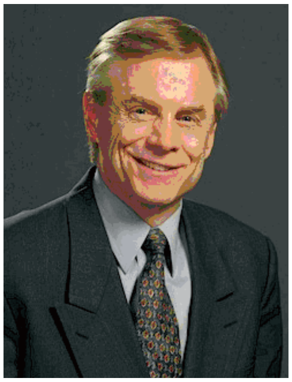
Homeland Security

DHS Cyber Preparedness eNewsletter

Volume II, Fall 2006

Contents



Andy Purdy
Acting Director,
National Cyber Security Division/US-CERT

A Message from the Acting Director

As many of you know, I will be leaving NCSD/US-CERT in October. In my two years as Acting Director, in collaboration with our stakeholders, we have made significant progress in advancing our two overarching priorities: the implementation of an integrated risk management program and the enhancement of the national cyberspace security response system.

We have established NCSD/US-CERT as the federal government's focal point for cyber security coordination and preparedness and significantly enhanced the situational awareness, analytic, and incident response capabilities of US-CERT. We established the IT Government Coordinating Council and assisted in the creation of the IT Sector Coordinating Council to facilitate the coordination of policy development and infrastructure preparedness planning.

We helped to create the National Cyber Response Coordination Group (NCRCG), the principal interagency forum to coordinate intra-governmental and public/private preparedness efforts to respond to and recover from large-scale cyber attacks.

Using a risk-based approach to cyber security, we have focused our efforts on programs addressing current vulnerabilities, such as our Control Systems Security Program and our Internet Disruption Working Group, as well as programs focused on preparing for current and future cyber security challenges such as software assurance, training, and education.

We have also helped to raise public awareness of the importance of cyber security because if we can encourage all Americans to maintain safe online practices, we can reduce our collective cyber risk.

As a result of these efforts and our collaborative public and private partnerships, I believe we are more prepared for a coordinated and effective response to cyber attacks.

I would like to extend a warm welcome to Greg Garcia, the Department's first Assistant Secretary for Cyber Security and Telecommunications. As many of you know, Greg has worked very closely with NCSD in his role on the IT Sector Coordinating Council and the National Cyber Security Partnership, and I share the confidence of our stakeholders that he will be able to significantly further our progress on all fronts.

I would like to thank the dedicated staff of NCSD/US-CERT who work tirelessly day in and day out to protect our critical infrastructure. I would like to thank DHS leadership, especially Secretary Chertoff, Deputy Secretary Jackson, and Under Secretary George Foresman, for their commitment to cyber security. And I would like to thank you, our dedicated private and public sector partners, for the time, energy, and resources you have dedicated to enhancing the cyber security of our great nation. I look forward to continuing to work with you on our common cause in my new role.

With Best Regards,

Andy Purdy
Acting Director,
National Cyber Security Division/US-CERT

Risk Reduction Activities Highlights

National Cyber Security Division

Background

The highly distributed and interconnected nature of the Information Technology (IT) Sector and the cyber elements that comprise all the other critical infrastructure/key resources, both physically and logically, requires that protective actions and programs be implemented both within and across the sectors.

Threat analysis, vulnerability assessment, and consequence analysis provide the foundation for determining the risk associated with an asset, system, network, or function. Generally, as owners and operators and other organizations, including the Department of Homeland Security (DHS), conduct risk assessments across assets, systems, networks, or functions, or sets of assets or systems, the results are prioritized to help identify where risk reduction activities are most needed for infrastructure protection. The National Cyber Security Division (NCSD) is actively engaged in a variety of risk reduction activities that are highlighted below.

