Response	Gene Schultz
October	**29-31**	**28th Annual Computer Security Conference and Exhibition**	
October	31-Nov. 2	3-Day CISSP Prep for Success	Team
November	1-2	How to Develop Information Security Standards and Procedures	Tom Peltier
November	1-2	Intrusion Techniques and Countermeasures	Rik Farrow
November	1-2	Technical Recovery of Electronic Evidence	Peter Garza
November	1-2	How to Develop a Winning Security Architecture	David Lynas
November	1-2	Internet Security Tools and Techniques	Fred Avolio
November	1-2	Windows 2000 Security	Joel Scambray
November	1-2	Securing E-Business: A Technical Guide to Implementing PKI	Anish Bhimani

Training Schedule by Class
and Table of Contents

register online at
www.gocsi.com

Phone 415.947.6320
Fax 415.947.6023
Email csi@cmp.com

CSI's "Stamp of Excellence" Instructor Team

We take pride in the high caliber of our instructors—they define CSI's training quality and set us apart from the rest. Each class is developed by an expert specializing in a particular security area, be it Internet, Windows, intrusion detection and response, PKI or management—and your seminar will also be taught by that same expert. Class format includes facilitated group discussion as well as lecture, ensuring you receive benefit from the resources of the entire room. Your learning experience is enhanced through the practical knowledge and experience of others who've been there.

Frederick M. Avolio,
President of Avolio Consulting, Inc., has been involved in Internet computing and communication since the early 1980s, working with Internet security systems for over 10 years. He led the team that created the first commercial Internet firewall offering, and helped create the commercial security products division of Trusted Information Systems, enabling a successful public offering and subsequent acquisition.

Areas of expertise include firewalls, intrusion detection, cryptography, security management, and electronic mail systems. He is a top-rated speaker and contributor to CSI, Networld+Interop, USENIX, SANS, TISC, and other security-related forums. Avolio is the co-author, with Paul Vixie, of *Sendmail: Theory and Practice* published by Digital Press.

Anish Bhimani
is Senior Vice President and Chief Technology Officer of Global Integrity Corporation. In this position, he is responsible primarily for the introduction of new technologies into Global Integrity's professional services offerings, as well as the development of new technologies to address the evolving security threat. His primary efforts focus on the deployment of security technology to support electronic business initiatives over the Internet. Prior to joining SAIC, he was the Director of Bellcore's Security and Fraud Reduction Group, responsible for all data communications security consulting performed by Bellcore. Anish is a recognized expert in the area of Internet security and has spoken to numerous industry groups around the world. He is the co-author of the book *Internet Security for Business* and has appeared on *NBC Nightly News* and *Dateline NBC*.

Kevin Brown
is a sixteen-year veteran of the information protection profession and currently Senior Information Security Consultant with Global Integrity Corporation, an SAIC company.

Kevin specializes in assisting organizations in implementing public key infrastructures, including the analysis of specific client E-commerce challenges. Kevin's experience encompasses security architecture and management process design for public key infrastructures including PKI supported web-based enrollment, identity verification, roaming credentials, and digital signing. He built and heads up Global Integrity's PKI lab, which conducts extensive, independent PKI product research and evaluation for Global Integrity clients.

Rik Farrow,
one of CSI's most highly respected technical advisors, is a lively and interesting teacher, who makes difficult topics easier to understand. Through the use of anecdotes and real-life examples, Farrow emphasizes important points, yet provides the technical depth needed by the more experienced attendee. He has been working with the UNIX system since 1982, first managed an IP network in 1986, and has been teaching classes in security since 1987.

Farrow wrote the second book on UNIX system security (Addison-Wesley, 1991), consults, and is a columnist for *Network* and *;login:* magazines. He is an advisor for e-commerce and security companies, and has licensed his Intrusion Techniques and Countermeasures course to an agency of the Department of Defense.

Peter Garza
is the case agent who not only managed but also executed the first ever court-ordered wiretap on an Internet connected network, tracking the activity of Julio Ardita, the Argentine hacker who used Harvard University's network to attack multiple research sites via the Internet. During his ten years as Special Agent for the Naval Criminal Investigative Service, Peter's experience in gathering electronic evidence for federal law enforcement has ranged from the reconstruction of accounting systems in large procurement fraud cases, to forensics in both target and hacker computer environments.

Peter has leveraged his work in federal law enforcement by founding Evidentdata, Inc., a computer forensics and incident response consulting firm located in Rancho Cucamonga, California.

"Mr. O'Leary's enthusiasm is contagious. Could have been a 'dry' subject but instead it was very interesting and helpful."

– Ray Baumlerr,
Systems Security Officer,
U.S. DHHS / SAMHSA

"Instructor was very knowledgeable and motivating. Gave great examples and real-life situations to help class relate. Did wonderful job of demonstrating how to apply concepts to your individual organization."

– Samantha Peebles
Security Consultant, SNCG

David Lynas, CISSP

is Director of Professional Relations, Global Security Practice, Netigy Corporation. He is an internationally renowned information security consultant with nearly twenty years practical experience.

In high demand as a presenter all over the world, David has presented more than thirty sessions to major international conferences since 1996, has chaired tracks on Security Strategy and Network Security at COMPSEC in London, and is Founder and Chairman of COSAC, the Irish International Conference on Computer Security, Audit & Control.

In recent years David has specialized in designing and implementing business driven security strategies and complex technical security architectures for an extensive list of blue chip clients and Federal Government agencies.

John O'Leary, CISSP

is the director of education for Computer Security Institute. His background spans three decades as an active practitioner in information systems security and contingency planning.

Mr. O'Leary has designed, implemented and managed security and recovery plans for networks ranging from single site to multinational. His extensive knowledge of the subject matter combined with an engaging and entertaining teaching style have won John acclaim as CSI's all-time highest-rated and most requested instructor. O'Leary has trained thousands of practitioners, regularly conducts on-site programs at major corporations and government facilities worldwide, and facilitates all meetings of CSI's Working Peer Groups, where fifty security professionals share best practices.

Justin Peltier, CISSP, MCNE, MCP, CCSE, RHCE, CCNA

Justin's years of experience have been dedicated to planning, designing, and implementing technical security solutions in a wide range of operating environments including Novell, NT, Sun Solaris, LINUX, and Netscape systems, as well as with Ethernet, Token Ring, TCP/IP, and IPX/SPX topologies and protocols. He currently serves as Chief Technical Engineer for Netigy and is the company's primary technical instructor in the areas of vulnerability assessment, risk analysis, virtual private networking, policies and procedures, and penetration testing. Previously, he served as Director of Security for Ideal Technology Solutions, responsible for network consulting and support nationwide for clients such as Detroit-Edison, Rockwell International, and Stroh's.

Tom Peltier, CISSP

is currently Director of Methods and Administration for the Netigy Corporation's Global Security Practice. Previously, he was National Director for Consulting Services for CyberSafe, Corporate Information Protection Coordinator for Detroit Edison, and Information Security Specialist for General Motors.

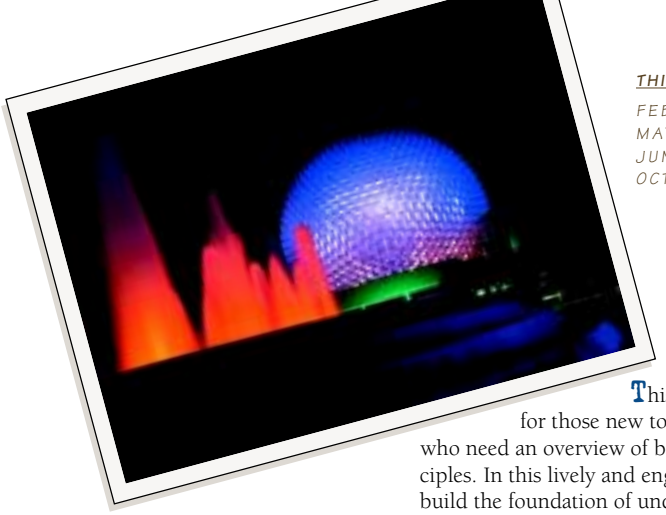
Tom has received the 1999 ISSA's Individual Contribution to the Profession Award, the Computer Security Institute Lifetime Achievement Award and CSI's Information Security Program of the Year Award. He conducts numerous seminars and workshops on various security topics and has led seminars for CSI, Crisis Management, American Institute of Banking, the American Institute of Certified Public Accountants, Institute of Internal Auditors and ISACA.

Joel Scambray, CISSP, CCSE

is a co-author of *Hacking Exposed (www.hackingexposed.com)*, the international best-selling Internet security text recently updated with a Second Edition. Joel also writes the monthly *Ask Us About Security* forum for Microsoft's TechNet website, and co-authors the weekly *Security Watch* column at *InfoWorld Magazine*. Joel's published work draws primarily on his experiences as an IT security consultant for clients ranging from members of the Fortune 50 to newly minted startups. He is currently Managing Principal with Foundstone Inc. *(http://www.foundstone.com)*, and previously held positions as a Manager for a BigX consulting firm, Senior Test Center Analyst for InfoWorld, and Director of IT for a major commercial real estate firm. Joel is a Certified Information Systems Security Professional (CISSP) and Certified Checkpoint Security Engineer (CCSE).

Dr. Eugene Schultz, CISSP

is the Research Director and a Trusted Security Advisor for Global Integrity Corporation. In this role, he conducts research and consulting activities in addition to providing strategic guidance to corporate clients. He also concurrently serves as an Adjunct Professor of Computer Science at Purdue University. An expert in Windows NT, UNIX, and network security, Dr. Schultz has also provided expert testimony for both the U.S. Senate and the House of Representatives and served as an expert witness in court cases. He has co-authored two books (*UNIX: Its Use, Control and Audit* and *Internet Security for Business*), sole-authored one (*Windows NT Network Security*), and published over 90 articles. He has presented over 140 talks, including numerous keynote addresses, at a variety of conferences throughout the world.



THIS CLASS OFFERED:

FEB.	6-7	GAITHERSBURG, MD
MAY	7-8	ORLANDO, FL
JUNE	16-17	NEW ORLEANS, LA
OCT.	27-28	WASHINGTON, D.C.

You Will Learn:

- *Common threats to information assets*
- *What to look for in an intrusion detection product*
- *The importance of a security awareness program*
- *Security issues and vulnerabilities associated with your organization's use of the Internet*

You Will Leave With:

- *A solid foundation in concepts of IS security*
- *Resources for future help with Internet security*
- *Understanding of countermeasures to network vulnerabilities that will work in your particular environment*

This course is designed for those new to security or for those who need an overview of basic security principles. In this lively and engaging seminar we'll build the foundation of understanding you need to secure the networked systems of today and tomorrow, relating information systems security goals and objectives to organizational mission performance. You will gain a solid understanding of the fundamentals of security and the entire range of issues that an accomplished practitioner must address, and return with suggestions and ideas that can be used now to augment the security of all your systems.

Day One

Reasons for Concern — We'll analyze the conflicting priorities and business environment factors that have brought security concerns to the forefront of management attention and look at the ever-growing extent of organizational reliance on computer systems and networks. Learn what other factors are driving the need for better security of systems and information.

Relation to Mission Performance — We'll examine the relationship between productivity and security, identifying sources of error and penetration threats. You'll learn computer security principles and ways of addressing exposures that tie to organizational culture

Program Organization —You'll learn the elements of an effective security program and see how they fit together. See how policies and procedures act as the foundation for a program and show management's support. Tie security planning to organizational goals and objectives. We'll examine how risk analysis, training and awareness, audit and monitoring, and handling incidents relate to each other in an effective program. Pin down responsibilities for security throughout the organization.

Jargon and Terminology — You'll learn the terminology used in general information systems security, encryption and network security, with an eye toward understanding the underlying principles and technology. We'll use state-of-the-art technology — the flipchart — to simplify and amplify explanations in this section.

Day Two

Network Security — We'll start by identifying the unique security challenges of networked systems, defining the three basic goals of network security and how to achieve them. What are the major vulnerabilities in your current networks and what are the countermeasures you can take to successfully combat them? You'll also learn how to identify areas of future concern

Internet Security — We examine the Internet from a security perspective. Is there any inherent protection? What are the primary threats? Learn about firewalls, what they are, why they are necessary but not sufficient for the protection of valuable resources. We'll look at ways to effectively control inbound and outbound traffic on the Net. We'll identify resources to help you with Internet security, and explain why most security problems on the Internet are not really Internet problems.

Intrusion Detection —Analyze some high-profile incidents to help identify different types of attack that you must defend against. You'll learn how to detect trouble and what to look for in an intrusion detection product.

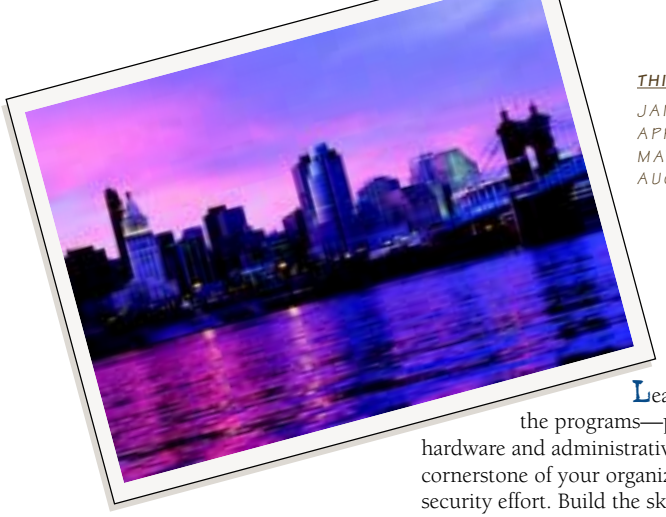
Personnel Security — Learn the value of background checks and the necessity of linking with the Human Resources section. Understand why violations of security rules must be dealt with quickly and consistently, consequences and possible punishments. Determine proper procedures for information security in the event of personnel terminations.

