NEbraska CERT Conference 2003

Computer Security and Information Assurance

August 5 - 7, 2003

Scott Conference Center

Omaha, Nebraska, USA

Presented by

NEbraskaCERT

Monday	**OPTIONAL CISSP / SSCP EXAM** see page 3 for additional details			
Tuesday	**7:30 - 8:30**	**8:30 - 9:30**	**9:45 - 10:45**	**11:00 - 12:00**
Technical	**REGISTRATION & CONTINENTAL BREAKFAST**	**TT-1:** Intro to Forensics 101	**TT-2:** Incident Preparation & Response (MIPR)	**TT-3:** Process Capability for Information Assurance
Expert		**TE-1:** AI Techniques	**TE-2:** z/OS (MVS) Security	**TE-3:** Implementing Enterprise Info Security
Manager		**TM-1:** Proactive Network Security	**TM-2:** Mexican Federal Security Processes	**TM-3:** Org Issues of Implementing IDS
General		**TG-1:** $(ISC)^2$ Certification	**TG-2:** Fiber Optic Vulnerability	**TG-3:** Net Sec Controls for Intrusion Prevention
Wednesday	**8:00 - 8:30**	**8:30 - 9:30**	**9:45 - 10:45**	**11:00 - 12:00**
Technical	**CONTINENTAL BREAKFAST**	**WT-1:** Computer Forensics Exposes the Crime	**WT-2:** Wireless LANs, Lessons Learned	**WT-3:** Secure Software Development Techniques
Expert		**WE-1:** How To Conduct a Cyberspace Autopsy	**WE-2:** Checkpoint NG VPN / Secure Remote - I	**WE-3:** Checkpoint NG VPN / Secure Remote - II
Manager		**WM-1:** Justify the ROI	**WM-2:** Wireless Network Security	**WM-3:** Insider Threat
General		**WG-1:** HIPAA Security Update	**WG-2:** Challenges of Enterprise Security	**WG-3:** 802.1x & Network User Authentication
Thursday	**8:00 - 8:30**	**8:30 - 9:30**	**9:45 - 10:45**	**11:00 - 12:00**
Technical	**CONTINENTAL BREAKFAST**	**HT-1:** Open Source & Incident Response - I	**HT-2:** Open Source & Incident Response - II	**HT-3:** Missing Links of an Enterprise Security Plan
Expert		**HE-1:** Network Perimeter Security - I	**HE-2:** Network Perimeter Security - II	**HE-3:** Network Perimeter Security - III
Manager		**HM-1:** Back to the Future - I	**HM-2:** Back to the Future - II	**HM-3:** Info Sec Career Guidance
General		**HG-1:** AirCERT - I	**HG-2:** AirCERT - II	**HG-3:** Application Security
Friday & Saturday	**OPTIONAL NSA IAM TRAINING COURSE** see page 6 for additional details			

12:00 - 12:45	12:45 - 1:45	2:00 - 3:00	3:15 - 4:15
LUNCH	Keynote Speaker: **Ray Semko**	**TT-4:** Best Practices for Secure Development	**TT-5:** Free Security
		TE-4: Implementing Linux Network Security - I	**TE-5:** Implementing Linux Network Security - II
		TM-4: Days in the Life of a Hacker	**TM-5:** Security Policies
		TG-4: Enhancing Security Arch w/multi-level IDS	**TG-5:** The War Against Spam

12:00 - 12:45	12:45 - 1:45	2:00 - 3:00	3:15 - 4:15
LUNCH	Keynote Speaker: **Jim Christy**	**WT-4:** Are We Ready for Cyber Terrorism?	**WT-5:** Web Application Security Risks and Concepts
		WE-4: How To Write a Security Policy	**WE-5:** Deploying an IDS Solution for Internet Hosts
		WM-4: Ethical Hacking	**WM-5:** Risks of Developing a Security Ops Center
		WG-4: Viable Information Assurance Program - I	**WG-5:** Viable Information Assurance Program - II

12:00 - 12:45	12:45 - 1:45	2:00 - 3:00	3:15 - 4:15
LUNCH	Keynote Speaker: **Rich Pethia**	**HT-4:** System & Network Hacking - I	**HT-5:** System & Network Hacking - II
		HE-4: Secured n-Tier Web Services	**HE-5:** Secured n-Tier Web Services
		HM-4: Privacy & Security Laws - I	**HM-5:** Privacy & Security Laws - II
		HG-4: Risk Management - I	**HG-5:** Risk Management - II

For details on each session, to include speaker and abstract information, see pages 7-14

Information about our keynotes is available on page 5

GLANCE AT-A-

About NEbraskaCERT Conference 2003

NEbraskaCERT, which is comprised of volunteers dedicated to information security awareness and sharing, presents the 5th annual Computer Security and Information Assurance conference in Omaha, Nebraska.

Recently the military reorganized and shifted its information operations center to the United States Strategic Command located at Offutt Air Force Base, Nebraska. This shift made Omaha the central hub for security-related matters for the Department of Defense.

NEbraskaCERT has been closely associated with Offutt since its first conference in 1999, when three Offutt Majors rallied the local community to create a conference dedicated to the free exchange of ideas on security matters. With the sponsorship of the CERT Coordination Center, NEbraskaCERT Conference (formerly CERT Conference) was born. This conference is designed for those organizations whose livelihood depends on ensuring their information remains intact and accurate. This event will be a forum whereby organizations can share lessons learned, discover what has worked for others, and immediately apply their newly found knowledge.

This year we offer 3 days of general sessions, tutorials, and activities with four concurrent tracks--Technical, Expert, Management, and General. We offer the latest information on new regulations, ethics, cutting-edge technology, and much more. New this year is an additional optional two-day Information Security (INFOSEC) Assessment Methodology (IAM) Training course for certification by the National Security Agency as an IAM professional.

"There is no security on this earth. Only opportunity." *<Douglas MacArthur>*

CISSP / SSCP Exams August 4, 2003

As an additional attraction, NEbraskaCERT is hosting the CISSP and SSCP certification exams one day prior to the conference. Anyone who sits and passes one of these exams and attends the conference will be eligible to claim CPE credits toward maintaining their certification.

CISSP

The CISSP certification identifies you as a security professional who has met a certain standard of knowledge and experience and who continues to keep his/her knowledge current and relevant to what is happening in the practice of Information Security. CISSPs must have a minimum of three years experience in one or more of the ten Common Body of Knowledge (CBK) domains. The CISSP program certifies IT professionals who are responsible for developing the information security policies, standards, and procedures and managing their implementation across an organization.