Improving the Security of the Information Technology Sector. The IT Sector, also referred to as the "IT Industrial Base," is comprised of the producers of hardware, software, and IT services. NCSD is working collaboratively with our private and public sector partners in the IT Sector through the IT Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) to develop the IT Sector Specific Plan (SSP). The IT SSP, which will be finalized in December 2006, will describe a framework and approach for assessing risk, developing and implementing protective programs, sharing information, identifying research and development requirements, and measuring effectiveness and progress. IT Sector security partners are encouraged to participate in the development of the IT SSP through the SCC and GCC framework established under the National Infrastructure Protection Plan (NIPP). The IT SSP will also be shared with other sectors to promote collaboration across the sectors. Through implementation of the protective measures that result from the IT SSP, NCSD and the Sector's actions will reduce risk to the IT Sector. For more information on improving the security of the Information Technology Sector, please contact IT.sector@dhs.gov.

Promoting More Secure and Better Quality Software Products. NCSD's Software Assurance initiative is a comprehensive strategy that addresses people, process, technology, and acquisition throughout the software lifecycle. Efforts to encourage the routine development and deployment of trustworthy software products through public-private partnerships make a significant contribution to securing cyberspace and our Nation's critical infrastructure. These efforts will encourage the production of more secure and higher quality software by promoting the development of practical guidance, review tools, and research and development investment in cyber security. The overall goal is to enable secure and reliable software that support mission requirements and, therefore, more resilient organizations.

Upcoming Software Assurance initiatives include the fifth annual Software Assurance Forum "Enabling Software Assurance and Cyber Security." The forum is being hosted by DHS National Cyber Security Division, and Office of the Assistant Secretary of Defense (Networks and Information Integration). It is scheduled to take place in McLean, VA on October 2-3, 2006. Last minute registrations will be accommodated each morning from 7:30-8:30am during the forum.

For more information about promoting secure and better quality software products please visit: https://buildsecurityin.us-cert.gov.

Reducing the Impact of Attacks on Control Systems. NCSD's Control Systems Security Program (CSSP) is addressing control systems cyber vulnerabilities. Control systems are computer-based systems used within many infrastructures and industries to monitor and control sensitive processes and physical functions. The CSSP develops and implements initiatives aimed at reducing risk and impacts of a cyber attack against critical infrastructure control systems. It coordinates government and industry activities to facilitate control system incident management, provides timely situational awareness information, and manages control system vulnerability and threat reduction activities. For more information on reducing the impact of attacks on control systems, visit: http://www.us-cert.gov/control_systems/

Providing Cyber Guidance to Critical Infrastructures. NCSD sponsors and develops cyber security guidance and best practices documents in partnership with public and private entities and participates in various interagency committees and working groups, as well as standards bodies. NCSD is heavily involved in assisting Sector Specific Agencies (SSA) in the integration of cyber security into their Sector Specific Plans (SSPs), as annexes to the National Infrastructure Protection Plan. NCSD is providing resources and expertise to a number of the SSAs as they develop their initial draft SSPs and will continue to provide assistance as they finalize and implement their SSPs. This assistance includes several guidance resources, such as an SSP Cyber Guidance Checklist to aid sectors with incorporating various aspects of cyber security in the development of the SSP; a Cyber Research and Development (R&D) overview that provides additional information to help SSAs in the development of the Critical Infrastructure / Key Resource Protection R&D chapter of the SSP; and Cyber Protective Programs Overview that provides information to aid SSAs in the drafting of the cyber component of the Develop and Implement Protective Programs chapter of their SSP. In addition to supporting the SSAs in the development of their SSPs, NCSD is charged with reviewing the cyber aspects of the final SSPs to ensure the cyber aspects are properly addressed. As a cross-sector cyber resource to the federal government, NCSD will continue to develop and provide resources as requested. For additional information on cyber guidance to critical infrastructures, please email IT.sector@dhs.gov.