Introduction to Computer and Network Security

John O'Leary

"Most knowledgeable instructor I have been instructed by in all the computer courses I have taken. He speaks with such enthusiasm you know he loves his job. As a student this was refreshing to see."

- Gord Antle
Security Analist, TSE



THIS CLASS OFFERED:

JAN.	30-31	PHOENIX, AZ
APR.	24-25	CINCINNATI, OH
MAY	22-23	ROCKVILLE, MD
AUG.	7-8	GAITHERSBURG, MD

You Will Learn How To:

- *Identify key projects to implement in order to "raise the bar" for the security function at your organization*
- *Develop and fine-tune a security policy statement*
- *Raise the level of security awareness throughout your organization*
- *Interface more effectively with internal groups whose support and commitment you need*
- *Deliver planned objectives, building your credibility and track record*
- *Recognize pitfalls to avoid—and how to cope if you don't*

John O'Leary facilitates quarterly confidential dialogues with more than fifty information security professionals from leading U.S. companies via CSI's Peer Group meetings. If you can't join a Peer Group, attending this course will be the next best thing, where John shares the combined wisdom of his own experience as well as that of your peers. This course picks up where textbook knowledge stops short: it teaches you about how to get the job done and what's working for others!

Learn how to develop the programs—physical, software, hardware and administrative—that will be the cornerstone of your organization's information security effort. Build the skills to develop these crucial programs, whether you're creating them from the ground up, or administering or improving programs already in place.

In this workshop, we'll outline the key skills you need to perform the crucial multi-disciplinary job of Information Security Professional (ISP) effectively and show you how to acquire and enhance them. We'll emphasize the need for continuous learning as the environment rapidly changes.

Day One

Organization of the Security Function — Start by identifying the commonalities and differences in real-life ISP job descriptions. What are the key security responsibilities of the ISP? Take a look at the ISP function from the point of view of other organizational departments, and understand how other groups' perceptions of the security function affect your ability to get the job done. Learn the pros and cons of placing the security function at various organizational levels, and how organizational placement can increase—or hinder—effectiveness.

Required Skills for ISPs — Learn which skills are most necessary and valuable for an ISP and how you can develop them. Identify sources of information to help build those skills, and evaluate the long-range career opportunities. Learn why this position emphasizes managerial, rather than technical skills, and how effectively written communication can make or break the security program. Here, we'll also cover specialized terminology you should know for systems and network security, contingency planning and encryption.

Staffing the Function — One of the major challenges of managing an IS security function today is finding enough qualified, motivated people to handle the array of tasks. We'll analyze the advantages and disadvantages of different backgrounds for the IS security job and cite some successes and failures in bringing people into this discipline. The expansion in scope and size of the function has driven many organizations to consider outsourcing as a solution. Investigate what security tasks can reasonably be outsourced for your organization.

Day Two

ISP Responsibilities — Compare the steps different organizations have taken in building their security programs. Learn which steps from which methods would work for you. Find out why appropriate, well-crafted policies, standards and procedures build the foundation for an entire security program and why security awareness is such a vital element. Learn the components of a risk analysis and the difference between a qualitative and a quantitative risk assessment. Identify the three components of computer viruses; how they work and what you can do to protect your organization. Determine whether the information classification scheme in use at your shop is realistic and discuss the renewed emphasis on physical security in times of multi-gigabyte storage on palmtop devices with wireless Internet connection. Examine the three phases of activity for a business continuity plan and learn effective ways of building and testing a plan including critical parts of the client/server environment.

Managing Security —Learn strategies for managing data security successfully: how to obtain support and commitment from all levels of the organization. Identify the organizational interfaces you need to build and nurture to be effective. Select strategies for goal setting and determining priorities that will help support the mission of your organization. Investigate ways to measure your progress, pitfalls associated with the ISP function and how to avoid them; and keys to the effectiveness of your program and your performance as a security professional.

Management Skills for a Superior Information Security Program

John O'Leary

Formerly titled "How to Become an Effective Information Security Professional"

"Excellent session. If John hasn't already written the book on his material, he should."

– Ted Lyman
ISO, College of William and Mary

THIS CLASS OFFERED:

APRIL	3-4	GAITHERSBURG, MD
JUNE	16-17	NEW ORLEANS, LA
NOV.	12-13	SAN FRANCISCO, CA

You Will Learn How To

- *Create an information security policy*
- *Establish a supporting mission statement*
- *Identify the key elements of an information security policy*
- *Win management support and approval*
- *Establish a supporting review team*

You Will Leave With:

- *The ability to critique existing policies*
- *An initial draft policy for information security*
- *A project plan outline for policy development*
- *A number of checklists and document examples*

See also "How to Develop Security Standards and Procedures" (page 9) — an excellent follow-up course.

Implementing the controls required to meet business objectives can be a seemingly overwhelming task. First you must lay the cornerstone of your information protection program: a set of concise, effective information security policies and procedures that, together, will serve as the foundation for all future implementation of controls.

During this two-day, working seminar, we will examine how to tie security goals to the business objectives. We will review the key elements that form the foundation of an effective set of policies and procedures. We will critique examples of existing information security policies and identify pitfalls to avoid. To ensure that this seminar is a true learning experience, the instructor will lead a number of facilitated exercises that will allow the attendees to draft an initial information protection policy statement, an information security mission statement, and an information security procedure table of contents. We will also explore the creation of a review panel for the documents and how to obtain management support for the completed documents.

Day One

Getting Started – The development of enterprise-wide policies and procedures should be managed as any project. We will examine each of the phases of a typical project development life cycle (analysis, construction, test, production and maintenance) and what the deliverables are for this project. We will identify where to obtain the background information needed to begin the project. Finally, we will establish definitions of policy, procedure, standard, guideline and regulation.

Project Scope Management – We'll examine how to ensure that the policy and/or procedure development project includes all the work required, and only the work required, to complete this specific project. We will review the contents of project scope statements and then the attendees will assemble into their groups and create a scope statement for their project. When the drafts are completed, the group will critique each of the scope statements.

Policy Statement Development – We will examine the key components of an effective policy statement and identify key pitfalls to be on the alert for. Using a policy development checklist, we will examine existing policy statements and critique them for effectiveness. Using the information presented, the attendees will form work groups and will draft an information protection policy that will be critiqued by the other groups.

Day Two

Information Security Policy – Using industry accepted standards, we will identify what key items should be included in an information security policy statement. We will address the enterprise's definition of information security; management's intentions; explanation of requirements and laws; definition of general and specific goals; and the process for reporting security incidents.

Establishing Review Teams – Since every document that is published will have to be reviewed for form and content, we will examine the methods used to get the document you create reviewed, readable and ready for publication. We will explore the concept of a core team and a support team, identifying common problem areas to avoid.

Gaining Senior Management Support – Even though one group of senior management has been charged with implementing the information security policies and procedure document, much of senior and middle management may be unaware of this mandate. We will identify key elements in making your document marketable to this group of management and to the employees at large.

How to Develop Information Security Policies

Tom Peltier

"Tom has an uncanny way of making you see the light."

– Donald L. LaBarre, Jr.
Data Security Analyst,
State of Connecticut DMHAS

THIS CLASS OFFERED:

APRIL	5-6	GAITHERSBURG, MD
JUNE	21-22	NEW ORLEANS, LA
NOV.	1-2	WASHINGTON, D.C.
NOV.	14-15	SAN FRANCISCO, CA

You Will Learn How To:

- *Create an information security standards document*
- *Develop procedures*
- *Identify the contents of a procedure document*
- *Use subject matter experts to your advantage*
- *Establish a supporting review team*

You'll Take Back With You:

- *Draft information standards and procedures*
- *A table of contents for the procedures documents*
- *A number of checklists and document examples*

This course is intended for those who have working policies in place or who have already taken "How to Develop Information Security Policies" (page 8).

During this two-day, working seminar, we will examine how to write effective supporting standards and how to tie them to the policy statement. By ensuring that business objectives or the enterprise's mission is met, the standards will have a better chance of being accepted and implemented.

Procedures are as unique as the organization; there is no generally accepted standard for the proper way to write a procedure. The look of your procedures is determined by what will work best to provide the target audience with what they need. In this session we will examine a number of different procedure styles—what they look like and how they are used.

Day One

Introduction — We will discuss the common definitions for *policy, standard, procedure and guideline.* As a team we will determine which definition meets our general needs and how to alter the definition to meet the specific needs of our organizations. The class will divide into teams and participate in an exercise to reinforce concepts discussed. We will also look at common pitfalls to avoid and what makes up an effective standards statement.

Standards — The are many existing sources for supporting standards. Both the banking and the healthcare industries have standards that have been established by regulations or requirements from the federal government. We will explore where to find industry-specific standards and how to make them apply to your organization.

Procedure Style — There are perhaps as many as ten different styles of procedures, each having its advantages and disadvantages. We will examine three of the most popular forms of procedures and will identify the positives as well as any shortcomings, of each. Among those presented will be *narrative, flow chart and playscript.*

Day Two

Procedure Table of Contents — Since most employees will not read the procedures cover-to-cover, it is the table of contents that will be most used in the procedure document. Using a facilitated approach, we will identify the contents that could be part of an information security procedure document. We will then review the typical procedure structure and define the terms *topic, section and subject.* Using this information, each of the groups will work to put the contents of the facilitated session into a logical sequence.

Techniques on Writing Procedures — After presenting the "do's and don'ts" of procedure writing, we will review the actual method for writing procedures effectively. A procedure is the step-by-step process that an employee will use in order to complete a specific task. In order to write a procedure, then, it will be necessary to have a strong understanding of the task at hand. Very few of us have a sufficient level of knowledge for every subject, therefore, it will be necessary for us to seek out subject matter experts (SME) to help in the development of procedures. We will examine the process used to get SMEs involved in the procedure development process.

Gaining Support — Even though one group of senior management has been charged with implementing the information security procedures document, much of senior and middle management may be unaware of this mandate. We will identify key elements in making your document marketable to this group of management and to the employees at large.

How to Develop Security Standards and Procedures

Tom Peltier

"Tom is a great instructor! Very enthusiastic. Lots of interesting stories that related. Makes computer topics and learning fun."

- Carla Cameron
Security Analyst Trainee,
Transamerica Distribution Finance

THIS CLASS OFFERED:

MAY	24-25	ROCKVILLE, MD
SEPT.	17-18	SAN ANTONIO, TX
OCT.	27-28	WASHINGTON, D.C.

You Will Learn How To:

- *Evaluate tangible and intangible risks*
- *Use the qualitative risk analysis process*
- *Identify elements that make up a strong BIA*
- *Conduct risk analysis with confidence*

You Will Leave With:

- *A process to pre-screen applications and systems for quicker risk analysis*
- *A customized business impact analysis methodology*
- *A set of standard controls to be used in your risk process*
- *A set of EXCEL spread sheets containing the basic documents*
- *A thorough understanding of the risk management process*

By implementing an effective risk management program, many organizations have progressed to view security and controls as business enablers. Security is now being viewed as a component of the business operations by creating opportunities to use information technology in ways that would not otherwise be feasible. This workshop will address risk management principles that have been implemented by business, industry, private companies, utilities and government, examining how to link these principles to the business objectives or mission of your organization. After completing this course, you will be prepared to implement a business-orientated risk management program.

Risk Analysis Basics – Every risk analysis methodology uses the same basic process. We will briefly examine the standard methodology and will assist you in internalizing the methodology for your own organization.

Qualitative Risk Analysis – You will learn this method of systematic examination of assets, threats, and vulnerabilities that establishes the probabilities of threats occurring, the cost of losses if they do occur, and the value of the safeguards or countermeasures designed to reduce the threats and vulnerabilities to an acceptable level.

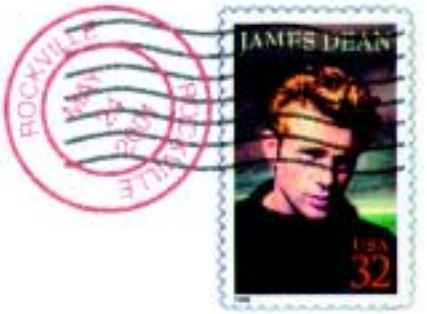
Qualitative Methods – To reinforce the qualitative process, we will examine and work a number of practical applications of this methodology. Included in this process will be a vulnerability analysis, hazard impact analysis, scenario analysis, threat analysis and questionnaires.

Developing a Pre-Screening Process – By conducting a quick review of the application, system or other subject, the organization can determine where to expend its limited resources. You will be shown examples of pre-screening methods and how they are used in different organizations. Breaking into groups, you'll then develop a pre-screening process for your own organization.

Facilitated Risk Analysis Process (FRAP) – Using the qualitative approach and the results from the pre-screening, we will examine the most popularly used method of risk analysis in use today. The Facilitated Risk Analysis Process (FRAP) will be reviewed and you'll conduct your own case study FRAP. Each attendee will examine and critique the process and the instructor will assist in customizing it for your own organization.

Customizing a Business Impact Analysis for Your Organization – Using all of the techniques discussed, attendees will study a facilitated process to review the impact on customer business process if that resource becomes unavailable. The BIA is used by organizations to determine critical resources. Once the critical resources are scored, the organization can then identify appropriate controls to ensure the business continues to meet its business objectives or mission. Attendees will then break into groups and develop a BIA to meet their organization's needs.

Using Qualitative Risk Analysis in Information Classification Methodology – We will examine the four essential aspects of information classification: (1) information classification from a legal standpoint, (2) responsibility for care and control of information, (3) integrity of the information, and (4) the criticality of the information and systems processing the information. Attendees will review examples of the existing classification policies and then review two methodologies to assist the user community in classifying the information under their control.