SSCP

The SSCP certification identifies you as a security practitioner who has met a certain standard of knowledge and experience and who continues to keep his/her knowledge current and relevant to what is happening in the practice of Information Security. SSCPs must have a minimum of one year experience in one or more of the seven CBK domains. The certification is targeted at network and systems security administrators, who provide day-to-day support of the network and security infrastructure.

Registration for these Exams

These exams are conducted by $(ISC)^2$.
To register, you must do so separately from any registration for NEbraskaCERT Conference 2003.
Registration information is available at www.isc2.org.

REASONS TO ATTEND

Networking Opportunities

Past attendees cite networking opportunities as the number one benefit and reason to attend this conference! Sure, there's plenty of quality speakers and sessions, but the real value comes from sharing experiences and learning from others interested and concerned with security. The schedule is set up to ensure you'll have plenty of time to meet others and make long-lasting and helpful contacts at breakfasts, lunches and breaks, giving you the opportunity to learn from other attendees, not just the speakers.

Pick Your Sessions

NEbraskaCERT Conference 2003 has arranged its sessions into four tracks; Technical, Expert, Management, and General, to give you an idea what type of session to expect before you walk in the room. However, you're not locked into a track. Feel free to mix and match the sessions you think interest you the most, regardless what track they've been categorized into.

Security Information & Solutions You Can Use

Speakers with real-world experience will discuss solutions you can take back with you and implement. Our sessions have been selected to provide you with the opportunity to achieve just the right balance between technical and management issues.

Take advantage of available Discounts

NEbraskaCERT Conference has revised its discount process yet again for this year's conference, allowing for greater savings, simply by registering by July 10, 2003. Also, after July 10th, anyone who has attended a previous CERT Conference sponsored by NEbraskaCERT, is a Full-time Student, works for the Government or holds their CISSP certification is eligible to take advantage of a $50 discount off the full conference registration. Or, if you're attending in a group of 5 or more, take advantage instead of the $100 per person discount. *See page 17 for more information.*

More Sessions per Day

This year's lineup offers an additional 4 sessions each day.

Wake up to Continental Breakfast

Continental Breakfast is provided each day you attend.

Lunch is on us!

Full course lunch buffet is included in the conference fee and provided for each day you attend.

CONTENTS:

KEYNOTE SPEAKERS

Ray Semko, Diceman of the Interagency OPSEC Support Staff

Known to many in the OPSEC and defense communities as the "DICE Man", joined the IOSS on January 18, 2000. Ray brings more than 30 years of military and government security and counterespionage experience, but he is most closely associated with his Defensive Information to Counter Espionage (DICE) briefings. He has been presenting these around the world since he initially created them for Defense Intelligence Agency (DIA) employees in 1988. Ray will be traveling for the IOSS to raise awareness of the threats to U.S. security and the value of OPSEC in neutralizing these threats.

Ray, a native of Pittsburgh, PA, joined the U.S. Army at 18 and served in Vietnam. He retired from the Army after 21 years-17 spent as a counterintelligence agent. He joined the DIA in 1988 and was the first DIA representative to the IOSS in 1989. He was also a regular speaker at the national OPSEC conferences. In addition to his counterintelligence duties, Ray has performed OPSEC assessments for the Army, Pentagon and Joint Chiefs of Staff, among others.

Prior to joining the IOSS team, Ray worked as a Counterintelligence Officer for the Department of Energy (DOE) since 1992.

At DOE, his DICE briefings were so highly requested that had his schedule permitted, he could have given one every day of the year. Ray revamps the immensely popular DICE briefing yearly to keep it fresh-and the threat information viable.

When not briefing, Ray spends time with his family in rural PA. Ray has officiated almost every sport and was once the coach of the Italian National Football team. Ray also works as a deejay in his few moments of spare time.

Jim Christy, Deputy Director/Director of Operations, Defense Cyber Crime Center

Supervisory Special Agent James V. Christy, II is the Deputy Director/Director of Operations, Defense Computer Forensics Lab, Defense Cyber Crime Center. Jim is an Air Force Office of Special Investigations, Computer Crime Investigator. As the Dir of Ops for the DCFL he has four sections with over 40 computer forensic examiners that support Major Crimes & Safety, Counterintelligence and Counterterrorism, as well as Intrusions and Information Assurance cases for the Department of Defense.

SA Christy served as the DoD Representative to the President's Infrastructure Protection Task Force (IPTF) from Sep 96 - May 98. The President signed Executive Order, 13010 on 15 Jul 96, creating IPTF to protect the Nation's critical infrastructure from both physical and cyber attacks. Prior to the IPTF, Jim was detailed to Senator Sam Nunn's staff on the Senate, Permanent Subcommittee on Investigations as a Congressional Fellow, Jan - Aug 96. Senator Nunn specifically requested Jim's assistance for the Subcommittee to prepare for hearings in May - Jul 1996, on the vulnerability and the threat to National Information Infrastructure from cyberspace. In 1986, Jim obtained some notoriety as the original case agent in the "Hanover Hacker" case. This case involved a group of German hackers who electronically penetrated DOD computer systems all over the world and sold the information to the Soviet KGB. The case was detailed in the best seller, "The Cuckoo's Egg", by Dr. Cliff Stoll. The Public Broadcast system has also produced a docu-drama on this case.

In a murder investigation in 1991, the suspect cut two floppy diskettes into 23 pieces with pinking shears. No agency was able to recover any of the data until Jim and his deputy developed a technique for less then $150. Jim was able to recover 85%-95% of the data from each piece of diskette. The suspect when confronted with the evidence, confessed, pled guilty and was sentenced to life in prison. This case was profiled on the "New Detectives" series on the Discovery Channel, 2 Jan 99.

Rich Pethia, Director, NSS Program, Software Engineering Institute, Carnegie Mellon University

Richard D. Pethia established the CERT Coordination Center (CERT/CC) in 1988 to serve as focal point for resolving Internet security incidents and vulnerabilities. In 1995, he broadened the scope of the security effort and created the Networked Systems Survivability (NSS) Program at the Software Engineering Institute (SEISM). The NSS Program ensures that appropriate technology and systems management practices are available to help computer users and systems administrators recognize, resist, and recover from attacks on networked systems. The CERT/CC continues to serve the Internet community as a part of the NSS Program.

Mr. Pethia has given various government testimonies on topics ranging from e-commerce to the vulnerability of networked systems. Some of his most notable testimonies include Internet Security Issues, presented to the U.S. Senate Judiciary Committee; Removing Roadblocks to Cyber-Defense, presented to the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information; and Information Technology-Essential But Vulnerable: Internet Security Trends as well as Information Technology-Essential But Vulnerable: How Prepared Are We for Attacks?, both presented to the House of Representatives Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations.

