

Get into a Hacker's Mind. It's Your Best Defense

The Cyber Warrior Courses are uniquely designed to teach you how to view your computer network security the way a hacker would. You'll learn...

- Hacker methodology, tools, techniques, and strategies
- Defensive measures you can implement to protect your network

There is a Cyber Warrior Course for Every IT Security Professional

Cyber Warrior Fundamentals: Two-day overview of hacker methodology and defensive measures for IT security managers, system administrators, and project leaders.

Cyber Warrior Executive: Half-day intensive training specifically for C-level executives and senior officers.

Cyber Warrior Hands-On Lab: Two-day lab providing hands-on application of hacker tools, techniques and strategies for system administrators, network/security engineers, and IT professionals. Prerequisites: Cyber Warrior Two-day Basic Course or instructor permission.

Cyber Warrior Forensics and Incident Response: Two-day comprehensive introduction on response to network intrusions and security violations. Aimed at incident response teams, IT security and project managers and systems administrators.

Cyber Warrior End User: Two-hour condensed training for personnel that touches a computer keyboard.

Cyber Warrior DIACAP Introduction Course: One-day comprehensive outline of the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP). The Introduction to DIACAP Course provides the practical foundation for conducting certification and accreditation in accordance with the new DoD certification and accreditation process. This course provides detailed essential and in-depth instruction, covering eleven modules,

essential to any DIACAP certification accreditation effort.

Cyber Warrior DIACAP Transition Course: Half-day condensed training of the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP). The Transition Course provides the straight forward "how-to" steps on transitioning from DITSCAP to DIACAP.

Cyber Warrior DCID 6/3 Course: Three-day comprehensive training of the United States Intelligence Community's (IC) guidance for securing IC information systems in accordance with the Director of Central Intelligence Directive (DCID) 6/3. This course discusses the basic security requirements set as well as the information system certification and accreditation guidance applicable to all IC organizations.

Cyber Warrior Introduction to DCID 6/3 Course: One-day condensed training of the United States Intelligence Community's (IC) guidance for securing IC information systems in accordance with the Director of Central Intelligence Directive (DCID) 6/3. This course discusses the basic security requirements set as well as the information system certification and accreditation guidance applicable to all IC organizations.

How to Register

For course information please contact CyberWarrior@ngc.com.

Discounts

Please note that ISSA members as well as government and military personnel receive discounts on each course.

These courses satisfy continuing professional education (CPEs) credits for security recertification.

When America Needs Trusted IT Solutions, We're There

For more information on Northrop Grumman solutions and services, please send inquiries to Intel-Info@ngc.com or call 703-818-7400.

NORTHROP GRUMMAN

DEFINING THE FUTURE™

Learn to Protect Your Networks

Cyber Warrior

Do You Know Who's in Your Network?

It's not just about your local computer network, it's about much more: we're talking about a complex system with millions of computers operating on many networks, running thousands of applications and programs. We're talking about the Internet.

The sheer complexity of this system makes it difficult to understand and defend against attacks. That's why your network can be vulnerable in many ways and you may not even know it. Modern day computer systems, comprised of millions of lines of software code, are wrought with bugs and exploitable weaknesses. Education is your best defense. Understanding the fundamental concepts of how computers and networks operate is important, but it is becoming crucial to understand how attackers are exploiting weaknesses in these systems, and how to defend your network against them.

Northrop Grumman—A Name to Trust in IT Security Training

Northrop Grumman brings a unique perspective to IT security training. We're trusted to provide security for some of the nation's most important networks, including those of the U.S. Government and the Department of Defense—networks that are subject to attacks from the most advanced hackers using the latest tools and techniques. If you are concerned about maintaining the highest security for your business or agency, Northrop Grumman's Cyber Warrior Courses will make you aware of the latest threats and how to defend against them.

The Cyber Warrior Course curriculum is divided into two training categories: (1) Security Awareness Courses, (2) Certification & Accreditation Courses.