Exercising Plans, People, and Processes. Exercises are one of the mechanisms used to understand how to enhance our nation's cyber preparedness and better manage and reduce risk. The Cyber Storm Exercise conducted in February 2006 examined response, coordination, and recovery mechanisms to a simulated cyber event within international, federal, state, and local governments, in conjunction with the private sector. The exercise simulated a sophisticated cyber attack through a series of scenarios directed against critical infrastructures such as energy and transportation and the federal, state, and international governments with the intent of disrupting government operations and degrading public confidence. Through exercises such as Cyber Storm, DHS is examining the national cyber incident response and critical information sharing paths and mechanisms among public and private sectors as well as identifying policy issues that affect response and recovery. Exercises also provide insight into ways to improve and promote public and private sector interaction toward enhancing situational awareness that supports public and private sector decision making, communicating appropriate information to key stakeholders and the public, and planning and implementing appropriate response and recovery activities. For more information on NCSD exercises, contact Jeffrey Wright, Director of Exercises, NCSD at jeffrey.wright@dhs.gov.

Training and Education. Making an investment in the future of security is a key part of reducing vulnerabilities over time. To protect the critical infrastructure, our nation must focus resources on training a talented and innovative pool of citizens that specialize in securing our cyber infrastructure. NCSD and the National Security Agency (NSA) have collaborated to amplify an existing, successful program – the Centers of Academic Excellence in Information Assurance Education Program (CAEIAE). Through this partnership, NCSD and NSA are promoting higher education in information assurance (IA) to increase the number of IA professionals.

Mitigating the Threat Presented by Globalization. Traditionally, the federal government has been able to rely on U.S.-based hardware and software suppliers and U.S.-based network operators. Now, many suppliers are offshore, and even U.S.-based companies use research and manufacturing facilities elsewhere for much of their work to take advantage of lower costs and other business savings. Mergers and acquisitions have changed the ownership and management within the telecommunications and IT sectors, placing foreign companies in control of domestic operations. Globalization and its consequences are permanent and irreversible, and are only likely to have greater impact over time. To mitigate and reduce the risk presented by globalization, NCSD co-chairs the Committee on National Security Systems' (CNSS) Global IT Working Group (GITWG). The GITWG has developed a risk mitigation strategy to minimize the security risk to national security systems (NSS) stemming from the rapidly changing global environment. The strategy is focused on enhancing the security and resilience of United States Governance IT and telecommunication infrastructures; identifying and mitigating opportunities for exploitation; increasing adversaries' cost and risk of exposure; and reducing adversaries' confidence that an attack will be effective. More information on CNSS can be found at the CNSS website: http://www.cnss.gov/. ◆

Guest Article: Implementing the NIPP Information Sharing Model

A key element of the recently released National Infrastructure Protection Plan (NIPP) is the goal of enhancing information sharing between industry and government, as well as within industry. The NIPP provides a framework for doing this, through Sector Coordinating Councils for private industry and Government Coordinating Councils for the public sector to collaboratively address policy issues and operational information sharing mechanisms. It is the responsibility of each sector to develop an information sharing model based on the NIPP framework. The Information Technology-Information Sharing and Analysis Center (IT-ISAC) is designated by the IT Sector Coordinating Council, and is recognized by DHS, as the information sharing organization for private industry within the IT sector.

While establishing these structures are both useful and appropriate, it does not mark the beginning of the IT Sector's collaboration among industry, government and other sectors. The IT-ISAC, for example, has been working with our colleagues in industry and government since 2001 to build systems, processes and procedures to get useful information to the right people in a timely fashion within the IT sector. Our members pre-designate specific representatives in their companies to receive information. A member of the IT emergency response team, for example, might have access to cyber information while the Chief Security Officer might have access to information on cross sector and physical information.

The IT-ISAC's 24x7 Operations Center analyzes and delivers this information whenever circumstances require. The goal of the IT-ISAC is to share useful information and not just to share information for the sake of sharing information. Therefore, the Operations Center verifies the source and authenticity of the information, analyzes its severity and collects other associated data before deciding whether it is useful to members. This asset is enhanced through the expertise within our membership, which is leveraged to conduct collaborative analysis on specific incidents.