NSA IAM TRAINING

This year's conference offers an optional 2 days of training and certification (August 8 - 9, 2003) by Security Horizon for the National Security Agency's (NSA) Information Security (INFOSEC) Assessment Methodology (IAM) Training

What is IAM?

The IAM is a detailed and systematic way of examining organizational vulnerabilities and was developed by experienced NSA and Commercial INFOSEC assessors. NSA is providing the IAM to assist both INFOSEC assessment suppliers and consumers requiring assessments. This market was originally created by the PDD-63 (now PDD-1) requirement for vulnerability assessments of automated information systems that support the U.S. Infrastructure. In addition to assisting the governmental and private sectors, an important result of supplying baseline standards for INFOSEC assessments is fostering a commitment to improve organizations' security posture.

Individuals will be trained in the IAM so they can use their INFOSEC analysis skills along with the IAM training to provide the standardized IAM assessment service. Since the IAM is a baseline methodology, the final results of the assessment service are highly dependent on the INFOSEC and analytic skills of the assessors. For this reason it is suggested that individuals have either the proper experience or take additional INFOSEC training prior to taking the IAM course. Currently, companies and government organizations looking for outside help assessing the security posture of their information systems can choose from dozens of commercial firms that advertise INFOSEC assessment capabilities. Although these contractors all provide INFOSEC assessment services, their processes, terminology, scope and costs vary widely. The IAM course was developed for the benefit of organizations trying to obtain an INFOSEC assessment that meets their needs.

The IAM course is a two-day course for experienced Information Systems Security analysts who conduct, or are interested in conducting INFOSEC assessments of information systems. The course teaches the NSA INFOSEC assessment process, a high-level, non-intrusive process for identifying and correcting security weaknesses in information systems and networks.

Students may be eligible to receive NSA Certificate of Completion and be listed as an IAM Certified Individual on NSA's website (http://www.iatrp.com). Attendees who feel they meet the following requirements will need to submit documents proving eligibility. Security Horizon will coordinate the work experience and paperwork with NSA, in advance of the class. Submission of paperwork no later than 15 days prior to the class is highly recommended to ensure all paperwork is approved and the certification exam is issued by the NSA. However, registration may be taken up to 7 day prior to the course start date.

- Certification application to show (see http://www.securityhorizon.com/training/iam/reg.html) :
    - Contact Information
    - U.S. citizenship
    - Five years of demonstrated experience in the field of INFOSEC, COMSEC or computer security, with 2 of the 5 years of experience directly involved in analyzing computer system/network vulnerabilities and security risks.
- NSA must approve all attendees expecting to receive the NSA certificate. In order to accomplish this, Security Horizon needs completed Registration Packages from all attendees ASAP. It is HIGHLY recommended that all attendees provide their registration packets to Security Horizon no later than 15 days prior to the course start date, to assure completion of NSA processing. Otherwise, no guarantee of NSA review and approval can be made.

To qualify for an IAM certificate of completion, students must:

- Gain qualification approval from NSA (coordinated by Security Horizon);
- Attend all of the two-day class;
- Demonstrate an understanding of the IAM through group exercises and class discussions; and
- Obtain a passing grade (at least 70 percent) on the IAM test.

Direct any questions to Security Horizon at info@securityhorizon.com **or call** 719.488.4500

REGISTER TODAY AND SAVE UP TO $400!!!

Pricing: Standard.....$1200

Early Registration Discount (If registered and paid NLT July 8, 2003).....-$100

Affiliation Discount (ISSA, ISACA, InfraGard, Military, Fed/State Gov't, Law Enforcement).....-$100

NEbraskaCERT Conference Attendee Discount.....-$200

TT-1:
Introduction to Forensics 101
Joseph A. Juchniewicz, Americredit

The ability to have a valid, reliable medium for information transfer has grown from a select group of universities, into the juggernaut of today's information highway. As with any kind of technology, some individuals may corrupt the system and use it for malicious or illegal activities. These threats need to be examined to discover if they are internal "employees" or external "hackers". To create a defense against these threats, today's security professionals require the ability to not only gather information, but to be able to present the data to management, lawyers or even a judge and jury at a level that they can understand and make valid conclusions if called upon to do so. In the current environment computer forensics is in its' infancy, but is starting to be a widely used tool. Its importance is starting to take shape and be recognized, for its importance and within the next five years, will be an integral part of any computer investigation.

TT-2:
Methodology for Incident Prevention & Response (MIPR)
Robert Bagnall, CSC's Defense Core Team

The MIPR is a process for standardizing how contractors deliver CERT services at customer locations. The analogy is that McDonald's became a global American icon by making sure that the burger you order in California tastes the same as the one you order in Nebraska - or Washington, DC. You expect the same level of service delivery everywhere you see their sign, and it should be no different with CERT operations delivered by the same company. Through a series of steps with consistent processes and supportive technologies [such as asymmetrical agent defenses], Bagnall demonstrates how to standardize CERT delivery, regardless of customer, as well as how to provide a consistent level of skilled personnel to each operation.

TT-3:
Process Capability for Information Assurance: Security Engineering Practices for Better Bottom-Line Results
Matthew O'Brien, SAIC

Assessments of an enterprise's security posture have historically taken a balance sheet approach: listing discrete technical strengths and weaknesses at a specified point in time. This emphasis often obscures the issue of an enterprise's ability to consistently execute security-engineering practices that prevent, identify and remedy security vulnerabilities. Capability maturity models provide a framework to build process capability. For Information Assurance, process capability maturity is the heart of the matter--the robustness of an enterprise's security posture is ultimately dependent upon consistent execution of security engineering practices.

TT-4:
Best Practices for Secure Development
Ron Woerner, Nebraska Department of Roads

The National Strategy to Secure Cyberspace says, "An important goal of cybersecurity will be the development of highly secure, trustworthy, and resilient computer systems." But how do we do that?! This session will discuss general security guidelines for developers and will explain methods of security and software engineering. The presenter will give specific tips on secure programming that will benefit developers, program managers and project leaders alike. You will leave this session understanding how to develop your own methodology for creating secure code to help meet this critical goal of the Cybersecurity Strategy.