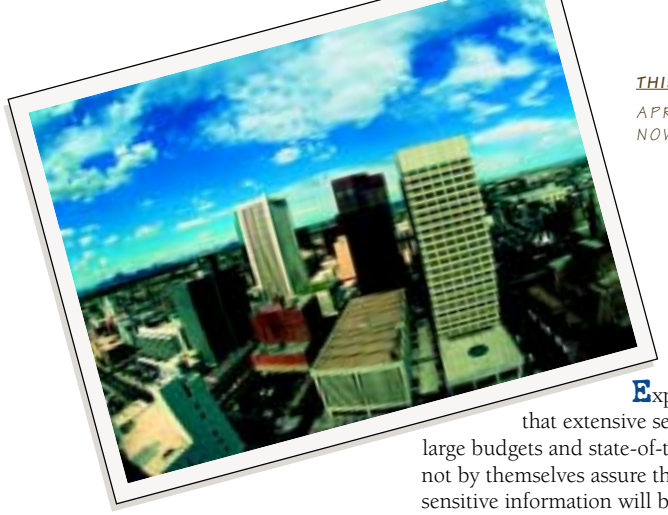


Facilitated Risk Analysis for Business and Security

Tom Peltier

"Excellent seminar and instructor. I now know how to begin the process and I have a method I can directly apply to my work environment."

– Steve Caunter
Chief, IT Client Services, PMRA



THIS CLASS OFFERED:

APR. 3-4 PHOENIX, AZ
NOV. 27-28 GAITHERSBURG, MD

You Will Learn How To:

- *Identify the key ingredients in a successful security training and awareness program*
- *Define, segment and target key employee groups within your organization*
- *Gather and organize a wide variety of training techniques and materials for maximum impact*
- *Evaluate the results of your security awareness training*

You Will Leave With:

- *A tailored individually developed plan for building security awareness at your organization*
- *17-page actual case study of a security awareness program developed by one organization after taking this class*
- *A resource list of sources for security awareness materials and information*

Experience has shown that extensive security programs with large budgets and state-of-the-art technology will not by themselves assure that valuable and sensitive information will be protected. Since most data processing errors are caused by well-intentioned but careless employees and most computer crime is committed by authorized users, employee attitudes and motivations must be a critical concern of all security programs.

Learn how to build security awareness in all employees from the executive offices to the janitorial staff. Receive practical ideas and techniques for delivering security training, customized according to your audience. Find out how to plan and execute a program that's right for your specific organizational environment and budget.

Day One

An Awareness Program is Crucial — Analyze the benefits of a security awareness program—and the pitfalls of not having one. Receive strategies and tips on how to sensitize employees to appreciate the importance of protecting information resources, and how to deliver the security message to those hardest to reach.

Security Training Team — Learn the benefits of the team approach, how large this team should be, which functional areas should be represented, and who, specifically, should be on it. Identify the key players, as well as the peripheral people needed to ensure an effective effort.

Target Population — Look at techniques for segmenting your audience into homogeneous and manageable groups. Then discuss the tools needed to determine the level of current security awareness for each group, including "walk around" inspections.

Training Implementation — Discover what type of information to gather and present, how to organize your presentation for maximum impact and which meeting techniques are most effective. Learn how to develop an approach that's on target for each audience segment, including what topics to cover and at what level of depth.

Day Two

Training Objectives — How should the target audience "change their ways" as a result of the security awareness program? Examine the techniques for identifying and measuring this change. Learn the best ways to make sure the program is genuinely working and how to justify its continued existence to top management.

Information Sources — Discover the excellent educational materials that are currently available from sources that include the federal government, professional organizations, trade publications and more. Learn how and where you can acquire materials.

Training Techniques — Analyze in detail a wide range of awareness techniques, including formal courses, informal briefings, on-the-job guidance, in-house publications, self instruction and videos. Consider the pros and cons of each and discuss when each is most appropriate.

The course is structured so that when you're done you'll have a security awareness plan tailored for your organization's specific needs ready to bring back and use on the job. A case study is included from one organization who took this class and followed through on its plan.

How to Create and Sustain a Quality Security Awareness Program

John O'Leary

"Really great course - the interactive discussion was KEY! And John is awesome."

– Hillary Elizabeth Winiarz
CIO IT Security, Anderson Consulting

THIS CLASS OFFERED:

FEB. 8-9	GAITHERSBURG, MD
MAR. 29-30	ST. LOUIS, MO
MAY 9-10	ORLANDO, FL
SEPT. 25-26	NEW YORK CITY

You Will Learn How To:

- *Identify current network security concerns*
- *Conduct a thorough network vulnerability assessment*
- *Determine what tools will be necessary to conduct the assessment*
- *Use your findings to support organization needs*

You Will Leave With:

- *A checklist of network security concerns*
- *An assessment report outline*
- *An understanding of the network assessment process*

See also "How to Perform a Technical Network Vulnerability Assessment" (page 22).

One dangerous tendency often seen in those charged with protecting networks is to leap into the procurement and installation of sophisticated, costly and cumbersome "solutions" that might actually have a negative impact on organizational productivity. Before implementing expensive barriers to protect the network, the wise security professional conducts a network vulnerability assessment to make sure that the right things are being protected in the right way.

This course analyzes the makeup of a successful Network Security Assessment project. An effective assessment will evaluate the risks associated with *your specific operating environment.* The process must include identifying risks associated with the current environment as it is and as it will evolve. It requires an evaluation of existing control measures and recommendations for improving the protection of your organization's network. We'll also explore administrative elements of an assessment, such as who should be a part of the team and what should be included in the assessment report.

Day One

Assessing Network Concerns — We will examine current trends in network incidents with an eye toward predicting the future, working an exercise to identify and rank your organizations' network concerns.

Examining the Network Configuration — We will concentrate on assessing the network as a discrete entity as well as analyzing the security needs and peculiarities of individual components. We will discuss how to leverage the work of other employees and get them to run tools to examine the security of network devices (routers, bridges, gateways, hosts, servers, and cabling).

Critiquing Policies — Securing your organization's network begins with a security policy that articulates procedures for protecting information and network assets in accordance with your business goals, good business practices, commonly-accepted security practices, and outside regulatory requirements. To reinforce the material, attendees will develop and critique a network security policy.

Day Two

Developing a Tailored Network Security Checklist — Starting with some industry-accepted standards and adding a dash of your own relevant experiences, we will identify and discuss elements expected to be found in a secure network environment. Based on the discussions and the material, we will develop an initial network security checklist.

Intrusion Detection and Security Assessment Software: Myths and Reality — Using a five-dimensional model we will see how to categorize an attack on a network by placing it into one or more classes in each dimension. Our discussions will also cover the three phases of an attack and what products can be used to help identify an attacker.

Tools of the Trade — Saving precious staff time with tools and appropriate automation is an excellent way to magnify staff capabilities. The first step here is to identify where tools are needed and the potential problems involved with their implementation. We will examine what to look for in effective security assessment tools, where to get them as cheaply as possible and how to implement them with the least perturbation.

Typical Vulnerability Report — The end deliverable from your network vulnerability assessment will be a published report. We will examine what elements make up an effective report document, how to use the document to meet your objectives, and how the report can be used by management to show that they are meeting their "duty of care" requirements.

How to Manage a Network Vulnerability Assessment

John O'Leary

"Very informative course, good opportunity for networking, a lot of valuable take backs."

– Keith Broad,
Team leader, IT Security Union Gas

THIS CLASS OFFERED:

JAN.	22-23	ONTARIO, CALIFORNIA
FEB.	15-16	MARIETTA, GA
APR.	16-17	ONTARIO, CALIFORNIA
JUNE	7-8	MADISON, WI
JULY	16-17	ONTARIO, CALIFORNIA
OCT.	4-5	PHOENIX, AZ
OCT.	27-28	WASHINGTON, D.C.
DEC.	3-4	ONTARIO, CALIFORNIA

Resources you'll leave with:

- *Interactive list of relevant WWW sites*
- *CD-ROM containing:*
  - *demo/shareware/freeware tools*
  - *exemplar documents of reports, chain of custody, evidence label*
  - *guidelines and other forms*
- *Other resources for IT investigators*

See also "Technical Recovery of Electronic Evidence" (page 28).

Today's technology driven economy has greatly impacted the role of information security professionals, who are now expected to assist in diminishing the financial liabilities, both corporate and management's own personal liability, tied to the spectrum of electronic abuse scenarios—whether by outsiders, employees, business partners or competitors

This course will teach IT and information security professionals how to effectively manage a forensics investigation, whether the goal of that investigation is to avoid litigation through carefully crafted employee administrative action or to cooperate with law enforcement on a civil case surrounding a computer crime.

A well managed investigation begins with a sound understanding of the forensic principles used in gathering technical evidence, since all incidents will potentially involve the collection of electronic evidence. Although others will most likely run the tools that accomplish the task, awareness of forensic principles will help ensure that information is collected in a manner that will guarantee its usefulness in taking administrative action, litigation, or referral to law enforcement. We will explore case studies of recent and past investigations in order to illustrate key teaching points: response to employee misconduct, insider attacks, hacker attacks on your network, or the theft of intellectual property. From interviewing and report writing techniques to subpoenas and seizure orders, this course will explore and expand upon all areas of the forensic investigation process.

Course Content:

- How computer forensics can be a tool for decision makers and legal counsel
- Electronic records discovery – both sides of the fence
- Effective strategies in the collection of electronic evidence
- Investigative issues for computer subpoenas and seizure orders
- Skills the technical investigator must have
- Forensic techniques in a heterogeneous computing environment – palmtops to servers
- Network forensics – a systems approach to computer forensics
- Experience-based case studies involving the recovery of digital evidence
- Analysis strategies in the review of acquired electronic evidence
- Evaluating and presenting recovered remnant or residual data
- Practical technical report writing (based on real experience with senior executives in private and judicial organizations)
- Free stuff – overview of free, almost free, and demos of tools you can use to begin forensic analysis of electronic evidence
- You get what you pay for…demo of valuable forensic software tools
- Technical interviews – more than "just the facts"
- Evidence documentation and processing
- Internet defamation cases – tracing words on the Web
- An insider's view of several prominent intrusion cases
- Lessons learned - strategies for dealing with unexpected situations in the field
- Policy issues
  - electronic records retention policy
  - HR issues (monitoring, searching)
  - dealing with law enforcement

Practical Forensics: How to Manage IT Investigations

Peter Garza

This course covers a combination of technical, procedural, and managerial information and is thus appropriate for both technical and non-technical attendees, and a must for those who are involved in planning and implementing an incident response capability.

THIS CLASS OFFERED:

FEB.	13-14	MARIETTA, GA
JUNE	5-6	MADISON, WI
JUNE	16-17	NEW ORLEANS, LA
OCT.	27-28	WASHINGTON, D.C.

Systems, applications and networks have become more complex and diverse and are thus increasingly difficult to defend. Seventy percent of all respondents to the 2000 CSI/FBI Computer Crime Survey reported experiencing at least one significant security-related incident. While prevention and avoidance are certainly our preference, the realities of this challenge dictate that organizations be prepared to respond to incidents in a way that will best mitigate risk.

We define an incident as *an adverse event in a computer system and/or network; or the threat of an adverse event.* This two-day course explores the many types of incidents: intrusions (comprising a minority of incidents), denial of service attacks, malicious code, extortion, hoaxes, embezzlement and fraud, and integrity attacks—and the complications of dealing with each type of incident.

Incidents almost invariably follow a predictable cycle; we will explore the six stages and present a framework for incident response that is based on this incident lifecycle process, from preparation through follow-up. Attendees will learn strategies for gaining support from management, funding groups and business units and considerations involved in forming and managing an effective incident response capability.

The instructor will draw on a multitude of case studies from his experience as founder and manager of the U.S. Department of Energy's Computer Incident Advisory Capability (CIAC). Students will work several practical exercises, including writing incident response procedures and planning the proper use of deception servers (honeypots) for their site.

Course Content

- Introduction to incident response
- Risk analysis — using results to gauge your efforts
- 6-Step framework for incident response
- Types of incidents (intrusions, denial of service, malicious code, extortion, hoaxes, embezzlement and fraud, integrity attacks)
- Tracing network intrusions
- Forensics and legal issues
- Designing and deploying deception servers (honeypots)
- Responding to insider attacks
- How to form and manage an incident response team
- Future directions

Student Exercises

- How to write incident response procedures
- How to design and deploy deception servers (honeypots)

A 6-Step Framework for Incident Response

Gene Schultz

THIS CLASS OFFERED:

FEB.	15-16	MARIETTA, GA
APR.	5-6	PHOENIX, AZ
JUNE	21-22	NEW ORLEANS, LA
OCT.	2-3	PHOENIX, AZ
NOV.	1-2	WASHINGTON, D.C.

You Will Learn:

- *Scanning techniques including DNS, ping, fping, nmap, mscan, sscan, strobe, stealthy scans, ftp-bounce, nc, NAT10, SNMP*
- *Exploit tools, such as sniffit, l0phtcrack, hackdll, getadmin, sun-loadmodule, ttjamsession, linux-abuser, iishack.asm*
- *Denial of service attacks, for example: smurf, Teardrop, Boink, the UDP bomb, and Winnuke.*
- *Tools for hiding intrusions, such as rootkits, z2, fix, bindshell, pinsh, relays, tunnels, eggdrop, and Trojan horses*
- *Countermeasures, including firewalls, encryption, IDS systems, system hardening*
- *Security features of UNIX and NT operating systems*
- *TCP/IP implementation details sufficient for understanding probes, attacks, and countermeasures*

You Will Leave With:

- *Resources for finding new attacks*
- *Techniques for monitoring networks and systems*
- *Methods for restoring compromised systems*
- *Comprehensive understanding of probes and attacks, and the tracks they leave behind*

Even as the number of security products increases, defenders remain woefully clueless about how hackers operate, whether adolescent hobbyists or international terrorists. Defenders know less about how their computers and networks are attacked than do the attackers. The primary reason for this has to do with the limited resources of the defenders, compared to those of the legions of attackers.