In today's interdependent economy it is essential that information be shared across sectors. This is why the ISACs from across the critical infrastructure sectors have been cooperating and coordinating through the ISAC Council to maximize information sharing across sectors. This cooperation occurs on a daily basis, when the operations centers of the various ISACs communicate through regularly scheduled calls to share information on cyber and physical threats. The operations centers then determine what information is relevant to share with their members. The IT-ISAC hosts these cross-sector operational calls and actively supports other information sharing initiatives.

This cooperation also extends to the development and implementation of specific cross sector initiatives. The ISAC Council is developing a framework to formalize and routinize information sharing. The goals are to increase trusted information sharing and analysis efforts across all NIPP stakeholders to support the broadest possible reach so that no relevant entity is excluded; support the development and dissemination of useful and actionable information products; realize cost efficiencies and reduce redundancy, where possible; and promote clear and definable framework requirements, definitions and objectives.

The Department of Homeland Security and state and local governments are key partners in these efforts. The Multi State ISAC, for example, is a member of the ISAC Council. In addition, the United States Computer Emergency Readiness Team (US_CERT) participates in the daily cyber calls hosted by the IT-ISAC, and the Department of Homeland Security's National Infrastructure Coordination Center routinely interacts with the various ISAC operations centers. From a policy perspective, Assistant Secretary Bob Stephan has been supportive of the ISACs and their missions, and the IT-ISAC looks forward to working with Greg Garcia, the new Assistant Secretary for Cyber Security and Telecommunications.

Moving forward under the NIPP framework, we need to continue to advance our efforts to build a culture of sharing, where each partner understands the value in sharing information. Despite our progress, there are still too many potential negative consequences of information sharing, such as unauthorized disclosure and liability, and perceptions of not enough benefits. While having a final rule in place for implementing the Protected Critical Infrastructure Information (PCII) Act is helpful, it also, by itself, is not enough. The government must demonstrate it has the ability to keep the shared information confidential, and the capability to turn shared information into useful and timely analytical products to industry.

Even as those issues are being addressed, the ISAC structure provides a trusted forum for information sharing and analysis under the NIPP framework. In the IT-ISAC, for example, confidentiality is guaranteed for those who want it and information dissemination is governed by our Non Disclosure Agreement, which each company agrees to as a condition of membership. Twice a week calls with our members builds familiarity and confidence. This provides a trusted framework for information sharing.

The challenges to information sharing are vast and complex. No single organization can solve these challenges in isolation. Some entities are too large for trusted information sharing, and smaller networks often are not useful for the mass dissemination of information. But, with the support of the IT Sector Coordinating Council and the IT Sector Specific Agency, the IT-ISAC provides a trusted forum for sensitive information sharing and collaborative analysis. In this way we have a vital role in enhancing the security of the information infrastructure that propels the global economy.

Scott C. Algeier is the Executive Director of the Information Technology-Information Sharing and Analysis Center (www.it-isac.org). He can be reached at salgeier@iss.net. ◆

Complete: The Cyber Storm Public Exercise Report

The Department of Homeland Security (DHS) announces the release of the Cyber Storm Public Exercise Report. The report details the key findings of Cyber Storm, the largest, most complex multi-national government-led cyber exercise to date. Cyber Storm examined response, coordination and recovery mechanisms to a simulated cyber event within international, federal, and state governments, in conjunction with the private sector.