TT-5:
Free Security
Ron Woerner, Nebraska Department of Roads

Security is unique in the IT world; many security tools, documents, and programs are available for free (or very little cost). This presentation will show many of the free security tools available on the Internet. These tools can be used for vulnerability assessments, penetration testing, intrusion detection, incident response, and security management. Other resources include policies and procedures, awareness programs, education and training. All of it is available at little or no cost. So if your security program is strapped for cash, you can use these resources to help you in your day-to-day security activities. (Shh, don't tell the vendors…)

WT-1:
Computer Forensics Exposes the Crime
William Siebert, Guidance Software

The use of computers to perpetuate cybercrime is a never-ending race of threats and responses. Almost all crimes affecting businesses involve a computer used for e-communication or as the actual means of committing the offense. Many types of crimes such as intellectual property theft, fraud, identity theft, copyright piracy, not to mention trafficking of illegal digital images and content, involve the malicious use of information technology. With the ability to expertly investigate and preserve data, exposing digital traces of unthinkable crimes, many of today's criminals have been removed from our communities.

WT-2:
Wireless LANs, Lessons Learned
David Borden, ACS Defense

After hearing the session, the student should understand the various relevant IEEE Protocols dealing with wireless networking. The student should be able to describe good wireless network security practices

and know why they are important. They should be able to list adversaries' attacks on the wireless network and describe the defense against each attack. The student should be able to describe wireless intrusion detection system techniques and know how they differ from wired systems. They should leave the session with a feeling that they could employ wireless networking without fear of hacker attack using the techniques enumerated.

WT-3:
Secure Software Development Techniques

T Steven Barker, Raytheon

This presentation makes the case for software designers and developers to build secure principles into software from the beginning. Security requirements should be built, budgeted, and scheduled into the project development just like all other requirements. The Presentation Objective is to provide basic concepts for improving software security, highlight the major coding mistakes that lead to insecure software, and present the case for secure design.

WT-4:
Are we ready for CyberTerrorism?

Staniford Stuart, Silicon Defense

How do we prepare ourselves for the potential impact of a cyberterrorist threat? What types of security approaches will protect us? Many factors such as new government regulations and legislation, legal liability, the cost of business disruption, cyberterrorism and the September 11th terrorist attack, are moving businesses into new areas of responsibility. Navigating the labyrinth of security solutions and recent legislation is crucial for IT professionals in today's networking environment.

WT-5:
Web Application Security: Risks and Concepts of Security

Kris Drent, Security PS, Inc.

Drawing from years of field experience and research, this eye-opening session puts web applications security in perspective and presents an overview of the kinds of vulnerabilities and risks that are prevalent in web applications today. The topics of this event include: application of information security principles, web application risks and vulnerability examples, network/host security versus web application security, and first steps toward mitigating web application security risk. This seminar is designed for anyone actively involved with designing, developing, auditing, or deploying web applications within their organization.

HT-1, HT-2:
Open Source and Incident Response, Parts I & II

Joe Loftshult, InteliData Technologies

When you know, or suspect, that one or more of your systems has been compromised and you want to investigate the incident, how do you do it? You can buy a commercial product (hardware and/or software) that will assist you in the incident response and/or forensic analysis process, but why spend thousands of dollars on such products when you can achieve the same results using open source tools. The open source community has provided many terrific tools ranging from the standard Unix/GNU tools to toolkits such as TASK to bootable, all-inclusive toolkits such as F.I.R.E. This presentation will describe some of the tools available in the open source world, with an emphasis on the F.I.R.E. (Forensic and Incident Response Environment) toolkit. This presentation is targeted at those who are in positions in which they may need to respond to security incidents and don't want to spend a fortune putting together a good "jump kit."

HT-3:
How To Identify The Missing Links In Your Enterprise Security Plan

Charlie Young, Unisys

Recent IDC research on public and private enterprise data security reveals an alarming lack of appropriate security standards, as well as a lack of independent industry benchmarks to evaluate security policies that are in place. In this presentation, the speaker will discuss the critical need for enterprise security planning to ensure that all business processes, systems and data are protected against unauthorized breach or disruption, man-made or otherwise. He will describe the essential components of a strategic comprehensive plan that encompasses all physical, operational, cyber, and financial aspects of enterprise security. This session provides a framework for achieving a zero-gap security plan that meets the ISO 17799 industry standard, and that integrates security best practices into all organizational processes and policies.

HT-4, HT-5:
System and Network Hacking, Parts I & II

David Askey, TechNow, Inc.

This two-hour tutorial exposes the strategies and attacks of the hacker. Question and answer session follows the tutorial. Attendees do not just get lectured on vulnerabilities and exploits, but see hands-on demos of network attacks utilizing systems, routers, and switches. This inspires the attendee to really think about their enterprise implementations. The specific attacks demonstrated are ARP spoofing, switch attacks, router attacks, session hijacking, and the effects of network visibility in viewing file, web traffic displayed in a browser, and email. Also a step-by-step demo is given on how Trojans and backdoors that circumvent Firewalls and Router access control lists are deployed. Then we'll discuss how the backdoor Trojans are used to deploy agents that perform the network attacks. The technical process of the attacks is discussed prior to each demo and live packet traces are displayed during the demo.

TE-1:
AI Techniques
Steve Nugen, NuGenSoft

Models and methods associated with machine intelligence can be leveraged to create more powerful InfoSec attacks that discover and exploit vulnerabilities, adapting to evade detection. These same methods can also be leveraged for stronger assessments, smarter detection, and adaptive countermeasures. The presenter will review published research in this area and some of his own thoughts on the subject.

TE-2:
MVS (z/OS) Security Issues
Steve Wiggin, Mutual of Omaha

An overview of the MVS (z/OS) operating system and what all those acronyms mean, like APF, SVC, SMF, and TSO. This session will give a basic description of the MVS environment and present some issues that, as a security professional, you will probably want to look into when you get back to your company.

TE-3:
Implementing Enterprise Information Security
Dave Young, West Interactive Corporation

In this session, Dave will discuss InfoSec from a high-level management perspective in a general sense rather than focusing on one particular technology, policy, or control. He will present the importance of end-to-end security of an organization and how to identify and implement the appropriate levels of security. Additionally he will discuss strategy behind identifying and managing risks that are a key factor in determining areas of focus. Dave will also discuss staffing and budget as well as ROI and its importance in the continued support and success of the overall initiative. Finally the business side of InfoSec; the importance of understanding the business and customizing security to meet its needs as well as the needs of clients; and utilizing InfoSec as a business enabler.