This course helps to even up the playing field by describing in detail intrusion techniques. Attackers have a wide range of motivations, from the casual cracker to the dedicated spy, and this affects their styles of attacks. Depending on the style, an attacker may scan blindly for interesting targets, or probe carefully and surreptitiously for weaknesses in a particular network. The serious attacker will cover his or her tracks by relaying IP connections through intermediate sites, making backtracing the attacker extremely difficult.

This course focuses on remote probes and attacks accomplished over network links. The first step in most exploits is to gain interactive access to the target. Through the use of numerous example exploits, the course participant will learn how to use probing and exploit tools found on the Internet. Some tools not in wide distribution will also be described and demonstrated where possible. Hacker tools used to hide evidence, edit logs, and disguise tools will be explained, as well as techniques for discovering when logs have been modified and finding Trojan horses.

Current countermeasures against attacks include firewalls and Intrusion Detection Systems. But in many cases, firewalls are poorly configured, or the product chosen does not match the security requirements. IDS systems come in many types, and each has its strong and weak points.

Other countermeasures require a dedicated security group which understands the nature of attacks and appropriate defenses. The ability to monitor network activity in realtime, capture an attacker's keystrokes, shut down the attack, and trace the attacker to his or her source are critical to protecting network security.

This course also covers enough information about how TCP/IP works so that attacks that rely on TCP/IP can be readily understood. Where necessary, security features of UNIX and NT systems will also be discussed, so that workings of exploits will make sense to participants.

Audience

Intermediate to advanced, UNIX and NT system and network administrators, incident handling team members, information security and audit professionals, IP network managers.

This course was selected by the U.S. National Security Agency as the foundation for establishing their own internal training program on defensive techniques for network intrusions.

Intrusion Techniques and Countermeasures

Rik Farrow

"Excellent instructor with a high ability to transmit information."

- Theo Kaelyn
Chief Info Security Officer,
Qantas Services

THIS CLASS OFFERED:

FEB.	1-2	PHOENIX, AZ
MAY	8-9	VALLEY FORGE, PA
AUG.	27-28	OTTAWA, CANADA

You will Learn:

- *The different types of firewalls, their strengths and weaknesses.*
- *VPNs and VPN standards*
- *What strong user authentication means and when and how to deploy it*
- *How to assess the security of your network*
- *How different types of firewalls are installed and managed*
- *How different types of VPNs are suitable for different tasks*
- *Deployment considerations for firewalls, webservers, and VPNs*
- *Challenges of securing the road warrior and telecommuter*

You Will Leave With:

- *White papers on security technologies and types of products*
- *Selection criteria for firewall products and add-ons*
- *Checklist for auditing the security of your network, gateway, and public servers*
- *Directory of security sites, servers, and mailing list*
- *Pointers to free, on-line security resources*
- *Questions to ask your firewall vendor(s)*
- *Questions to ask your VPN vendor(s)*

This course presents detailed information about defending your IP networks from attack. Firewalls have been a "must have" since before the Internet came into common use. VPNs have been around almost as long, but only recently have been "actively deployed" by organizations.

In this course we explore using Internet firewalls and virtual private networks (VPNs).

Any poorly configured server or desktop may be vulnerable to attack, any application server can have bugs that permit unauthorized access, and every communications path is vulnerable to eavesdropping. We will discuss these vulnerabilities, and show how firewalls can be configured to protect against many of them. Different types of firewall technology will be defined and discussed, giving an overview of their strengths and weaknesses. Representative products will be compared and contrasted.

We will also discuss VPNs, by laying the cryptographic foundation and discussing the types of VPNs in use and where they are deployed. We will discuss deployment considerations, infrastructures needed (or not needed) and how to develop a rollout plan.

Students are encouraged to bring examples of firewall and VPN deployment considerations for class analysis and discussion.

Course Outline:

1. Firewalls

Introduction to Internet Firewalls

- Different Types of Firewalls
  - Simple Packet Filter overview
  - Stateful Packet Filter overview
  - Application Gateway overview
  - Hybrid overview
  - Firewall Appliances
  - Firewall Multiservers
  - Personal Firewalls
- Weaknesses: Known and Imagined
- Criteria: How to pick a firewall
- Configuring and managing Firewalls
  - Simple Packet Filter
  - Stateful Packet Filter
  - Application Gateway
- Additions to Firewalls
  - Strong User Authentication
  - Content Screens
  - Intrusion Detection
  - Honey pots and traps
- Questions to ask Firewall Vendors
- 10 Ways Your Firewall's Security Can Be Weakened

2. VPNs

- Cryptography for VPNs
- The technologies and types of VPNs
  - Gateway to Gateway
  - Mobile User to Gateway
  - IP Layer
  - Circuit Layer
  - Application Layer
- Deployment Considerations and Rollout Requirements
  - Firewalls and VPNs
  - "To PKI or not to PKI"
- Questions to ask VPN Vendors

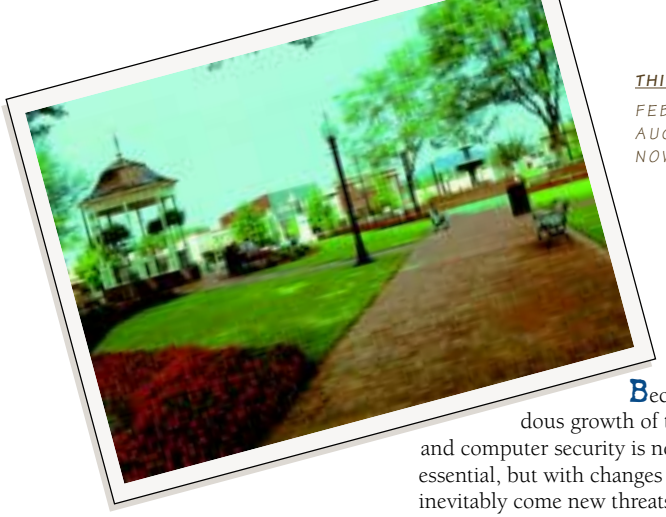
3. Assessing your network security

Firewalls and VPNs: Introduction and Best Practices

Fred Avolio

"Fred rates right up there with Tom and John. A big plus for CSI courses is the high quality of the instructors."

- Duanne Hardy
Data Security Specialist
Utah Department of Health,
Office of Information Technology



THIS CLASS OFFERED:

FEB.	13-14	MARIETTA, GA
AUG.	29-30	OTTAWA, CANADA
NOV.	1-2	WASHINGTON, D.C.

You Will Learn:

- *Cryptographic basics*
- *Defensive and offensive methods and mechanisms, including multiple firewall deployment and management*
- *VPNs: types and deployment, site-to-site and user-to-site*
- *Intrusion detection systems: types, strengths, weaknesses, and use*
- *The 10 worst Internet threats and how to counter them.*
- *The 10 management errors that lead to vulnerabilities and how to avoid them*
- *Hacker tools to use to test and verify firewalls and ID systems*

You Will Leave With:

- *Checklist for responding to ID reports*
- *Checklist for a quick and accurate security assessment of your enterprise network*
- *White papers on security technologies and products*
- *Contact information for keeping up with security advisories and vendor patches*
- *Pointers to free and commercial solutions*
- *Directory of security sites, servers, and mailing lists*

Because of the tremendous growth of the Internet, network and computer security is now recognized as essential, but with changes in technology, inevitably come new threats, vulnerabilities, and increased risk. The paradigms for security that were established a few short years ago must metamorphose in order to meet the challenges of these changes. No longer is antivirus software on every desktop and a single firewall on a gateway sufficient. It's time to progress from defensive solutions, to enabling solutions.

This course is for network managers, system administrators, and security managers who already know the basics and want to move to the "next level" of internetwork and computer security, beyond antivirus software and firewalls.

This course will survey what lies beyond firewalls. We are in "the next generation" of Internet use, and must start today rolling out additional mechanisms and employing added methods. We will also discuss the growing trends in security which lead to insecurity.

Upon completion of the course, participants will have a good working understanding of cryptography and its use in network defense, intrusion detection system use, and techniques for securing the telecommuter and traveler. The participant will be able to evaluate advanced tools and plan their deployment and use.

(Note: we will touch only briefly on firewalls and VPNs, as they are covered in another course.)

Course Outline

- How bad guys break into networks — threats and vulnerabilities
- Multiple layers and multiple methods in security
- Cryptography for network and computer defense
- Intrusion Detection Systems
  - A taxonomy of IDS
  - Where and how to deploy IDS
  - How to make the most use of IDS
  - Dealing with IDS information overload
- Adaptive and Reactive Security
  - Examples
  - How to effectively use them
- The Fuzzy Network Security Perimeter Becomes Fuzzier
- Securing the Road Warrior
  - Special needs, special vulnerabilities
  - Protection of communications
  - Protection of data
- The 10 worst security threats and how to counter them.
- The 10 management errors that lead to vulnerabilities and how to avoid them
- Hackers tools for verification and testing
- Ultimate security — what to do with unlimited people, time, and funds

There will be opportunities to share concerns, suggest solutions, and map plans during class discussions through interactive problem-solving workshops.

Caveat emptor: This is an update of last year's "Advanced Network Security." If you took that class, you shouldn't need to take this one.

Internet Security Tools and Techniques

Fred Avolio

"This class helped fill in the missing pieces I needed for security solutions. It also cleared up a lot of misconceptions I had."

– Clint Bodungen
Information Security / Systems Engineer, SynchroNet

Prepare for Professional Certification with CSI's new 3-Day CISSP® Prep-for-Success Workshop

- *Team-taught by subject matter experts across the ten domains of information security—an industry first!*
- *Minimal, 3 day time investment away from the office delivers a full 20 intensive hours of instruction*
- *The most cost-effective and time-efficient certification training approach available in the industry*
- *Designed to leverage prep time by identifying your weak areas and applying credible resources for self-study—at your own pace and site*
- *Will significantly improve your familiarity with the CISSP® examination and strategies, boost your pre-test confidence and increase the probability of examination success*

If you've been in the information security field for a few years and are looking to achieve professional certification as a CISSP® (Certified Information Systems Security Professional) this is the course for you!

Gauge your ability to pass the CISSP® exam and leave this course with a customized, focused plan to reinforce your areas of weakness. Individuals who are concerned that their years of experience may be too heavily skewed toward just one aspect of the expansive information security Common Body of Knowledge (CBK) will benefit from this workshop.

Perhaps you have an abundance of management and administrative experience but are wondering just how much technical knowledge it will take for you to pass the exam...or vice versa! CSI has developed its new 3-day CISSP® Prep-for-Success Workshop expressly for you.

Over an intense three day period of instruction, attendees will learn from a hand-selected team of subject matter experts, credible and current in the domains they teach.

Course Content Includes:

- Overview of the 10 domains of the Common Body of Knowledge (CBK) for the information systems security field:
  - Access Control Systems & Methodology
  - Telecommunications & Network Security
  - Security Management Practices
  - Application and Systems Development
  - Cryptography
  - Security Architecture and Models
  - Computer Operations Security
  - Business Continuity & Disaster Recovery Planning
  - Law, Investigations and Ethics
  - Physical Security
- In-class diagnostic test comprised of 125 sample test questions (half that of the actual CISSP® examination) with a follow-up critique of your performance
- CISSP® Exam overview and strategies
- Specific, credible resource list for self-improvement in each domain
- Pre-class assignment — ensures your maximum benefit in time spent away from the job

Space is limited and we anticipate rapid sell-outs, so sign up early!

Tuition: $1495 per person

New to the field of information security or considering entering it?

People who are new to the information security field will benefit from the condensed overview this session gives on the CBK, but are advised that this course is not intended to provide education in the foundation principles or practices of information security. For you, CSI recommends both "Introduction to Computer and Network Security" (page 6) followed by "Management Skills for a Superior Information Security Program" (page 7).

Take This Course Post-Conference:

Note: for the convenience of our conference attendees we've planned two of the four CISSP® Prep sessions around our two major conferences: June 20-22 in New Orleans following NetSec and October 31-November 2 in Washington, DC following the Annual conference. These two sessions will have a Wednesday 1:00 pm start time, immediately following the conference activities. This may allow non-conference attendees to fly in the same day the class starts. Please plan your flight schedules and conference attendance accordingly!

The CISSP® Prep workshop is available for presentation to your staff at your site. Contact CSI's Pam Salaway at 631/878-2205 or email psalaway@cmp.com.

THIS CLASS OFFERED:

MAR. 14-16	PHOENIX, AZ	
JUNE 20-22	NEW ORLEANS, LA	(JUNE 20 BEGINS AT 1 PM)
SEPT. 19-21	SAN ANTONIO, TX	
OCT. 31-NOV. 2	WASHINGTON, D.C.	(OCT. 31 BEGINS AT 1 PM)

Tag-Team of Domain Experts

Patrick D. Howard, CISSP

Domains of expertise:
Law, Investigations, and Ethics; Physical Security; and Security Management Practices.

With over 25 years experience in the security profession, eleven of those years spent conducting and managing information security architecture projects, Pat's range of experience includes information security program management, threat and vulnerability assessment, risk analysis, business continuity and disaster recovery planning, security policy development, crime and investigations, system certification and accreditation, security awareness and training program development, and physical security. While associated with the U.S. Army, Comsis Corp., PRC, Troy Systems, and Ernst & Young LLP; his clients have included U.S. federal and state governments as well as private sector clients in the financial services and telecommunications industries. Since November 1999, he has served as Manager, Methods and Administration, Netigy Corporation, San Jose, California.

Cheryl Jackson, CISSP, CBCP

Domains of expertise:
Business Continuity Planning and Disaster Recovery Planning; Operations Security; and Applications and Systems Development.

Cheryl has over nineteen years experience in information services specializing in the analysis, design, and implementation of comprehensive information protection solutions, including the technical tools, vulnerability assessments, risk analysis, and requisite policies, standards, guidelines, and procedures for safeguarding corporate information resources. She has extensive consulting experience with major organizations in multiple industries including investment banking, oil and gas, manufacturing, energy, transportation, and communication. She is currently part of Netigy's Global Security Practice and is responsible for the development of Netigy's methodologies and tools in the security management process arena.