The Cyber Storm Public Exercise Report highlights eight major findings:

- Interagency Coordination: Interagency and cross-sector information sharing enhanced coordination, communication, and response
- Contingency Planning, Risk Assessment, and Roles and Responsibilities: Clearly defined processes and procedures increased ability to plan for and assess situations and establish trust during a crisis
- Correlation of Multiple Incidents between Public and Private Sectors: The cyber community was effective in addressing individual threats and attacks, but faced challenges in creating a broad situational awareness during coordinated cyber attacks
- Exercise Program: Ongoing exercises will strengthen awareness of cyber incident response, roles, policies and procedures
- Coordination between Entities of Cyber Incidents: Establishing expectations, roles, processes, and communications will improve coordination and response as the number of cyber incidents increase
- Common Framework for Response to Information Access: Early and ongoing information sharing across governments and sectors created a common framework for response and strengthened relationships between domestic and international response partners
- Strategic Communications and Public Relations: Public messaging is an important aspect of incident response, as it provides the public and private sector with critical information and empowers them to take appropriate action to protect themselves and critical infrastructure
- Improvement of Process, Tools and Technology: Improved processes, tools and technology focused on the prioritization of physical, economic and national security impacts of a cyber incident will benefit the quality, speed and coordination of response

DHS and the National Cyber Security Division (NCSD) are working with public and private sector partners to: address the report's findings and lessons learned; enhance cyber security situational awareness, preparedness, and response; leverage new and existing partnerships; further define roles and responsibilities; examine the policies, procedures, and other organizational changes that might enhance the state of our cyber security; and improve cyber incident coordination and response.

Cyber Storm emphasized the Administration's commitment to cyber security and preparedness. The planning and implementation of Cyber Storm involved 115 public, private, and international agencies, organizations, and companies. The exercise simulated a sophisticated cyber attack through a series of scenarios directed against critical infrastructures. Each of the scenarios was developed with the assistance of industry experts and was executed in a closed and secure environment.

A copy of the Cyber Storm exercise report can be found at: http://www.dhs.gov/interweb/assetlibrary/prep_cyberstormreport_sep06.pdf ◆

October is National Cyber Security Awareness Month

The Department of Homeland Security's (DHS) National Cyber Security Division (NCSD) in collaboration with the National Cyber Security Alliance (NCSA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) is preparing for the third annual National Cyber Security Awareness Month, October 2006.

NCSD, NCSA, and MS-ISAC will sponsor and participate in a number of events and activities aimed at promoting cyber security awareness to industry, government, academia, small businesses, home users, and consumers. "Increasing awareness of cyber security to all cyber security users is essential to improving the safety of the cyber infrastructure and lowering our overall risk," states Liesyl Franz, Deputy Director Outreach and Awareness, NCSD.

The theme for Awareness Month 2006 is "Cyber Security: Make it a Habit." The concept is to illustrate to home users and small businesses the importance of regularly checking and updating security software to ensure computers, connections, and information are all secure. The goal of this campaign is to close the gap between what people know, and the actions they take towards integrating cyber security into their lives. Several collaboration initiatives supporting National Cyber Security Awareness Month, include:

NCSA Initiatives

NCSA is launching a new, grassroots cyber security outreach program targeting small businesses in multiple U.S. cities. As part of this grassroots effort, NCSA presenters will speak to more than 500 U.S. small businesses across the country.

"During the month of October, we are asking the public to be more conscientious and diligent about Cyber security," said Ron Teixeira, executive director of the National Cyber Security Alliance. "Research shows that although people know about online threats and preventive measures, they are simply not taking steps to stay safe online. So we are asking people to "Make cyber Security a Habit" in October, in hopes that they will continue the habit through October and beyond."

MS-ISAC Initiatives

MS-ISAC will coordinate state and city sponsored events for non-technical audiences. Working with Microsoft Corporation, MS-ISAC will produce a public service announcement geared towards home users which can be customized by location for each state. In addition, MS-ISAC is launching basic cyber security training for state employees and webcasts will target the K-12 audience.