TE-4, TE-5:
Tutorial & Case Study in Implementing Linux Network Security, Parts I & II
Oskar Andreasson

In the first session Oskar will bring into focus a brief overview of iptables and IP system controls (ipsysctl) structures later used in the case study. Iptables is a set of programs and applications used to control the firewalling capabilities of the linux kernel, or netfilter as it is also called, while ipsysctl is a set of structures inside the kernel that is possible to set during runtime of the Linux OS. Both of these give tremendous power and possibilities when setting up Linux security properly. Additionally, he will look at different ipsysctl's, such as the IP forwarding, reverse path filters and garbage collection thresholds available through ipsysctl at runtime, as well as how the iptables applications work among other things. During the second part of the tutorial he will take a look at a case study, where students set up a webserver with connections to databases and an application server both on the local host and on other hosts on a separate network. Oskar will also discuss decisions and different possible paths to take.

WE-1:
Computer Forensics - How to Conduct a Cyberspace Autopsy
Doug Conorich, IBM Managed Services

In today's network-centric world, where technology and business are converging, any disruption to the flow of information can be devastating. More and more companies are becoming e-businesses. If someone were to breach the security of your system, would you be ready? Are you prepared to track this perpetrator to find out what he accomplished during this breach? What will you do now that you have the evidence? Computing environments need to address many protection issues where keys, locks and fences just are not enough. Mr. Conorich will show step-by-step how a break in can be discovered and how the hacker can be tracked through the system. He will discuss tricks hackers use to prevent discovery and what you can do to thwart them. Additionally, he will discuss how a company can handle incident management and some of the legal considerations a company must consider when investigating an incident.

WE-2, WE-3:
Checkpoint NG VPN/Securemote, Parts I & II
Barry Cooper, FishNet Security

In this session, Mr. Cooper will demonstrate Check Point remote access solutions. These solutions enable teleworkers to securely connect to corporate resources. Check Point provides client options to meet the needs of any organization. Mr. Cooper will also discuss such things as encryption, data authentication, personal firewalls, secure configuration verification, and advanced management.

WE-4:

How to Write a Security Policy

Doug Conorich, IBM Managed Services

In the past business managers have regarded computer security as something that doesn't have to concern them. However, recent events such as the continuous attack by viruses, network worm invasions and high school pranksters have increased their awareness and concern. If someone were to breach the security of your system today, would you be ready? Are you prepared to track this perpetrator to find out what he accomplished during this breach? What will you do now that you have the evidence? These and many other questions to be answered and they need to be answered before something happens to you. Today's computing environments need to address protection issues where keys, locks and fences just are not enough.

WE-5:

How to Deploy an IDS Solution for Internet Hosts

Doug Conorich, IBM Managed Services

Understanding how to deploy an Intrusion Detection System to protect your Internet facing hosts can be a real challenge. IDS can collect huge amounts of data from their daily operations. Mr. Conorich will discuss how to choose an IDS for your organization and how to deploy it to the best advantage. He will explain both network-based and host-based IDS solutions, explaining the pros and cons of each and how they can be best deployed to work together. Mr. Conorich will address alarm filtering and response escalation procedures. New correlation methods will be discussed.

HE-1, HE-2, HE-3:

Network Perimeter Security, Parts I, II & III

Marty Gillespie, Haverstick Government Solutions

The learning objective of this tutorial is to teach the basic fundamentals of Network Perimeter Security including perimeter fundamentals, components and design. This includes: Fundamentals, Firewalls, Security Policies, Routers, Intrusion Detection Systems, Virtual Private Networks, Host Security, Design Fundamentals, Architecture, VPN Integration, Performance Issues, and Sample Designs.

HE-4, HE-5:

Secured n-Tier Web Services - Case Study, Parts I & II

Matthew Marsh, Paktronix Systems LLC

In these sessions we expose in gory detail the design, planning, and implementation of a secure n-tier web services environment. The environment discussed went into production in March of 2003. It consists of a traditional multi-server distributed system designed and built with confidentiality, integrity, and authentication fully incorporated from the beginning. We expose and illustrate actual security practices running within the context of the system and discuss the real world tradeoffs needed to implement usability. The first session covers the design and planning of the connectivity and security matrix including software selection and design goal tradeoffs. The second session covers the actual implementation with discussion of operating system realities as versus ideal security and interoperability. Where applicable, we illustrate the parametric fitness of the system for consideration under ISN certification structures.

TM-1:

Proactive Network Security

Fred Kost, nCircle

Security is on the minds of all top executives and protecting corporate digital assets has surged to one of the key business objectives. Security vendors tout silver bullet solutions, yet Nimda, Code Red and Slammer consistently prove otherwise. Many companies and government institutions implement reactive security strategies and technologies that are difficult to manage and often ineffective. This session uses case studies to delve into corporate successes and failures in identifying and addressing network vulnerabilities before they jeopardize business continuity.

TM-2:

A Methodology to Implement, Operate, and Maintain an Information Security Process

Leonardo Garcia, Intelematica

The main objective of this session is to share with the audience the experience at the Mexico Federal Government projects. This session will cover implementation, operation, and maintenance of information security processes and will explain the methodology and how this methodology has fundament on an strategic, tactic and operative program.

TM-3:

Organizational Issues of Implementing IDS

Shayne Pitcock, First Data Corporation

Companies are aware of the need for a firewall to deny unauthorized access, computing hacking, or intrusions to their computing systems. Companies may also be aware of the need for Intrusion Detection Systems (IDS). The company that wishes to implement IDS tools must understand that installing the IDS tools is only 20% of the effort. The remaining 80% of the effort to implement IDS tools requires that a company must work through issues identified in this session.

TM-4:

Day in the Life of a Hacker

Michael Endrizzi, InterSec

"Day in the Life of a Hacker" is an interactive introduction to the techniques of Internet hackers and the serious dangers they pose to organizations. This interactive presentation designed to be understood by the CEO, technical workers, or your everyday employee, challenges the audience to play the roles of a hacker versus security analyst in a game of measures, attacks and countermeasures. The audience attempts to identify defenses as the hackers work to find these major weaknesses. Highlights include a detailed analysis of buffer overflow and Malicious Mobile Code (Java/ActiveX) attacks that have crippled the Pentagon and Microsoft.

TM-5:

Security Policies: Your First Line of Defense

Bruce Hartley, Privisec

The foundation of a successful information security program is a strong security policy. Without one, your company's systems are more vulnerable to attack, both internally and externally. The initial policy must also be continually reviewed, updated, and communicated to ensure it addresses your changing business needs and/or regulatory requirements, such as the Gramm-Leach-Bliley Act and HIPAA. An equally important part of an effective security policy is the development of implementation standards, which are designed to translate the policy into operating system-specific configuration guidelines. These guidelines ensure that IT professionals can easily implement the policy for each operating system on the network. This session will address the basic steps of developing an enterprise-wide security policy.