Justin Peltier, CISSP, MCNE, MCP, CCSE, RHCE, CCNA

Domains of expertise:
Telecommunications and Network Security; Cryptography; Access Control Systems and Methodologies; and Security Architecture and Models.

Justin's years of experience have been dedicated to planning, designing, and implementing technical security solutions in a wide range of operating environments including Novell, NT, Sun Solaris, LINUX, and Netscape systems, as well as with Ethernet, Token Ring, TCP/IP, and IPX/SPX topologies and protocols.
He currently serves as Chief Technical Engineer for Netigy and is the company's primary technical instructor in the areas of vulnerability assessment, risk analysis, virtual private networking, policies and procedures, and penetration testing. Previously, he served as Director of Security for Ideal Technology Solutions, responsible for network consulting and support nationwide for clients such as Detroit-Edison, Rockwell International, and Stroh's.

Thomas R. Peltier, CISSP

Domains of expertise:
Security Management; Access Control and Methodologies; and Operations Security.

Heading up CSI's energetic "tag-team" of expert instructors and quality-assuring their efforts is long-time security professional and popular CSI instructor, Tom Peltier. Tom is currently Director of Methods and Administration for the Netigy Corporation's Global Security Practice. Previously, he was National Director for Consulting Services for CyberSafe, Corporate Information Protection Coordinator for Detroit Edison, and Information Security Specialist for General Motors. Tom has received the 1999 ISSA's Individual Contribution to the Profession Award, the Computer Security Institute Lifetime Achievement Award and CSI's Information Security Program of the Year Award.

3-Day CISSP® Prep-for-Success Workshop

NEW 2001

CISSP®

CISSP® is a registered trademark of (ISC)2, the International Information Systems Security Certification Consortium, Inc. (ISC)2 is the not-for-profit organization that administers the certification examination and authorizes professional certification for the information security industry. For more information about the CISSP® designation and requirements for certification, please visit their website at www.isc2.org

THIS CLASS OFFERED:

APR.	26-27	CINCINNATI, OH
SEPT.	19-20	SAN ANTONIO, TX
NOV.	29-30	GAITHERSBURG, MD

You Will Learn:

- *Cryptographic principles, trends, history and usage*
- *Where encryption belongs in securing your organization's information assets*
- *Relevant cryptographic terminology used in detailed security analysis and marketing material*
- *Differences between secret key and public key encryption systems*
- *How public key cryptography works in a network*
- *The role and benefits of Certificate Authorities and how to go about implementing them in your environment*
- *How to get buy-in among managers and users for encryption-based solutions*

Use encryption technologies to maximum advantage through a solid understanding of how they work and what capabilities they provide. Understand in practical terms what encryption is, what it can and cannot do, where it's been, where it's going and where it fits in the securing of your vital information assets. Learn why no matter what other controls anyone considers for current and future networks, encryption must always be there, either separately or as part of the structural framework. Analyze the entire area of Public Key Infrastructure from a practical business perspective. Participate in discussions that examine effects on end users, administrators and network performance. Learn what is involved, how it could affect your operations, and what you need to do to make PKI implementation successful.

Day One

Introduction and Foundation — First build the foundation required for understanding cryptographic principles, trends and usage, analyzing encryption's role, examples of good and bad cryptographic implementation and where it fits in securing an organization's assets. Discover the vocabulary of encryption: the most important terms, algorithms and current jargon.

Digital Signatures — Learn how public key cryptography can also be used to ensure messages have not been doctored in transit and that it indeed came from whoever said they sent it. We'll look at the one-way encryption of message hashing algorithms and explain the value of this approach to message integrity. Using encryption technology to put a "digital signature" on a message lets us know that the "from" address or field is accurate...as long as the sender's password has not been compromised.

Types of Encryption — Emphasizing non-DOD applications, dig into pertinent managerial issues as well as technical aspects of key management, DES, RSA and Public vs. Secret key encryption schemes, analyzing for effectiveness and limitations. Without trying to make attendees "cryptanalysts" or "cryptologists", we'll attempt to explain why public key cryptography is such an elegant piece of applied mathematics, and why it's so slow. We'll also show why, when it comes to encryption key size, larger is usually, but not always, better.

Day Two

Certificate Authorities (CA's) — Some say we cannot engage in electronic commerce without a CA acting as a trusted, independent third party. Others assert that the CA serves primarily as a mechanism for lawyers to insert themselves into Internet business activities. Analyze the phenomenon of certificate authorities to see how much truth (if any) there is in either of these perceptions. Learn where and how CA's fit in a public key encryption infrastructure, what services they can provide and how to implement certification authorities within your own environment if you choose to forego commercially available services.

Selling encryption to management and users — You'll learn several of the common reasons for resistance to security controls incorporating encryption and also analyze some underlying, often unstated reasons. Receive practical suggestions on methods to overcome both the stated and unvoiced objections and get the ball rolling.

A Practical Guide to Encryption and Certificate Authorities

John O'Leary

"This was very interesting. It seems to cover the whole subject. It is a good reminder to implement PKI."

- Andre Chicoine
Senior Consultant, Information Security, IBM

THIS CLASS OFFERED:

MAR.	13-14	NEW YORK CITY
JUNE	16-17	NEW ORLEANS, LA
AUG.	9-10	GAITHERSBURG, MD
NOV.	1-2	WASHINGTON, D.C.

You Will Learn:

- *The pros and cons of different PKI architecture*
- *How to decide whether to insource or outsource a PKI*
- *What to look for in choosing a PKI solution*
- *How to integrate a PKI into your existing security infrastructure*

You Will Leave With:

- *A list of PKI selection criteria*
- *A summary of available PKI solutions*
- *A firm understanding of how to choose and design a PKI solution.*

Organizations looking to deploy e-commerce initiatives are faced with the issue of how to secure transactions in a fast-moving environment. Companies looking to support authenticated, encrypted, validated transactions often look towards emerging security technologies to support e-commerce. This course will explore the evolving Public-Key Infrastructure, and its role in enabling e-commerce initiatives. We will begin with the role of public-key cryptography in securing electronic commerce and the need for a public-key certification infrastructure (PKI) as a basis of trust in public keys. We will explore how certification authorities, registration authorities, and directory services work, and who is building these products.

The focus of the course will be on practical solutions to integrate these products into a complete e-commerce solution. Attendees of this course will obtain an understanding of the various components of a PKI, as well as the PKI's role in supporting e-commerce. Both global and local solutions, along with ways to link the two, will be explained, with emphasis on the architecture and deployment of actual solutions in a corporate environment. The course will also discuss some of the legal questions surrounding the use of public-key certificates within an organization.

Course Outline

- Requirements for secure e-commerce
- The basics of public-key cryptography
- Applications that make use of PKI
- The role of the various components of the public-key infrastructure
- Issues of integration of the PKI with applications
- The role of the Certification Practice Statement (CPS)
- Outsourcing and management issues
- Product selection requirements
- Available products and services
- Interoperability issues with products and components

Securing E-Business: A Technical Guide to Implementing PKI

Anish Bhimani,

Kevin Browne

"Instructor very knowledgeable, learned a lot, course was useful for implementing CA's in our organizations."

– Jason Pantalone
RMP Technologist, Passport Office

THIS CLASS OFFERED:

JUNE	16-17	NEW ORLEANS, LA
SEPT.	17-18	SAN ANTONIO, TX
OCT.	27-28	WASHINGTON, D.C.

How to Perform a Technical Network Vulnerability Assessment

Justin Peltier

You Will Learn How To:

- *Identify tools to assist in network vulnerability assessment*
- *Conduct a thorough network vulnerability assessment*
- *Identify where to obtain tools*
- *Combine the output from tools to see a complete picture*

You Will Leave With:

- *An understanding of how to run vulnerability assessment tools*
- *A list of common tools and their locations*
- *An ability to search the internet for updates and more information on vulnerability assessment*

See also "How to Manage a Network Vulnerability Assessment" (page 12).

With the proliferation of connected networks, in which it is common for an organization to have connected their resources to intranets, extranets, and the Internet, the number of potential malicious users grows exponentially. In order for an organization to combat the likelihood of service interruption and corruption of data, periodic vulnerability assessments are essential.

In this two-day, demonstrative workshop, we will examine how to conduct a cost effective vulnerability assessment, beginning with time maximization techniques and including all the tools of the trade. This class is targeted toward the technicians who will be running the tools, interpreting the results, and proposing corrective actions, and is a companion course to the CSI course titled "How to Manage a Network Vulnerability Assessment". A demonstration of the most popular tools and information on how to obtain them will be included.

Day One

Tool Selection: Selecting the appropriate tools — During this session discussion will focus on how to select the correct tools for your organization. Because you most likely will have limited funds with which to obtain tools, we will direct you to the Internet sites that offer the best tools for the lowest cost.

Tools will range from shareware to freeware and will also include commercial products that run on a variety of popular platforms and hardware architectures. We will also look at using different tools in tandem, in order to provide a more complete picture of all the network vulnerabilities.

Hints and Pitfalls — We will discuss how to approach known hacker sites to gain the tools needed to conduct a vulnerability assessment. We will review the requirements for establishing a quarantined environment to test freeware and shareware before placing it into the network.

Day Two

Technical demonstrations — During this session there will be a demonstration of common tools used in network vulnerability assessments. The focus will be freely available tools such as Nmap, Sam Spade, and Nessus. We will discuss how to install the products and what things to look for to ensure the installation has gone correctly. Discussion will follow covering technical advantages to running the tools on different operating systems.

Next, we'll examine outputs from each of the products and discuss what they mean to your enterprise. We'll show how to modify parameters to obtain additional information and how to fine-tune the search capabilities.

Finally, we'll take a look at commercially available products and examine the outputs from their reports. We will discuss the pros and cons of each product, what platforms they run on, what they search for and where to go to get additional information.

THIS CLASS OFFERED:

MAY	17-18	OTTAWA, CANADA
JUNE	21-22	NEW ORLEANS, LA
SEPT.	27-28	NEW YORK CITY

You Will Learn:

- *How to incorporate classic security goals of availability, integrity and confidentiality into your e-business security program*
- *How to analyze the architectural framework of security in your organization to see if it will support e-commerce*
- *Threats that make e-business dangerous and weak points in your defense that may allow the threats to cause damage*
- *Internal and external security controls that can help secure your web-based business environment*
- *Where different implementations of encryption fit into your defense posture*
- *The absolute necessity for rapid, accurate recovery from outages*

You Will Leave With:

- *An understanding of e-business security issues*
- *A self-developed blueprint for e-business security at your organization*

This course covers the essentials of e-business security and continuity. We will see how classical computer and information systems security principles apply in the warp-speed world of electronic commerce. We'll cover strategies for identifying risks and selecting and implementing appropriate countermeasures.

Day 1

Goals — We'll examine the goals of classical network security (availability, integrity and confidentiality) to see how they fit into the context of e-commerce, how to best achieve these goals and what it takes to determine how much of each is enough.

Architecture — Are the building blocks of security the same as always? Will the existing foundation of policies suffice, or will they have to be rewritten for the new environment? E-commerce usually means more security domains, probably more platforms, definitely more applications, perhaps all from different vendors and all using different mechanisms for security. Administration thus becomes much more complex. Perimeters are harder to define. Single sign-on might start to look like a more questionable proposition. Oh, and the marketing people want us to take a few bricks out of that firewall so potential customers can query our inventory files when they visit the website.

Threats and Vulnerabilities — We'll describe attack profiles and timelines, and compare the threats from insiders and outsiders, digging into their motivations. We'll discuss some actual events and probe for weaknesses that allow the threats to have severe impact. Inadequate staffing, lack of training, priorities, budget constraints and other vulnerabilities associated with e-business will be examined.

Internal Security — Operating system controls must be implemented for all platforms in the e-business environment. That means mainframe, linux, UNIX (all flavors), NT, NetWare, OS/400, Win 95, 98, 2000, maybe even whatever runs on those palmtops. Internal security must cover LANs, databases and data warehouses, customer information, employee information, sensitive corporate information… and the list goes on.

Day 2

External Security — This includes the perimeter of our computing environment. Here we deal with firewalls, intrusion detection/response and VPNs. External e-commerce security also might be expanded to include security for Intranets and Extranets. Forensics certainly becomes an element after an attack. We'll also discuss liaison with law enforcement.

Encryption — We'll look at digital signatures, one of the rocks on which e-commerce is built. After public key algorithms, the AES and message digests, we'll plunge headfirst into the murky waters of PKI to see if it is truly a necessary element of our e-business architecture. Other aspects of encryption also pop up in the e-world, notably steganography for digitally watermarking intellectual property and executives forgetting to encrypt the sensitive data on the notebooks they lose.

Recovery — Distributed denial of service attacks in 2000 highlighted the need for immediate recovery if the website is your sole business presence. We'll explore what must be considered when planning a website recovery, including the reality that when you outsource any or all of your e-commerce initiative, you are dependent on the other guy's recovery plans.

Elements of the Solution — You might consider outsourcing some of the security tasks. We'll discuss the pros and cons. Security awareness is still a crucial element of your overall e-security posture, as are reasonable policies, consequences for violations and continued vigilance.

NEW 2001

Management Essentials of E-Business Security and Continuity

John O'Leary

"Excellent instructor. Has depth of knowledge on many security topics and was open to all questions. I will willingly attend other courses he gives."

- Tom Scurrah
Executive Director, Bell Atlantic

THIS CLASS OFFERED:

MAR. 15-16	NEW YORK CITY
JUNE 21-22	NEW ORLEANS, LA
SEPT. 19-20	SAN ANTONIO, TX
OCT. 27-28	WASHINGTON, D.C.