"I am excited by the progress that the states are making in raising cyber security awareness, not only at the state level, but at the local level. Governments at all levels are interconnected and it truly takes a collaborative effort to insure the security of our information systems." *William Pelgrin, Chair, Multi-State ISAC*

NCSD Initiatives

NCSD is collaborating with NCSA and MS-ISAC on their various efforts, while conducting outreach to the technical audience during Awareness Month. NCSD speakers will give presentations on cyber security to a variety of technical audiences at events such as the Annual Security Symposium at the University of North Carolina at Charlotte, the Quality Assurance Association of Maryland Annual Conference, the National White Collar Crime Center Economic Crime Summit, and the International Association of Chiefs of Police Annual Conference, among others.

Since October was designated as National Cyber Security Awareness Month in 2004, it has been formally recognized by Congress, governors, municipalities and industry leaders. NCSD encourages everyone to participate in events and to talk to employees, peers, and business associates about National Cyber Security Awareness Month. Spread the word—help increase cyber preparedness!

For more information and to get involved in Awareness Month:

www.staysafeonline.com is the website of NCSA. It provides valuable information such as cyber security tips on safeguarding your personal information, protecting your children online, and software that can help you protect your data. This site also provides free information tailored towards different audiences—Educators, Family and Children, Small Businesses, and News and Media—based on their specific needs.

Onguard Online (www.onguardonline.gov) is a partnership between the federal government and the technology industry to help consumers protect themselves from internet fraud, secure their own computers, and guard their personal information. Users can obtain information on topics such as identity theft, online shopping and internet auctions, wireless network security, spam and "phishing" scams, spyware, and social networking sites.◆

United States Collaborates with Germany to Host International Watch and Warning Network (IWWN) Conference

IWWN Conference Communiqué

On 23 June 2006, in Washington, DC, USA, participants in the International Watch and Warning Network (IWWN) Conference issued the following joint statement:

The United States, in collaboration with Germany, hosted a multilateral conference on cyber security on 22-23 June 2006 in Washington, DC, USA focused on the continuing development of an International Watch and Warning Network. The conference brought participants together to address international cooperation on cyber watch, warning, and incident response, and mechanisms that further global collaborative efforts toward critical information infrastructure protection.

This conference follows the first international watch and warning conference co-hosted by the United States and Germany in October 2004 in Berlin, a subsequent workshop in March 2005 in Paris, the Global Ribbon Communication Check Exercise in February 2006, and other interim and on-going collaborative activities toward building an IWWN.

The following countries participate in the IWWN and attended the conference: Australia, Canada, Finland, France, Germany, Hungary, Japan, Italy, the Netherlands, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States.

Country delegations included government cyber security policy makers, managers of computer security incident response teams with national responsibility, and law enforcement representatives with responsibility for cyber crime matters.

The conference included: presentations on regional developments and collaborative efforts; reports on and lessons learned from recent cyber security exercises; a facilitated scenario-based discussion on a cyber incident with global impact; interactive discussions on information sharing mechanisms and approaches in the IWWN with immediate actions and longer term goals. The conference also marked the launch of an international collaboration portal for use by the IWWN for collaboration and information exchange.

The participating countries discussed:

1. The recognition and establishment of the IWWN as an international framework for cyber information sharing and incident response subject to national considerations. The IWWN reflects an arrangement among countries brought together by mutual self interest to exchange critical cyber incident information in order to defend critical national and global information infrastructures.
2. As an international framework for cyber information sharing and incident response, IWWN:
   a. Acknowledges existing and emerging regional information sharing arrangements, and
   b. Promotes communications between core national cyber-related functions including:
      i. government cyber security policy
      ii. national computer security incident response
      iii. cyber crime law enforcement
3. Participation in communications exercises utilizing the Critical Information Infrastructure Protection (CIIP) Directory of government points-of-contact to further continued participation by the core national cyber-related functions in the IWWN community.
4. Use of the international communications portal for communications and information exchange about on-going cyber related issues and cyber incidents to build global cyber situational awareness, enhance global partnerships for watch, warning, and incident response, and share information on national, regional, and international efforts toward greater cyber security.
5. As an international framework for cyber information sharing and incident response, the IWWN participants intend to:
   a. Maintain functional points-of-contact with national responsibility with watch, warning and incident response purposes;
   b. Utilize the international collaboration portal to share appropriate and non-sensitive information on an on-going basis for cyber watch purposes, which would include such aspects as:
      i. alerts and advisories
      ii. summary reports
      iii. ad hoc security products such as white papers, best practices, etc., and
      iv. permit translation for publicly available documents