WM-1:

Justify the Return on Investment

Chris Shepherd, ICCT Corp

Security investment is hard to quantify. The need is known, the impact is real, justifying it ahead of time is difficult. This session shows how to use business defined return on investment as a core and how to use realistic extrapolations to determine impact and loss deference of investing in appropriate security.

WM-2:

Wireless Network Security: Technologies, Guidelines & Management

Steve A. Rodgers, Security PS, Inc.

This informative session will discuss current wireless network technologies focusing on the security features and benefits of each. Implementation guidelines as well as management issues will also be covered. The topics of this session include: Wireless Network Technology Overview, Wireless Security Technologies, Guidelines for Secure Wireless Implementation, Management Issues, and Wireless Security Resources.

WM-3:

The Insider Threat - Are You Safe From Internal Attack?

Bruce Hartley, Privisec

Most companies recognize the need for network security and continually focus on maintaining adequate protection. Many have taken the steps necessary to safeguard their systems from external attacks. Often, however, these same companies overlook internal security despite the fact that a significant percentage of computer abuse stems from internal problems. Because an insider already has physical and logical access to the system, an understanding of what data is sensitive, and possibly an understanding of the security controls, the potential for misuse is very high. This oversight can unnecessarily expose a company to not only internal threats, but also successful penetration

when internal attacks occur. These vulnerabilities are easily preventable when strong internal security is maintained. This session will address the importance of protecting your organization from internal attacks, as well as provide information on how to improve your internal security.

WM-4:
Ethical Hacking: The Value of Penetration Testing
Bruce Hartley, Privisec

For competitive businesses, the goal of technology is to create competitive advantages. Today's powerful computing and networking environments create unlimited opportunities for innovative new customer services, increased employee productivity, and higher profitability. However, all the benefits of advanced technology can disappear in an instant if the system is not secure. As a company's dependence on enterprise computing and network systems increases, so does its dependence on security, data integrity, and reliability mechanisms. Unfortunately, computer crime and abuse is a serious is on the rise. One of the biggest reasons firms are vulnerable is because they have NOT established and implemented a formal security policy. As a result, their systems are NOT consistently configured and weaknesses are common. The session will cover the concepts and the process of both internal and external penetration tests.

WM-5:
Risk Considerations in Developing Security Ops Center
Ed Covert, ICS Corp

The nature of the threat to organizational infrastructures is evolving. The threats are becoming more complex and affecting systems at a higher frequency. Consequently, the mitigation strategies required to counter these threats must evolve as well. As more organizations begin to better comprehend this threat evolution, they must migrate their countermeasures and controls from a heterogeneous management strategy to a homogenous and integrated one. One of the most cost-responsible outgrowths of this strategy is the development and implementation of a Security OperationCenter (SOC) to coordinate the security management of the enterprise. There are several key considerations organizations must examine when attempting to coordinate potentially disparate operations and technologies. Using the Information Assurance Life Cycle (IALC) methodology, this presentation will discuss these considerations.

HM-1, HM-2:
Back to the Future, Parts I & II
John Casciano, SAIC

Mr. Casciano's presentation will draw historical parallels between the role played by Omaha and Nebraska during the Cold War and its new role in helping America cope with Twenty-first Century threats and vulnerabilities. Nebraska's position as both a major financial and security center as well as STRATCOM's new missions place Omaha and Nebraska at the forefront in a newly evolving concept of National Security. Nebraska, Omaha, STRATCOM, and its predecessor Strategic Air Command have a long history of thinking and acting globally, and that is exactly what is required in the first part of this century. Non-kinetic operations in cyberspace, both defensive and offensive, are a central part of Nebraska's future. The presentation will include a view of lessons from the past and their implications for the future as the regional players go forward.

HM-3:
Information Security Career Guide
William Sieglein, Fortrex Technologies Inc.

This tutorial provides: the history of the field and names some successful professionals, an outlook, a description of the current job titles/positions in this field, the minimum skills, knowledge and experience required to be successful in an information security career, a description of the minimal education and training and well as experience required, information on how to decide on goals and how to establish a strategy and tactics to achieve those goals, insight on improving your overall chances of succeeding in the field of information security, and case studies of various security professionals who have succeeded using diverse approaches.

HM-4, HM-5:
Privacy & Security Laws Parts I & II
Kate Wakefield, Costco

The legal landscape for Privacy legislation within the United States is a rapidly changing environment. Recently enacted legislation such as the Gramm-Leach-Bliley Act, and the finalization of HIPAA Privacy and Security rules, combine with existing sector-specific privacy rules to provide a highly regulated environment with serious civil and criminal penalties, as well as increased legal liability. Information security professionals need to be informed about legislation that applies to their organization so that they can implement appropriate policies, procedures, and security architectures. This tutorial will provide an overview of the relevant legislation, the types of information that must be protected in each state, and pointers to best practices for securing information.

GENERAL TRACK

TG-1:
(ISC)^2 Certification
Lynn McNulty, (ISC)^2

This session explores the professional certification process. Professional certification for information security careerists is a matter of individual choice. However there are several factors that now appear to be tipping the scale in favor of CISSP certification. First and foremost is the fact that the profession of information security is now recognized as a separate and distinct career field. Within the federal government, this fact is reflected in the President's Executive Order of October 2001 and the identification of information security as a defined specialty within the 2200 IT Job series announced by OPM in 2001. Secondly, Information Security is now seen as vital to the nations well being and to the effective functioning of the federal government. The establishment of the Office of Cybersecurity as part of the National Security Council staff structure is witness to this Twenty-First century reality. Finally, the strategic nature of the government's information security problem is now coming into focus. The OMB report on GISRA implementation correctly identified information security as a management issue, not a technical problem. The CISSP certification reflects an individual's ability to address security issues in a larger organizational context, as the certification emphasizes theory and concepts, rather than product specific knowledge. CISSP certification is an important investment in an increasingly important career field.

TG-2:
Fiber Optic Vulnerability
Mark Gross, NeSTronix, Inc

A major new threat to our national security and our national information infrastructure has been uncovered. Fiber optic networks form the backbone of our nation's economic well being. In fact, fiber optic networks form the communications infrastructure backbone for both government and industry. Recent technology advances have resulted in the ability to easily and inexpensively tap a fiber optic cable without detection. Our government's most secret and valued information is now exposed to those wishing harm to our nation. Our nation's military, intelligence, law enforcement, banking, and financial services information are now vulnerable. During this session you will learn how to counter this threat.