Value Proposition

- Save your company money by eliminating system downtime
- Protect your corporate information assets from theft
- Maintain your customers' trust by protecting their data

NORTHROP GRUMMAN

DEFINING THE FUTURE™

www.it.northropgrumman.com/ITSolutions

1795 Jet Wing Drive, Suite 200, Colorado Springs, CO 80916 719-638-1305
Northrop Grumman Information Technology, 7575 Colshire Drive, McLean, VA 22102 703-713-4000

© 2007 Northrop Grumman Corporation

D-00240d 10-23-2007





Cyber Warrior Comprehensive IT Security Awareness Courses

Cyber Warrior Fundamentals

The two-day Cyber Warrior Course uses fundamental computer and networking concepts as a foundation for in-depth description and demonstration of hacker tools, techniques, and strategies. This course covers the systematic, phased approach or methodology used by hackers in attacks as well as the defensive countermeasures that can be employed against them. Learn how to defend your networks through comprehensive analysis and demonstrations of the anatomy of an attack. The course is unique in its breadth and presentation methods, including more than 40 live demonstrations of hacker and security professional tools and techniques, with over 200 animated tutorial diagrams and screen-shots.

Who should attend:

- Directors, engineers, managers, staff, and project leaders working with computer systems and networks and those interested in the field of information security.
- System administrators who desire to broaden their expertise with network security concepts will also benefit from the course.

As an alternative to the two-day course, an executive-level version is also available for C-level executives and senior decision makers concerned about the network security of their organization.

Cyber Warrior Hands-On Lab

The two-day Cyber Warrior Hands-On Lab provides hands-on training in the use of hacker tools and threats for security professionals defending against attacks on public, private, government, and military networks.

The class includes more than 20 hands-on activities using hacker and security professional tools and techniques. There is one-on-one support during the two days to give the student the maximum amount of time to experience cyber warfare on a closed network.

Class size is limited to maximize the individual learning experience. All equipment will be provided.

Who should attend:

- System administrators, network/security engineers or other IT professionals who desire to broaden their expertise with network security concepts.

Prerequisites: Cyber Warrior Two-Day Basic Course or permission of instructor.

You'll be given a checklist at the end of these courses to run against your network systems. You'll see immediate measureable improvements and return on investment through implementation of Northrop Grumman's proven Cyber Warfare techniques.

Cyber Warrior Executive

As an alternative to the two-day Cyber Warrior Course, a half-day executive version is available. As an executive or decision maker, you must determine how to manage risk and protect your network. The Executive Course was designed specifically for nontechnical managers and staff to get them "up-to-speed" quickly on computer networking, security concepts, hacker methodology, and defensive countermeasures. This half-day course is a condensed version of the larger course offering and takes place in an informal setting that encourages questions, discussion, and interaction with the instructors.

Who should attend:

- Vice presidents, directors, managers, staff, and project leaders concerned with computer network security.
- System administrators who desire to broaden their expertise with network security concepts will also benefit from the course.

This executive-level version of the course is ideal for C-level executives and senior decision makers concerned about the network security of their organization. A two-day version is also available and recommended for a more in-depth presentation of the course material.

Cyber Warrior Forensics and Incident Response

A two-day comprehensive introduction to Forensics and Incident Response, this course was designed to help IT professionals understand how to prepare for and respond to internal and external network and information security violations.

This course is intended to cover entry level and intermediate concepts in digital forensics. It will also provide insight into the legal reforms that surround current privacy and compliance legislation. The issues covered are privacy protection, plans for data reduction, destruction during the course of business, and electronic document discovery and forensic examinations.

Explore forensic investigation techniques, including pre-incident preparation and methods that hackers use to evade audit logging controls and intrusion detection mechanisms. Jump-start the creation of an effective Computer Security Incident Response Team (CSIRT) by walking through the gathering of forensic evidence.

Who should attend:

- Managers, staff, and project leaders responsible for Computer Security Incident Response Teams and /or tasks.
- Law enforcement agents and intelligence analysts from both a national and business competitive interest.
- First Responders who desire to broaden their expertise with network security concepts.