c. Communicate and coordinate response in case of a cyber incident with actual or potential global impact, and

d. Pursue efforts to further forge international cooperation and coordination through consideration of enhanced information sharing, exercises, and strategic collaboration to reduce cyber risk. ◆

US-CERT update on Data Security and Privacy

The United States Computer Emergency Readiness Team (US-CERT) has been busy monitoring recent trends involving the acquisition of personally identifiable information (PII) by unauthorized, malicious users. PII is frequently associated with information security and privacy to indicate pieces of information that can be used as a point of reference for locating, identifying, or contacting an individual. It is information that helps to uniquely describe an individual, such as:

- Full name (if not commonly used)
- Email address
- Postal address
- Telephone number
- Driver's license number
- Unique physical characteristics such as face and fingerprints
- National Identification Number or Social Security Number

Individuals can help protect themselves by following these safeguards:

- Only discuss personal information with those individuals/companies who have a need to know.
- Dispose of personal mail or information appropriately, i.e., shred, burn, etc..
- Periodically check your credit report to monitor for fraud; under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus.

In situations where access to PII records is necessary, US-CERT recommends that proper safeguards and access controls be established. PII records should always be stored in a secure environment, and strictly adhered-to ground rules must be established for access to, checking-out, and checking-in such information.

Visit http://www.us-cert.gov/cas/tips/ST05-019.html for more information. ◆

Announcing the US-CERT Quarterly Trends and Analysis Report

US-CERT has released the first edition of its Quarterly Trends and Analysis Report created for the general public. It will be produced quarterly and posted on the www.us-cert.gov website. The report provides a snapshot of notable cyber security topics and trends as seen and reported to US-CERT. The inaugural issue features incident reporting statistics, information for improving your data security and privacy, an emerging threats summary, and links to helpful resources. To view this report, visit the US-CERT website, or click on http://www.us-cert.gov/press _ room/trendsandanalysisQ306.pdf ◆

NCSD and NCS Host Internet Disruption Working Group Table Top

The Department of Homeland Security's (DHS), Internet Disruption Working Group (IDWG), a strategic partnership between the National Cyber Security Division (NCSD) and the National Communications System (NCS), conducted a tabletop exercise (TTX) with government and private sector subject matter experts on June 15 2006. The TTX involved a facilitated discussion of three scenarios, and it provided a forum for industry and government experts to explore the types of information and information exchange that each sector would find mutually beneficial during an Internet disruption. It also presented an opportunity for participants to examine industry and government roles and responsibilities in responding to an event.

The IDWG TTX provided a forum for industry and government experts to explore the type of information and information exchange that each sector would find mutually beneficial during an Internet disruption. It also presented an opportunity for participants to examine industry and government roles and responsibilities in responding to an event.

The goals of the TTX were to:
1) increase understanding of the "as is" information sharing environment between government and Internet owners and operators during heightened periods of interest affecting the Internet; 2) explore what thresholds should exist for exchanging information between industry and government, and identify the types of information that the private sector would find helpful from government and vice versa; and 3) clarify roles and responsibilities of industry and government in the event of an Internet disruption.

The findings of the TTX are in the areas of industry-government information sharing, incentives for implementing security measures, the inherent non-territorial nature of the Internet, public awareness, and the concept of a Cyber Incident of National Significance.