TG-3:
Network Security Controls for Intrusion Prevention
Greg Brock, Florida Association of Court Clerks

Many organizations face the challenge of balancing operational efficiency against network security controls. Problems arise when Operational Staff ignore or attempt to bypass the security controls that are in place on a network. This lack of ongoing control causes downtime and misuse of network resources. Many of the problems in information systems begin because administrators have put little or no network controls in place. This presentation will address the tools and techniques necessary to implement strong network controls.

TG-4:
Enhancing your Security Architecture with Multi-Level IDS
Mike Hrabik, Solutionary, Inc.

One of the largest challenges security professionals face today is deploying an enterprise security solution across large complex, interconnected, multi-layered network environment. During this presentation we will discuss how to look beyond single-system security solutions to a multi-level intrusion detection system through event correlation and analysis. We will also discuss how to make Intrusion Detection Systems scalable, reliable and customized for your environment.

TG-5:
The War Against Spam
Christopher Baker, MCSE

The war against unsolicited commercial e-mail is one of the Internet's hottest issues. Millions of hours are wasted by the task of deleting unwanted e-mail from inboxes. Spam also places unwanted loads on e-mail systems and bandwidth. And the most dangerous spam includes spyware that transmits information from the unknowing recipient's machine back to the sender. Unless you have no Internet connectivity at all, you are in the war against spam. In this one-hour presentation, Chris Baker will show the methods spammers use to harvest e-mail addresses and how to block the "harvest bots." He will feature techniques end-users can use to fight back against spam and will explain why simply ignoring them is not enough. He will discuss effective and ineffective methods that system administrators are employing in the war against spam. He will also demonstrate that sometimes the cure is worse than the disease.

WG-1:
HIPAA Security Update
James O'Connor, Baird Holm Attorneys at Law

As a security professional you may be asked to conduct an "Evaluation" of a security program as required by the final HIPAA Security regulations. What should this "Evaluation" look like? What liability do you undertake if you perform one in-house? What if you do it for a client? This presentation will address this issue and the changes between the preliminary regulations and the final rule. It will explore what those changes really mean and what pitfalls are lurking in the final regulations.

WG-2:
Challenges of Enterprise Security
Conrad Herrmann, Zone Labs
This session addresses the challenges of enterprise security, focusing on how to use comprehensive policy enforcement to impose strict security guidelines for every point on the network, without hampering employee productivity and efficiency.

WG-3:
802.1x and Network User Authentication
Doug DeYong, Enterasys
This session will begin with an overview of the 802.1x standard and introduce where it is used with in the network for authentication. We'll then follow-on with the various types of authentication methods and ways of exchanging credentials. We'll discuss some merits and demerits of each as well. This will lead us to 802.1x implementation and a cookbook for tasks required for a good setup. Finally we'll rap up with some special things you can do with policy once you know who the user is via 802.1x and how we can implement that policy on a variety of devices.

WG-4, WG-5:
Building a Viable Information Assurance Program, Parts I & II
Harry Bouris, Sumaria
This session will provide the student with the requisite knowledge and tools to develop a viable Information Assurance Program. First, will be a brief discussion of US Statute. Next the workshop will cover corporate policy including usage, passwords, screen savers, what not to put in a policy and the importance of a signed acknowledgement statement. Next the workshop will discuss personnel security including background checks, adverse conditions, etc. Additionally physical security will be explored, including the importance of low/no cost elements like locked doors, controlled entry, and visitor sign in. This session will also cover having an awareness program, network policy, continuity of operations plan and system accreditation.

HG-1, HG-2:
AirCERT, Parts I & II
CERT Coordination Center (Invited)
The AirCERT project involves the placement of Internet-based security event sensors on the networks of various organizations attached to the Internet. These sensors will log locally selected information on detected security events and anomalies to both a local database and a central database located at the CERT/CC. The CERT/CC is currently developing a prototype of this system using open source and low-cost components. They hope to see this concept expanded so that various types of sensors from many vendors will be able to interoperate with the processes and databases developed for managing and analyzing security event information. This tutorial will address how CERT/CC envisions this concept taking root, background and motivation, project description, Snort XML plugin, and Analysis Console for Intrusion Databases (ACID).

HG-3:
Application Security
S. Ramesh, Razorwire Security
This session is intended for a business audience, and technology will be discussed in terms of its impact on business and the bottom line. Application Security protects server-side applications from attacks that target application weaknesses. Application-based attacks use specialized attack data packets sent within legitimate communications such as web requests. Because the request itself is legitimate, firewalls, server hardening, and other network defenses are inadequate against this type of attack. This session covers strategies to protect you from application weaknesses. We will discuss different strategies that you can use to protect yourself from attacks that target your server applications. These include strategies that are applicable for generalized protection behind your network perimeter, and strategies to limit vulnerabilities of specific types of applications, such as databases and application servers. Additionally, we will discuss some real life situations in the financial, enterprise software, and communications industries, where application security greatly enhanced the security posture of customers who discovered weaknesses in their systems.

HG-4, HG-5:
How to Calculate Risk in a Practical Manner, Parts I & II
Gary Bahadur, Foundstone
Organizations now understand that addressing a threat or vulnerability is not a long-term solution for protecting a large enterprise. What has been lacking in security applications is a Risk rating and analysis methodology. A threat to the organization should be quantified and the impact to the organization measured. Based on measured Risk, resources can be allocated more efficiently and effectively. By addressing threats and vulnerabilities based on Risk, faster and more cost effective solutions can be put in place. Once you understand where the Risk is, you can quantify it and develop a model for rating threats based on the possible risk of damage or destruction to the organization. By providing a baseline checklist for security processes, procedures and products, the organization can have one common criterion for evaluation of their Risk and use numeric measures to track progress towards a secure environment.

PATRON SPONSORS

NEbraskaCERT

PRINCIPAL SPONSOR

SAIC An Employee-Owned Company From Science to Solutions®

GENERAL SPONSORS

BAE SYSTEMS

Carnegie Mellon Software Engineering Institute CERT® Coordination Center

Sumaria

Solutionary reliable, responsible e-security

NuGenSoft

First National Technology Solutions

Paktronix Systems Network Security Solutions

GIFT SPONSORS

FISHNET SECURITY.COM

Reboot The User

About Omaha, Nebraska

Omaha is a dynamic metropolitan area of 700,000 with over 18,000 businesses. Omaha has long been known as a destination where visitors can have fun and not have to worry about budget constraints. Some of the Midwest's finest visitor attractions are located here. This is a city with a rich past, vibrant present and exciting future. There is always something to see or do in Omaha. The community has a wide array of parks, museums, historical sites and entertainment areas that are open year-round. A number of activities are free or cost only a few dollars. Many of these attractions are unique to the Omaha area.

continued..