You Will Learn:

- *A structured process for designing a comprehensive eBusiness security architecture*
- *How to ensure the architecture meets the overall eBusiness goals of your enterprise*
- *How to 'Fast-Track' the design process to meet tactical 'Fast-Time-To-Market' business needs within a strategic architectural framework*
- *How to understand and meet both business and technical requirements*
- *Key eBusiness security strategies and how to deliver them as operational programs*

You Will Leave With:

- *A generic architecture design model*
- *An outline architecture framework customized to your enterprise needs for eBusiness*
- *Practical experience in using the architecture design process*
- *An outline Logical Domain model for your enterprise*
- *An outline Trust model on which to overlay physical deployments*
- *Reference tools for selecting the most appropriate technical and operational security mechanisms*

To be successful, security must meet the needs of business – but not just *any* business, *your* specific business and everything that makes it unique. If you need to deliver a security architecture that really *works* in an eBusiness culture, then this highly participative seminar is for you. We'll take attendees through a detailed and proven security architecture design process used successfully by a number of high profile multi-national organizations. It covers not just the theory of a leading security design process but provides participants with an intensive program of workshops so those participants are empowered to effectively apply good security in the workplace.

On completion of this seminar you will have developed an outline for a comprehensive strategy to create an effective eBusiness enterprise security architecture, or improve an existing program. The strategy developed will be applied to your own specific business requirements and these objectives will be achieved through an innovative combination of presentations, peer group discussions, team workshops, interviews and role-playing activities.

Course Content

1. The Challenges And Issues Posed By EBusiness
- Introduction
- The changing business environment
- An introduction to the business and security challenges and issues
- An introduction to the technical challenges

2. What Is Security Architecture And Why Do We Need It?
- The role of architecture in eBusiness
- The role of risk in architecture design

3. A Framework for Architecture Design
- Overview of the best practice approach
- The Business view (Contextual)
- The Architect's view (Conceptual)
- The Designer's view (Logical)
- The Builder's view (Physical)
- The Trademan's view (Component)
- The Facility Manager's view (Operational)

4. Contextual eBusiness Security Architecture
- Defining the business context for eBusiness
- Gaining Management buy-in and support
- Approaches to defining and validating short-term, medium, and strategic requirements
- Fast-Time-To-Market requirements in eBusiness

5. Conceptual eBusiness Security Architecture
- The strength-in-depth concept
- Security layering concept
- Layering in the technical reference model
- Information and Information Security concepts
- The trust concept & Trust Modelling
- Registration and certification concepts
- Business entities and trust relationships

6. Major Strategies Within The Conceptual eBusiness Security Architecture
- "Hot" eBusiness security strategies & concepts
- Cryptography, PKI, and Digital Certificates
- Tactical deployment of strategic objectives
- Strategies and concepts — interdependencies

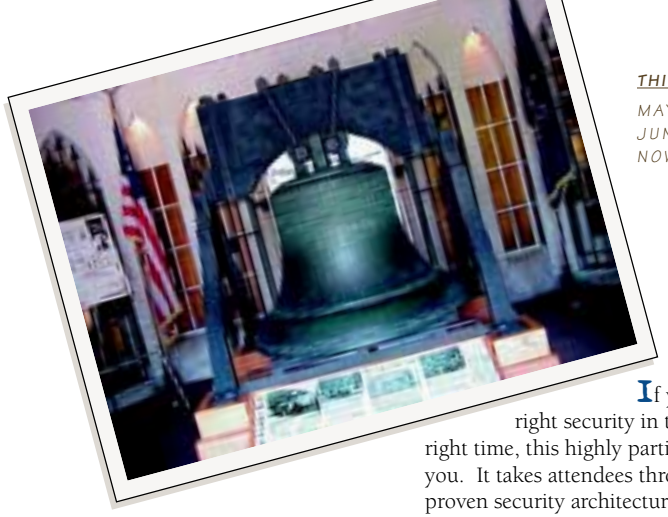
7. The Logical eBusiness Security Architecture
- Layering of logical services
- Defining logical network security domains
- Registration and certification
- Designing logical trust hierarchies

8. The Physical & Component eBusiness Security Architectures
- Physical security domain segregation
- Perimeter defense technologies
- Boundary definition and perimeter control
- Physical security mechanisms

9. Fast-Time-To-Market Architecture
- How to 'Fast Track' the architectural process
- Tactical solutions in a strategic framework

How To Design a Security Architecture For eBusiness

David Lynas



THIS CLASS OFFERED:

MAY	10-11	VALLEY FORGE, PA
JUNE	16-17	NEW ORLEANS, LA
NOV.	1-2	WASHINGTON, D.C.

You Will Learn:

- *How to ensure the architecture meets the overall goals of your enterprise*
- *How to understand and meet both business and technical requirements*
- *How to manage the design process and the resulting security program*
- *Key security architecture concepts and how to deliver them*
- *How to consolidate security solutions, improve efficiency and reduce costs*
- *How to select appropriate security technologies and architecture components*

You Will Leave With:

- *A generic architecture model and a supporting White Paper*
- *An outline enterprise architecture customized to your own business needs*
- *A detailed plan to validate enterprise business requirements for security*
- *Sample information collection documents*
- *A plan and method to implement and manage your security architecture*

If you need to deliver the right security in the right place at the right time, this highly participative course is for you. It takes attendees through a detailed and proven security architecture design process used successfully by a number of high profile multi-national organizations.

On completion of this class you will have developed an outline for a comprehensive strategy to create a winning enterprise security architecture, or improve an existing program. The strategy developed will be specific to your own business requirements and these objectives will be achieved through an innovative combination of presentations, peer group discussions, team workshops, interviews, and role-playing activities.

Security is an issue regarding your unique business, people and technical elements and requires a comprehensive program of counter-measures and solutions. Security Architecture can help solve these problems by providing:

- Strategic Architectural Framework to deliver business-driven technical solutions
- Inter-operability across systems
- Usability and scalability to fit business requirements
- Standardization of solutions
- Improved supportability
- Ease of integration
- Increased efficiency
- Reduced cost

Day One

- What is security architecture?
- Why is it needed?
- A framework for architecture design:
  - What are we trying to secure?
  - What is our motivation for securing it?
  - How should we secure it?
  - Who is involved in business and security processes?
  - Where should security be implemented?
  - When should security be applied?
- The role of risk in architecture design
- Defining the business context for security architecture
- Conceptual Architecture and key security concepts:
- Security attributes
- Business entities and their logical representation
- Trust and relationships between business entities
- Security associations between logical entities
- The defense in depth strategy

Day Two

- Logical and Physical Security Architecture
- The right place for Security – Network v. Application
- Security Policy architecture
- Security Domain modelling
- Logical and physical domains
- Role-based Access Control
- Authentication and Access Control services
- Security Management and the Operational Architecture
- Security service management
- Security mechanism and technology management
- Layer mapping and gap analysis
- How does the process work?
- Planning and management tools and techniques

How to Develop a Winning Security Architecture

David Lynas

"An orchestrated approach for providing a structure to enterprise security. All info security professionals should embrace this disciplined approach."

- Steven Scholochenko, CISSP, CISA,
Program Manager
U.S. Dept. of the Treasury

THIS CLASS OFFERED:

JUNE	21-22	NEW ORLEANS, LA
SEPT.	19-20	SAN ANTONIO, TX
NOV.	1-2	WASHINGTON, D.C.

3-DAY HANDS-ON VERSION OFFERED:

JAN.	24-26	ONTARIO, CA
APR.	18-20	ONTARIO, CA
JULY	18-20	ONTARIO, CA
DEC.	5-7	ONTARIO, CA

Technical Recovery of Electronic Evidence

Peter Garza

You Will Learn How to:

- *Select and use the tools that acquire and analyze digital evidence*
- *Present digital evidence*
- *Perform evidence recovery and analysis tasks using a sampling of tools*
- *Approach the evidence collection process with project planning techniques, including time and cost estimates.*

You Will Take Back With You:

- *CD-ROM containing:*
  - *demo/shareware/freeware tools*
  - *sample documents of reports, chain of custody, evidence labels*
  - *guidelines and other forms*
- *Interactive list of relevant web sites*
- *Other resources for IT investigators*

See also "Practical Forensics: How to Manage IT Investigations" (page 13).

Those responsible for conducting today's IT investigations, whether involving employee or external misconduct, are expected to have the level of technical sophistication necessary to review and evaluate electronic evidence, providing credible counsel about that evidence to decision makers. A familiarity with the tools used in acquiring and analyzing digital evidence is essential to fulfilling this role in today's work environment. Experience shows that sooner or later in all IT investigations, someone must sit down at the keyboard and extract electronic evidence in such a way that will make, not break, the pending civil case or employee administrative action. Evidence collection technicians must know how to skillfully make use of the tools and tasks of this new function.

This course will equip students with a complete understanding of the forensic techniques used by successful investigators when performing technical forensic tasks. Through an exploration of case studies that discuss first-hand lessons learned in real investigations, we will prepare students to begin evidence recovery tasks.

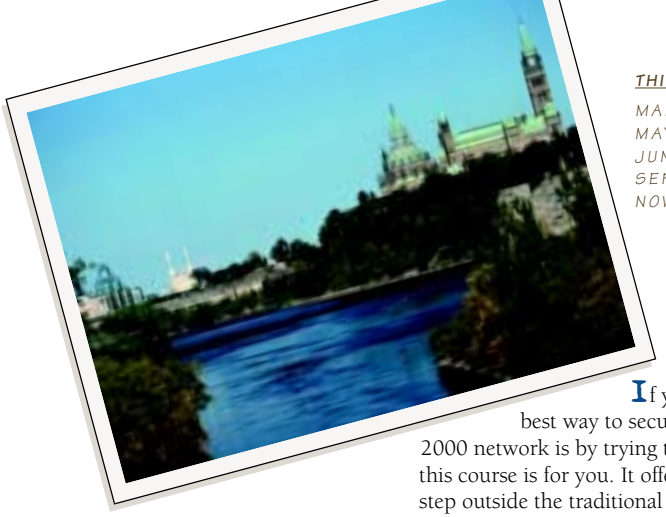
Course Content:

- Strategies for the recovery of digital evidence
- Preparing the specifications of your forensic toolkit
- The "duty expert" giving technical/operational advice
- Overview of data storage technology
- Remnant data that provide valuable clues:
  - Disk slack / memory slack
  - deleted files and memory page files
- Meta-data
- Dealing with encryption
- Forensic techniques in a heterogeneous computing environment – palmtops to servers
- RAID arrays, PC media, network appliances, Palmtops
- Adversarial vs. non-adversarial seizure of digital evidence
- Trouble shooting "in the wild"
- Case management techniques
- Demonstration of tools: *(NOTE: The 3-day course will provide hands-on training)*
  - image backup tools (e.g., Norton Ghost and Safeback)
  - forensic tools (Encase and Forensic Toolkit)
  - analysis tools (Orionlink and other analysis tools)
- Managing the data acquisition and analysis tasks
- Estimating and planning - task deconstruction

CHOOSE FROM TWO VERSIONS:

2-DAY LECTURE ONLY
OR
3-DAY HANDS-ON TRAINING

Investigation managers, legal counsel and evidence collection technicians will all benefit from this course. The three-day *hands-on* version is designed for those who find themselves "where the rubber meets the road"—at the keyboard deploying tools and techniques for the extraction of electronic evidence. The two-day *lecture-only* version of this course is ideal for those who will manage the forensic investigation.



THIS CLASS OFFERED:

MAR.	27-28	ST. LOUIS, MO
MAY	15-16	OTTAWA, CANADA
JUNE	21-22	NEW ORLEANS, LA
SEPT.	17-18	SAN ANTONIO, TX
NOV.	1-2	WASHINGTON, D.C.

You Will Learn:

- *How to assess Win 2000 security the way professional attackers do*
- *Best practices for hardening Win 2000*
- *What's new security-wise in Win 2000*

You Will Leave With:

- *A methodology for auditing your Win 2000 environment*
- *Checklists for securing Win 2000*
- *Tips for using new Win 2000 security features effectively*

If you believe that the best way to secure your Windows 2000 network is by trying to break into it, then this course is for you. It offers the opportunity to step outside the traditional IT administrator's shell and puts the students in the role of the hacker in order to more fully understand how to build Windows 2000 deployments that are secure from the most cutting-edge, real-world attacks.

The course will begin with a brief overview of security concepts to establish a framework for the ensuing material on attack methodologies.

Primary topics to be covered include:

- The Standard Hacker Methodology
- External vs. Internal Threats
- TCP/IP Host & Network Security Best Practices
- Social Attacks & Policy
- The "Low Hanging Fruit" Philosophy

Once the battleground has been populated, the attacks will begin. We will study the most effective mechanisms used by malicious hackers to compromise Windows 2000, based on field-tested, professional penetration research. We will cover such juicy targets as:

- The Web Application Layer & IIS5
- Password Weaknesses
- NetBIOS and SMB Vulnerabilities
  – Unauthenticated "Null" Sessions
- Trust relationships
  – LSA Secrets
- Client-side Attacks
  – Internet Explorer, Outlook
- Physical attacks
  – Encrypting File System
- Denial of Service

Feel like the bad guys have you outgunned? Don't despair — workarounds, solutions, and counter-measures will be outlined for each and every attack described. Unlike other courses that discuss Windows security in a vacuum, our emphasis on real-world attacks will leave students with more than just a cookbook of tips and settings to make Win 2000 more secure – you will walk away understanding the principles behind the vulner-abilities so that you can treat the causes of security problems rather than just the symptoms.

We'll finish the course with an overview of the great new security tools and features that shipped with Win 2000, and how they can help deter attacks globally across Win 2000 infrastructures.

Topics include:

- Group Policy
- Security Templates & Analysis
- IPSec
- EFS
- Kerberos
- Runas

Finally, the presentation will be dotted with references for further exploration and research, including books, mailing lists, people, and Internet sites. You will not find a more comprehensive Win 2000 Security boot camp – enroll today and get out from behind the security learning curve.

Windows 2000 Security

Joel Scambray

*This course is available for **on-site** presentation exclusively through CSI. Call Pam Salaway at **631.878.2205** or email psalaway@cmp.com.*

Duration: 2 days.