This TTX was the first TTX for the IDWG; and additional exercises are planned for 2007. For more information, please contact Michael Smith, IDWG NCSD Co-chair, at mike.c.smith@dhs.gov. ◆

Introducing the CyberCop Portal

The CyberCop Portal is the leader in bridging system stovepipes between organizations by providing a separate means to collaborate over the web using the security controls necessary to handle sensitive but unclassified law enforcement information.

The Portal allows users to share libraries of documents and case studies, send secure e-mail, participate in ongoing threaded discussions, create and distribute surveys and share online briefings. Membership to the CyberCop Portal is restricted to law enforcement/intel related partners.

The CyberCop mission is to provide individuals with an ultra-secure web-based environment to promote and facilitate the sharing of sensitive information among a cohesive network of cyber security, law enforcement, first responders, homeland defense and law enforcement related professionals from all levels of government; international, federal, state, local, and the private sector, regardless of department affiliation and jurisdictional boundaries. CyberCop is committed to providing a safe and secure environment where ideas can be freely exchanged to aid individual efforts and foster cooperative efforts in the fight against crime, terrorism, and the security of our homeland.

Why use the CyberCop Portal?

The CyberCop Portal demonstrates the potential for highly secure collaboration among users from diverse organizations without the expense and administrative burdens of VPN's or similar security strategies. By combining the use of 128-bit

NCSD Speaking Engagements

Listed are NCSD speaking engagements and events that are open to the public and press.

October 2-3, 2006

Software Assurance Forum, McLean, VA

Andy Purdy, Director, National Cyber Security Division

https://buildsecurityin.us-cert.gov/daisy/bsi/events/521.html

October 17, 2006

Texas State University Cyber Security Awareness Day, San Marcos, TX (via VTC)

Liesyl Franz, Deputy Director, Outreach and Awareness

http://www.vpit.txstate.edu/security

October 23, 2006

Rockwell Automation Fair. Baltimore, MD

Hun Kim, Deputy Director, National Cyber Security Division

www.automationfair.com

October 24, 2006

IDGA Border Management Summit. Washington, DC

Annabelle Lee, Director, Standards and Best Practices

http://www.bordermanagementsummit.com/cgi-bin/templates/genevent.html?topic=329&event=10789

October 24, 2006

Quality Assurance Association of Maryland Annual Conference. Baltimore, MD

Joe Jarzombek, Director, Software Assurance

http://www.qaiworldwide.org/conferences/index.html

October 24, 2006

Cyber Security Summit. Knoxville, TN

Mike Levin, Deputy Director, Law Enforcement and Intelligence

http://cybersecurity.utk.edu/index.htm

October 25, 2006

University of North Carolina, Charlotte Annual Security Symposium. Charlotte, NC

Joe Jarzombek, Director, Software Assurance

http://www.coit.uncc.edu/symposium/2006/site/index.cfm

October 25-27, 2006

Meridian Conference. Budapest, Hungary

Liesyl Franz, Deputy Director, Outreach and Awareness

http://www.meridian2006.org

November 14, 2006

National Native American Law Enforcement Association Conference

Albuquerque, MN

Hun Kim, Deputy Director, National Cyber Security Division

www.nnalea.org

SSL, security hardened operating environments, and tools with highly granular access controls, the portal can be securely accessed from organizations over which the sponsors have no systems configuration control and with no need to install and maintain client software.

Who uses CyberCop?

CyberCop is a private sector initiative that is supported by sponsors from both government and industry. The CyberCop Portal is in use by more than 8,700 members. All 50 states are represented on the portal as well as government agencies and over 40 countries. In addition, a number of agencies and organizations at the state and federal level involved in cybercrime law enforcement and INFOSEC pursuits have built and maintained sub-communities inside the CyberCop Portal.

To learn more, visit http://www.cybercopportal.org/index.htm ◆

The NCSD newsletter is a quarterly eNewsletter about the National Cyber Security Division at DHS. We welcome your feedback. If you have any comments about the newsletter or suggestions for items to include in future issues, please send them to: kristin.walters@associates.dhs.gov