About Omaha ..continued

Omaha is the corporate headquarters and main residential campus of Boys Town, which continues to provide care to hundreds of children and is open to the public. The Henry Doorly Zoo has won numerous awards and is one of the region's most popular attractions. This world-class zoo sits on 130 acres and is home to over 600 species and more than 18,600 specimens. Among the numerous exhibits are the world's largest indoor rainforest, an aquarium complex that includes a walk-through tunnel, the second largest free-flight aviary, and the Desert Dome, where three diverse desert environments have been re-created under the world's largest glazed geodesic dome.

The Omaha metropolitan area is also an active and diverse arts and entertainment base for the region, attracting artists from around the world. There is a professional symphony and opera company, as well as dozens of theaters and performing arts venues. The arts community welcomes everyone to participate in cultural activities.

Omaha Area Attractions:

The Old Market / Downtown
Henry Doorly Zoo; Desert Dome, Aquarium, Indoor Rainforest & IMAX 3D
Joslyn Art Museum
Strategic Air Command Museum
General Crook House
Mallory Kountze Planetarium
Riverboat Casinos
Heartland of America Park and Fountain
Omaha's Rosenblatt Stadium, Home of the College World Series
Durham Western Heritage Museum
Boys Town USA
Gerald Ford Birthsite
Omaha Botanical Gardens
River City Star

Airline and Hotel Information

Airline Travel to Omaha

Save up to 10% on airline travel by booking your flight with Midwest Express, the official airline carrier for NebraskaCERT Conference 2003. (use Convention/Meeting No:CMZ1254)
For more information or to book your flight, visit: http://www.midwestexpress.com/conventions

Hotels

The following hotels are located in close proximity to the Scott Conference Center:

Doubletree Guest Suites (402) 397-5141
7270 Cedar Street
Omaha, NE 68124

Quality Inn (402) 397-7137
2808 S. 72nd Street
Omaha, NE 68124

Super 8 (402) 390-0700
7111 Spring Street
Omaha, NE 68106

Hampton Inn (402) 391-8129
3301 S. 72nd Street
Omaha, NE 68124

Homewood Suites (402) 397-7500
7010 Hascall Street
Omaha, NE 68106

Holiday Inn (402) 393-3950
3321 S. 72nd Street
Omaha, NE 68106

Clarion (402) 397-3700
3650 S. 72nd Street
Omaha, NE 68124

Travelodge (402) 391-5757
7101 Grover Street
Omaha, NE 68106

Red Lion (402) 397-7030
7007 Grover Street
Omaha, NE 68106

REGISTRATION INFORMATION

NEbraskaCERT Conference 2003 Registration Fees:

Early Bird NEbraskaCERT Conference Registration (before July 10, 2003) = **$545***

* *Due to the economic advantage of choosing the Early Bird discount, all registrations received and paid before July 10, 2003 will automatically receive the Early Bird discount. Discount may not be combined with any other discount.*

NEbraskaCERT Conference Registration (after July 10, 2003) = **$695**

Discounts:

Alumni / Full-time Student / Government / CISSP Discount = **$50****

Discount for a group of 5 or more = **$100 per person*****

** *Alumni discount available to registrants who attended past CERT Conferences presented by NEbraskaCERT. To qualify for Full-time Student, Government, or CISSP discount, attendee must show valid ID during Conference Check-in. Each registrant may only claim 1 (one) of the discounts in this category for a maximum of $50. Discount may not be combined with any other discount.*

*** *Discount given only to groups who submit five or more registrations AT THE SAME TIME. Discount will not apply unless all registrations are received together. Discount may not be combined with any other discount.*

Conference Fees Include:

- Attendance to Sessions, Tutorials, and Panels for each day of registration
- Full Lunch
- Continental Breakfast and Afternoon Refreshments
- Printed Materials for sessions you attend*
- Access to electronic copy of presentation materials**

The Conference Schedule is subject to change due to availability of speakers and presentation materials. NEbraskaCERT may not be held liable for changes to the schedule beyond its control.

* When available, presentation materials will be available to attendees at the beginning of each session. A limited quantity of copies will be available, therefore availability will be on a first come, first served basis.

** Updated presentation materials will be available on the conference website as soon as presenters provide them to conference staff. Not all presenters provide their presentations for publication.

***** ATTENDANCE IS LIMITED TO FIRST 200 PAID REGISTRATIONS - REGISTER TODAY *****

Register by Mail:

NEbraskaCERT Conference
P.O. Box 825
Bellevue, NE 68005-0825

Register on the Web at:

http://www.certconf.org/register.php

Fax Registration form to:

(402) 551-9819

Cancellation Policy:

All cancellations must be made in writing and sent by mail using the address or fax # listed. All written cancellations must be received by July 5, 2003 and a $50 administrative fee will apply. All refunds will be processed within 30 days following the conference. If you cannot attend, you may transfer your registration to another employee within your company, provided notification of such change is made as early as possible.

REGISTRATION FORM

Name:_____
LAST *FIRST* *M.I.*

Title:_____

Company:_____

Address:_____
STREET ADDRESS / P.O. BOX *MAIL STOP / FLOOR*

_____
CITY *STATE* *ZIP / POSTAL CODE*

Phone:_____ **Fax:**_____

E-mail:_____

I would like my name to be included on the NEbraskaCERT Conference mailing list, YES____ or NO____

Payment Information:

NEbraskaCERT Conference, August 5-7 Base Price:	$695	$_____
Early Bird Discount (must register before July 10, 2003):	-$150*	$_____
Alumni / Full-time Student / Government / CISSP Discount:	-$50**	$_____
Discount for a group of 5 or more ($100 per person)	-$100**	$_____
	TOTAL:	**$_____**

See Registration Information Page for qualification requirements and restrictions

Payment Method:

_____Check, *enclosed payable to NEbraskaCERT Conference*

_____Purchase Order, *P.O. Number:* _____

_____Credit Card - Type: AMEX:____ VISA:____ Mastercard:____ Discover:____

Credit Card Number:_____Expiration Date:_____

Card Verification Value (last three digits of the number located on the signature strip):_____

Cardholder's Name:_____

Cardholder's Address:_____Zip Code:_____

Cardholder's Signature:_____

-- See Registration Information Page for Cancellation Policy --

NEbraskaCERT Conference
P.O. Box 825
Bellevue, NE 68005-0825

PRSRT STD
U.S. POSTAGE
PAID
BELLEVUE, NE
Permit No. 25

TO:

NEbraska CERT Conference 2003
Computer Security and Information Assurance

http://www.certconf.org