You Will Learn:

- *Information security basics: administration, product evaluation, risk analysis, DRP, incident response, awareness, vulnerabilities and countermeasures*
- *How performing security-related tasks well can often concurrently get other things done*
- *The urgency of trouble-shooting vs. implementing long-term solutions*
- *From team member to "cop": Ways to maintain the relationships and credibility necessary for effectiveness in all components of your job*
- *Ways to maximize your effectiveness by identifying points of overlap between jobs*
- *How to avoid losing sight of your primary job*

You Will Leave With:

- *Six completed exercises wherein you explain how you would handle a reality-based pressure scenario*

Continuing contraction of both corporate and government resources has forced more and more systems professionals and departmental function specialists to add information systems security to their roster of "other duties as assigned." If you are currently operating in this mode or see yourself there in the future, this two-day seminar is for you.

We will take a look at these questions and more: How can you be effective as a part-time security practitioner? How can you balance the requirements of your usual work function with the demands of the security job? What do you have to know? What can be set aside, and for how long? What's going to bite you if it doesn't get proper attention?

We'll survey how security works in some of the more popular platforms and identify sources where you can expand your detailed knowledge of the particular security controls available in your own environment. After this course, you should be more able to balance the competing demands of all your sub-jobs and do the security one especially well.

Day One

Challenges of part-time — We'll discuss the unique challenges involved in doing any function part-time vs. full-time. We'll look at the difficulties of shifting your mindset to an interrupting task and back again, and give suggestions for minimizing the disruption.

Security role vs. "other" role — We will examine the security function as a whole, to give you a broader view of your role and help you see where those potentially devastating errors lurk, waiting to be committed either by act or omission. Learn how others react to you when you are in your "security mode", and how to help avoid misunderstandings that can result when others' views of your role differ from your own.

Information security principles and practices — We'll give you a solid grounding in the philosophies and jargon of information systems security with an eye to tying security principles and practices to even the seemingly unrelated components of your variety of jobs. Discussions will cover not only the "how" but the "why" of security measures (anticipating your need to address that inevitable question by co-workers). You'll learn information security basics: administration, product evaluation, risk analysis, DRP, incident response, awareness, vulnerabilities and countermeasures.

Day Two

Challenges of being "multi-hatted" — We'll discuss setting priorities and personal goals, relating to co-workers differently in your various roles, gaining the support of others to assist you in your efforts, recognizing situations wherein you must stop and switch functions, leveraging information and techniques from one job function to the other and not losing sight of your primary job. We'll discuss the advantages as well as the downsides of being a part-time security person, especially in regards to how your co-workers react and interrelate with you as you act first in one capacity and then another.

Participative exercises — You'll engage in exercises designed to confront you with the type of scenarios that you should expect to see as a part-time security practitioner, taking into account corporate politics, group expectations and your need to enlist cooperation now and in the future.

How to Become an Effective Security Liaison: Security as a Part-Time Job Function

John O'Leary

"I really enjoy John O'Leary's courses. He is good at explaining issues and he keeps the class interested."

- Stacy Latterell
Information Security Administrator
The Antioch Company

*This course is available for **on-site** presentation exclusively through CSI. Call Pam Salaway at **631.878.2205** or email psalaway@cmp.com.*

Duration: 2 days.

You Will Learn:

- *Basic principles and technology of communications systems currently in use*
- *The three basic goals of network security and how they relate to your environment*
- *Critical vulnerabilities in communications systems and the safeguards available*
- *Network security terminology, and what it really means*
- *How to apply basic security principles to your particular communications configuration*
- *The importance of a focused awareness program*

You Will Leave With:

- *An understanding of the concepts, equipment and implementations of communications security*
- *Specific steps to take to avoid losing large amounts of dollars to telecommunications fraud*
- *A 3-step plan to minimize the threat to your organization posed by software piracy on internal networks*

This two-day workshop is for IT professionals, information security practitioners and auditors who need to understand the implications of communication methods, trends, and technologies from a security standpoint, and thus have a minimal technical foundation on which to build a framework for interacting with service providers and vendors. You'll get a basic understanding of technical underpinnings, procedures and skills needed to evaluate the risks to your communications systems and make good decisions regarding protection alternatives. The emphasis is on security principles and vulnerabilities and the practical safeguards you can take to mitigate, if not eliminate, the dangers. This course assumes no baseline knowledge of communications technology.

Day One

Communication Security Basics — We'll start by taking you through communications systems, concepts and components, tracking transmissions from end to end to give you a "big picture" of the entire process, explaining and analyzing dozens of terms in the ever expanding vocabulary of data communications security. Then, introducing the crucial concept of security domains, we'll show what happens when your data goes out over public networks and onto intranets, extranets or the Internet or into the custody of the "common carriers." You will learn vulnerabilities and protection strategies. We'll weigh the benefits and costs of encryption and other countermeasures. And, you'll see how to take the best advantage of available security provisions to protect vital communications channels.

Network Security — How does a communications system work? You'll find out by tracing a message through a network of clients, servers, backbones, encryptor boxes, firewalls, switches and modems, over wire, fiber and through the air. You'll learn how each can contribute to the strength or weakness of security in the network.

Transmission Technologies — Network security depends in part on the vulnerability of specific transmission methods. We will analyze the security of various implementations of metal wire, fiber optic cable, terrestrial microwave, satellite transmission, infrared and emerging technologies, focusing on inherent dangers and the protection they offer against unauthorized signal interception.

Day Two

Telecommunications — Your telephone system can be a major vulnerability. Hackers have taken over voice mail boxes and used company phone systems for criminal activity. Learn what the exposures are, what you can do to minimize your organizations' liability, and how you can prevent significant loss from phone fraud.

Networks — Local area networks and client/server systems present some formidable security challenges. What are the various network topologies and configurations, and how do they relate to security? What can we do to secure our LANs? We'll explain why an effective awareness program is so vital a part of LAN security.

Pressing Issues — What encryption methods are available and what factors affect the choice? What can you do to minimize the security exposure of Internet, intranet and extranet connections? Why is software piracy such a worrisome organizational danger in client/server systems? More importantly, what can we do about it? How does worldwide web commerce accentuate the need for rapid intrusion detection and response?

Point A to Point Z: A Primer on Data Communications Security

John O'Leary

"Great energy, enthusiasm, classroom management and anecdotes. He encouraged class participation."

– Ilene Switalski
Senior Systems Analyst, Philip Morris

Essential Training for the Decentralized Security Team

Duration: One day

John O'Leary

*This course is available for **on-site** presentation exclusively through CSI. Call Pam Salaway at **631.878.2205** or email psalaway@cmp.com.*

Your security department has been reallocated, leaving a skeleton few full-time security professionals teamed with an array of decentralized representatives. Whether you call them Local Security Representatives, Security Liaisons, or Departmental Security Officers, your security "point people" are no longer full-time security professionals. How will you provide them with a solid foundation in the principles of this newly-assigned job function?

Computer Security Institute has hand-crafted a unique on-site training session especially for these individuals, packaging it into one, cost-effective, intensive day. John O'Leary will deliver not only an understanding of security principles, but will deal with the everyday realities of functioning as a "part-time" security professional.

Course Outline

The Importance of the Security Function
- Why we need it
- Relationship to corporate mission performance

Foundation Security Principles
- Security and productivity
- Sensitive information
- Systems penetration threats
- Handling exposures
- Properties, principles, functions
- The Three Goals of a Security Program

Understanding the Terminology
- General
- Encryption/cryptography
- Network/telecomm

Today's Vulnerabilities and Countermeasures
- Strategies for protection
- Criteria for evaluating
- Encryption
- Authentication
- Access Control
- Specialized hardware
- Physical security
- Administrative controls
- Virus controls

The Security Professional
- Administration
- Risk analysis
- Incident response
- Awareness

Since presentation is private, at your site, you may select topics to stress, add on or omit.

New one-day duration designed as cost-effective training for your team at your site.

"John is great. He understands that we do not all understand the concepts. He's got a great teaching style and personality, and made the topic interesting and fun. It's nice to see that he enjoys what he does."

– L. Stephen Wilklow
IP Sales Associate, DMW World Wide

Computer Security: A Management Briefing

Duration: 2-4 hours

John O'Leary

*This course is available for **on-site** presentation exclusively through CSI. Call Pam Salaway at **631.878.2205** or email psalaway@cmp.com.*

This presentation will assist an organization's executives in understanding current, critical security topics and management's role in helping to protect corporate information resources.

Course Outline

Why We Need Security
- Conflicting priorities
- Examples of different security gaps
- Challenges and role of security

Security as a Business Enabler
- Security and Productivity
- Sources of Error
- Proprietary Information
- System Penetration Threats
- Handling Exposures

Management's Role in Computer Security
- Systems Life Cycle
- Program Organization
- Policies and Procedures
- Security Planning
- Risk Analysis
- Training/Awareness
- Handling Incidents
- Responsibilities

Current Topics
- The Internet and Security
- Inherent security limitations
- Vulnerabilities
- Lessons learned

Since presentation is private, at your site, you may select topics to stress, add on or omit.

"Excellent instructor.
Kept my undivided attention."

– Victoria Beale, Manager, Systems Division
Panama Canal Commission

Fast-Track Security Architecture Development Assistance

An Intensive 5-Day Project Conducted at Your Location

FAST-TRACK steers you through five highly productive days of delivery-focused activities designed to jump start your security architecture planning process.

Your Security Architecture will be unique because your business is unique. FAST-TRACK adapts to your needs so that no matter what type of business you are in, or what stage your architecture has reached, we will work with you to develop the five-day program that best helps you deliver the results you need.

With on-site help from Fast Track facilitators, your security architecture team will:

- Assess, understand and document your specific business requirements
- Define the key performance indicators and success metrics for security in your organization
- Produce the initial Security Architecture draft documents listed at left
- Create a project plan, to include goals, implementation schedules and migration strategies for presentation to management
- Evaluate the benefits of your draft Architecture and justify budget proposals with presentations to senior management

Information Security Awareness Program Development Assistance

An Intensive 5-Day Project Conducted at Your Location

Establish an information security awareness program across your entire organization.

This project will provide short-term assistance to your staff in planning an awareness program and its roll-out. The plan will be implemented by your team members according to schedules created as part of this project.

Program Goals

- Educate all awareness team members in order to allow maximum input of your specific concerns and prepare for ownership and maintenance by your staff.
- Assist in the creation of an information security awareness plan designed around the specific needs of your organization. Final document will be prepared by your team members.
- Provide a customized end-user awareness newsletter ready for reproduction and distribution to all employees on a quarterly basis.

Information Security Policies and Procedures Development Assistance

An Intensive 5-Day Project Conducted at Your Location

Establish or update your corporate information security policies and procedures.

This project will provide short-term assistance to your staff in creating the cornerstone of your information protection program —a set of concise, effective information security policy and procedure documents for publication. CSI will educate and prepare your team to proceed with the completion of this project following the CSI assistance plan.

Program Goals

- Educate all team members on proper development techniques for information security policies and procedures.
- Assist the team in identifying and prioritizing the array of information security issues which policies will address, using a compilation of examples gathered from hundreds of organizations.
- Assist the team in the on-site development of at least three critical information security policies, or others as prioritized:
  - — overall information security policy
  - — information classification policy
  - — electronic communications policy (Internet, e-mail, voice)

Five-Day Projects

Intensive Assistance Via 5-day projects conducted at your location

To schedule or for more information contact Pam Salaway at 631.878.2205 or email psalaway@cmp.com.

Join CSI's Working Peer Groups

The goal of the Working Peer Groups is to foster the exchange of information security best practices in a confidential and congenial setting, increasing members' overall knowledge of leading-edge solutions and their ability to make confident recommendations to senior management.

*Receive answers to your toughest security questions and share your discoveries with others—**Become a CSI Working Peer Group member.***

You will be part of a knowledge pool with decades of information security experience. This is a unique opportunity to refresh your efforts and gain a new perspective in a unique and confidential setting.

The security profession has historically been one of isolation–from others in the organization and, for reasons of confidentiality, from counterparts in other organizations. This isolation can create a tunnel-vision that suffocates creative solutions. Computer Security Institute's Working Peer Group was established at the request of member organizations as a solution to this tunnel-vision. Only through meaningful dialogue with your peers can you see your challenges and business from a whole new perspective.

Time spent with your peers is powerful

As a Working Peer Group member, you will discuss in confidentiality specific problems about your efforts to perfect an information security program that meets the needs of your organization today. You will return to your job not only with many realistic ideas to implement, but also a fresh new perspective on how to approach your problems.

Sample agenda from a recent peer group meeting

- Security status report from member company
- Notebook encryption products discussion
- Viruses, malicious code, hoaxes, chain letters, etc.: member presentations and discussion
- Setup and administration of mobile accounts discussion
- E-mail protection and security: roundtable discussion
- Electronic commerce security solutions and current practices: member case study
- PKI: two member presentations followed by discussion
- Privacy projects: outlines shared by two member companies
- Hybrid outsourcing issues and possibilities

Join us

To discuss your interest in joining a CSI Peer Group, please contact:

Pam Salaway

Manager of Special Programs

631.878.2205

631.874.5195 fax

psalaway@cmp.com

CSI Membership

Never has the information security industry experienced more profound and fundamental change than today. While this dynamic can be unsettling, it is also creating tremendous opportunities for people with specific industry knowledge and insight. Computer Security Institute (CSI) will help you develop and leverage your skills to best meet your specific job goals—as well as personal career goals.

As a CSI member, you'll receive information and exchange ideas about the important challenges of building and managing successful information security programs in today's competitive marketplace.

CSI Members Receive:

Computer Security Alert

Keep track of the rapidly changing information security industry with CSI's member-only monthly newsletter, Computer Security Alert. Our knowledge of the industry and access to the opinions of industry experts gives you perspective available nowhere else. Get the current news, information and analysis you need to do battle—and win.

CSI's Computer Security Journal

This quarterly publication gives you practical articles, case studies, technique outlines, commentaries, research papers and product reviews written by some of the industry's leading practitioners. These pros examine important new tools and concepts, offering expert insights on a wide variety of information security topics.

CSI's Buyer's Guide

This is the most comprehensive and up-to-date resource available in the computer security marketplace, featuring information on over 1000 products and services from approximately 500 vendors.

Tuition Discounts at CSI Conferences and Seminars

CSI members get $150 off tuition at CSI training events. Use it or let a colleague substitute.

Discounts on Security Publications

Save 20-25% on a variety of computer security-related publications.

And More

Registering for a Class?

CSI Members save $150 off tuition for CSI seminars and conferences.

You may use the registration form on page 36 to sign up for courses and membership, or use the form below to sign up for membership only.

Membership Registration:

❑ *Yes, enroll me as a member* ❑ *Send me information*

❍ 1 year	$197 (US/Canada/Mexico) or $237 (intl.)
❍ 2 years	$349 (US/Canada/Mexico) or $423 (intl.)
❍ 3 years	$469 (US/Canada/Mexico) or $567 (intl.)

Name_____

Title_____

Organization_____

Address_____

City_____ State_____ Zip/Postal Code_____

Country_____

Phone_____ Fax_____

Email_____

❍ **Please send invoice.**

❍ **Check enclosed U.S. funds made payable to Computer Security Institute**

❍ **Please charge my** ❍ **Visa** ❍ **Mastercard** ❍ **AmEx**

Card No._____ Expiration Date_____

Signature_____ Date_____

FAX membership application to (415) 947-6023
MAIL CSI Membership • 600 Harrison St. • San Francisco, CA 94107
WEB www.gocsi.com
CALL (415) 947-6320 to sign up by phone

More From CSI

CSI Publications

CSI Members save on these valuable publications:

IPAK-Information Protection Assessment Kit

The Information Protection Assessment Kit (IPAK) is a tool to help you determine how well your organization's information protection program is doing and where it should go in the future. The second edition features 11 categories, a new scoring system and an electronic version to make the process easier and more efficient.

— *25 page book; comes with disk.*
Member $157; nonmember $197

Annual CSI/FBI Computer Crime and Security Survey

The most widely quoted computer crime survey reveals annual trends. Learn where, how, and by whom cyber attacks are occurring, what financial losses are incurred and what organizations are doing to combat and prosecute intruders.

— *Free*

Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare, 4th Edition

This publication provides CEOs, CFOs, CIOs and other executives with a quick read on the latest cyber threats. It includes an exhaustive time-line of real-world incidents from 1970 to today, as well as 25 graphs, charts and maps from numerous studies. In 38 insightful, entertaining pages, corporate leaders and security professionals can get up to speed on the threats to the confidentiality, integrity and availability of the information that is the life's blood of their organizations.

– *Member $25; nonmember $37*

CSI Conferences

CSI Conferences set the industry standard, attracting thousands of information security professionals from around the world —the best way to network with your peers and advance your career.

NetSec2001: Technical Dimensions in Network Security

June 18-20, 2001, New Orleans

Over 85 sessions devoted to the security of Internet, electronic commerce and more.

28th Annual Computer Security Conference and Exhibition

October 29-31, 2001, Washington, D.C.

Over 130 sessions and the largest Exhibition of its kind, with over 180 security vendors.

FrontLine Awareness Newsletter for End-Users

Improve the security practices of your entire organization with FrontLine, *your personalized awareness newsletter*

FrontLine is a quarterly four-page newsletter, developed by Computer Security Institute (CSI) to increase end-user awareness of critical security topics pertaining to ***them***. A powerful awareness tool reaching every employee in the organization, ***FrontLine*** delivers and reinforces the security message in a friendly and easy-to-understand format.

Personalize it

Every quarterly issue carries your logo, company masthead, and your own column of about 350 words.

Distribute via printed copy, Intranet or use both methods

The subscription rate is the same for printed copy or Intranet distribution. CSI recommends using both formats and offers a special combination price.

Save time by leaving the work to us

CSI's own editorial staff researches and writes every ***FrontLine*** issue. You've got better things to do!

An annual subscription (4 quarterly issues) to *FrontLine* costs only $1,860. (US $1,900 for Canadian; US 1,940 for International). Both formats are only $2,760 (additional for Canadian and International subscriptions). You won't find a smarter way to invest in your security awareness program!

FrontLine addresses all critical end user topics:

- Password Protection
- Social Engineering
- Telecom Fraud
- Virus Prevention and Detection
- Data Back-up
- Computer Crime
- Internet Concerns
- Email Security
- Hacker Practices
- Physical Security

For Sample *FrontLine* Newsletter and Ordering Information:

Call (415) 947-6320 or
call Pam Salaway at (631) 878-2205.
E-mail *csi@cmp.com* or
psalaway@cmp.com.

A unique opportunity to partner with CSI — the CSI Training Trust

CSI Training Trust members are a select group of companies in the information security marketplace working in partnership with CSI to advance knowledge in the area of information protection. By hosting a CSI seminar, these leading companies show their commitment to furthering objective, third party education.

For further information on the extra exposure and benefits of forming this special alliance and becoming a Training Trust member, contact Pam Salaway at (631) 878-2205 or *psalaway@cmp.com.*

CSI
COMPUTER SECURITY INSTITUTE

Computer Security Institute
600 Harrison Street
San Francisco, CA 94107

Phone 415.947.6320
Fax 415.947.6023
Email csi@cmp.com
Web www.gocsi.com

CSI Information Security Seminars

where the industry goes for education

Four easy ways to register:

WEB www.gocsi.com
FAX 415.947.6023
PHONE CSI at 415.947.6320
MAIL TO Computer Security Institute
600 Harrison Street
San Francisco CA 94107

Please register me for the following seminars:

Circle appropriate fee for each class listed:

CLASS TITLE	DATES	CITY	CSI MEMBER	NON-MEMBER	GOVERNMENT (*)
1			$745	$895	$625
2			$745	$895	$625
3			$745	$895	$625
4			$745	$895	$625
3-DAY COURSES (*Circle*): Technical Recovery of Electronic Evidence (*Hands-on* Version)		3- Day CISSP® Prep for Success	$1,345	$1,495	

* *No other discounts apply to Federal Government rate.*

* *All fees are in U.S. currency drawn from U.S. bank.*

Membership: **1 Year**

❑ Yes, sign me up for CSI Membership (circle applicable rate): U.S. / Canada / Mexico $197

(*see page 33 for complete list of membership benefits*) International $237

Two-class discount: (*)

Register for 2 or more classes and subtract $95 on 2nd class, 3rd class etc. – $95

Team discount:

Register 2 or more people from the same organization at the same time and subtract $100 for 2nd person, 3rd person, etc. – $100

* *Two class discount does not apply to June or November classes or to Federal Government fee.*

Please place mailing label below, and make any necessary changes to name or address. Photocopy this form to register additional participants.

Name

Title

For CEU Credit Transfer: CISSP? ❑ yes ❑ no Cert. # _____

Organization

Address MS / Flr

City State Zip Country

phone fax

email

Are you a CSI member? ❑ yes: member# _____ ❑ no ❑ joining now

❑ Substituting for member: _____
NAME MEMBER#

How long have you been in info security? _____

Are you a government employee? ❑ U.S. Federal ❑ U.S. State ❑ Int'l Govt. ❑ County or Municipal ❑ no

Total enclosed: $

Payment:

❑ CHECK ENCLOSED (Please make check payable to Computer Security Institute)

❑ CREDIT CARD: ❑ Visa ❑ Mastercard ❑ AmEx

Card # exp. date

Signature

❑ Bank wire/electronic payment (please include a $20 service fee)

❑ Purchase order (attached) #_____

Questions about registering? Call our Registration Manager at 415.947.6320.
See facing page for registration information.

WBERC

Seminar Registration

Use form at left to register for a CSI Seminar or register directly on-line at www.gocsi.com

Registration Fees

Seminar fees are listed on the registration form. Fees cover admission and course materials. Fees are payable in advance by cash, check, VISA, MasterCard, or American Express. All checks must be drawn from a United States bank in US funds. CSI also accepts the U.S. federal government IMPAC credit card.

Cancellation Policy

If it is necessary for you to cancel your registration, we request that you submit your cancellation in writing. We must receive your cancellation request one week prior to the first day of the course. Payments are non-refundable. However, all pre-paid fees may be transferred to a future course. Substitutions are welcome at any time. Those who do not cancel and do not attend are responsible for the full registration fee.

Schedule Changes

CSI may occasionally find it necessary to reschedule or cancel a seminar. We will give registrants advance notification of such changes. CSI is not responsible for penalties incurred as a result of discount airfare purchases.

Continuing Education Credits: Automatic Reporting for CISSPs

All participants are eligible to receive 16 Continuing Professional Education (CPE) credits upon completion of each 2-day CSI seminar and 24 credits for 3-day seminars. CSI will automatically forward your certificate of completion for processing of the CPE units earned. If you are a CISSP and would like this service, simply list your certificate # in space provided on registration form.

Discounts

Member Discount —CSI members receive $150 off seminar tuition. For information on becoming a CSI member see page 33. You may sign up for membership on the seminar registration form to left.

Two Class Discount —Register for any two or more classes at the same time and receive $95 off the second, third, etc.

Team Discount —Register 2 or more people from the same organization at the same time, and subtract $100 for the 2nd, 3rd, etc. person.

Hotel Information

Accommodations

The hotels listed below are recommended. If you need the approximate room rates where not indicated for budget planning, please contact the hotel directory.

HOTEL-BASED TRAINING

The following four hotels are the training location as well as the accommodations.

New Orleans

Hyatt Regency New Orleans
@ Louisiana Superdome
Poydras at Loyola Avenue
New Orleans, LA 70113
504/561-1234

Phoenix, AZ

Crowne Plaza Phoenix Downtown
100 North First Street
Phoenix, AZ 85004
TEL 602/333-5000
800/359-7253

San Antonio, TX

La Mansion del Rio Hotel
112 College Street
San Antonio, TX 78205
210/518-1000
Training will take place at La Mansion and the Presidio, across the Riverwalk.

Washington, DC

Marriott Wardman Park
2660 Woodley Road NW
Washington DC 20008
202/328-2000

HOSTED TRAINING

NOTE: The following hotels are NOT the training location, but are listed for sleeping accommodations only.

Cincinnati, OH

Hyatt Regency Cincinnati
151 West 5th Street
Cincinnati, OH 45202
513/579-1234

Gaithersburg, MD

Gaithersburg Hilton
620 Perry Parkway
Gaithersburg, MD 20877
301/977-8900

Madison, WI

Woodfield Suites
5217 East Terrace Drive
Madison, WI 53718
608/245-0123

Marietta, GA

Wingate Inn
1250 Franklin Road
Marietta, GA 30067
770/989-0071

New York City

Wall Street Inn
9 South William Street
New York NY 10004
212/747-1500

Orlando, FL

Disney's BoardWalk Resort
2101 N. Epcot Resorts Blvd.
Lake Buena Vista, FL 32830
407/934-7639
(407/W-DISNEY)
Attendees may request rate quotes at other Disney hotels by using the same telephone number. Standard rates at all properties will apply.

Ottawa, Canada

Holiday Inn Plaza La Chaudiere
2 Montcalm Street
Hull, Quebec,
Canada J8X 4B4
819/778-3880

Phoenix I
January 30-31, February 1-2 and October 2-5, 2001

Crowne Plaza Phoenix Downtown
100 North First Street
Phoenix, AZ 85004
TEL 602/333-5000
800/359-7253

Phoenix II
April 3-6, 2001

Tempe Mission Palms
60 East 5th Street
Tempe, AZ 85281
480/894-1400

Rockville, MD

Doubletree Hotel
1750 Rockville Pike
Rockville, MD 20852
301/468-1100

San Francisco, CA

Hyatt Regency San Francisco
5 Embarcadero Center
San Francisco, CA 94111
415/788-1234

St. Louis, MO

St. Louis Marriott West
660 Maryville Centre Drive
St. Louis MO 63141
314/878-2747

Valley Forge, PA

Valley Forge Courtyard by Marriott
1100 Drummers Lane
Wayne, PA 19087
610/687-6700

Thank You to our 2001 Training Hosts:

American Family Insurance
Madison, WI

Depository Trust & Clearing Corporation
New York, NY

Edward Jones
St. Louis, MO

Levi Strauss & Co.
San Francisco, CA

Lockheed Martin
Marietta, GA
Valley Forge, PA

National Institute of Standards and Technology (NIST)
Gaithersburg, MD

Pinnacle West
Phoenix, AZ

Provident Bank
Cincinnati, OH

Salt River Project
Phoenix, AZ

U.S. Nuclear Regulatory Commission
Rockville, MD

Royal Canadian Mounted Police—Technical Security Branch
Ottawa, Canada

Walt Disney World Information Services
Orlando, FL

Computer Security Institute
600 Harrison Street
San Francisco, CA 94107

Phone 415.947.6320
Fax 415.947.6023
Email csi@cmp.com

Dear Information Security Professional,

Sign up now for the seminars that will keep your security program moving forward. CSI offers 21 seminars (8 brand new) on topics ranging from Intro to PKI to Windows 2000, for a total of 80+ publicly offered seminars in 2001.

Courses include:

- Internet Security
- Intro to Security
- Encryption & CAs
- Computer Forensics
- Security Architecture
- Incident Response
- Network Vulnerability Assessment
- Firewalls & VPNs
- Intrusion Management
- Implementing PKI
- E-Business Security
... Plus many more!

NEW! 3-Day CISSP® Prep-for-Success course – An industry first. The most cost-effective and time-efficient certification training approach available (pages 18-19).

Take a look inside and plan your training itinerary now. Register online at www.gocsi.com.

See you soon,

Computer Security Institute

P.S. Every CSI seminar in this catalog may be brought on-site to your organization. See inside for details.

To: