CYBERSECURITY RELATED INTERNET SOURCES

USEFUL SITES, PORTALS AND ORGANIZATIONS

CEO CyberSecurity Resource Center

http://www.technet.org/cybersecurity/

For many CEOs, information security risk management is a new area of responsibility. This web site helps CEOs come up to speed on information security risk management issues and quickly assess their own company's cyber preparedness.

Carnegie Mellon CyLab

http://www.cylab.cmu.edu

The CyLab in Carnegie Mellon University attempts to create a public-private partnership to develop new technologies for measurable, available, secure, trustworthy, and sustainable computing and communications systems and to educate individuals at all levels. CyLab is a university-wide, multidisciplinary initiative involving more than 200 faculty, students, and staff that builds on more than two decades of Carnegie Mellon's leadership in information technology. CyLab works closely with the CERT® Coordination Center, a leading, internationally recognized center of Internet security expertise. Through its connection to the CERT/CC, CyLab also works closely with US-CERT—a partnership between the Department of Homeland Security's National Cyber Security Division (NCSD) and the private sector—to protect the U.S. information infrastructure.

CyberSecurity Institute

http://www.cybersecurityinstitute.biz/

The Cybersecurity Institute is a world leader for digital forensics training. The more technical definition that the CyberSecurity Institute uses to describe computer forensics or forensic computing in the vein of computer crime or computer misuse is as follows: "The preservation, identification, extraction, interpretation, and

documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found."

Institute for Information Infrastructure Protection

http://www.thei3P.org/

The Institute for Information Infrastructure Protection (I3P) is an U.S. consortium of leading cybersecurity research and development organizations including universities, federally funding labs and non-profit organizations. The goals of the I3P are to address research and policy-related aspects of the vulnerabilities inherent in the information infrastructure, bring experts together to identify and mitigate threats aimed at the U.S. information infrastructure, and promote collaboration and information sharing among academia, industry, and government.

Institute for Security Technology Studies at Dartmouth College

http://www.ists.dartmouth.edu/

The Institute for Security Technology Studies (ISTS) at Dartmouth College and its core program on cybersecurity and information infrastructure protection research serve as a principal U.S. center for counter-terrorism technology research, development, and assessment. The institute is dedicated to pursuing interdisciplinary research and education for cybersecurity and emergency response technology. ISTS is also a member of the Institute for Information Infrastructure Protection (I3P). The site includes a large bibliography and description of current research.

CyberSecurity and Emergency Preparedness Institute

http://csepi.utdallas.edu/

The CyberSecurity and Emergency Preparedness Institute at the University of Texas at Dallas (UTD) focuses primarily on performing innovative digital forensics, information assurance and emergency preparedness research in areas including network survivability, rapidly deployable networks, sensor networks, reconfigurable hardware, self healing software, anti-piracy methods, signal processing, data mining, high assurance systems engineering, emergency response information systems and others. Importantly, the researchers have continually demonstrated their ability to deliver comprehensive, practical solutions at the device, system and network level.

Internet Crime Complaint Center (IC3)

http://www.ic3.gov/

The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI) and the U.S. National White Collar Crime Center (NW3C). IC3's mission is to address fraud committed over the Internet. The IC3 gives the victims of cybercrime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, local and international level, IC3 provides a central referral mechanism for complaints involving Internet related crimes.

The United States Computer Emergency Readiness Team

http://www.us-cert.gov/

The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the U.S. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cybersecurity information to the public. Information is available from the US-CERT web site, mailing lists, and RSS channels. US-CERT also provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the United States government about cyber security.

CERT Coordination Center

http://www.cert.org/

The Computer Emergency Readiness Team (CERT) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. The Center studies Internet security vulnerabilities; research is done on long-term changes in networked systems; and information and training is developed to help in improving security.

Australian Computer Emergency Response Team (AusCERT)

http://www.auscert.org.au/

AusCERT is the national Computer Emergency Response Team for Australia and a leading CERT in the Asia/Pacific region. As a trusted Australian contact within a

worldwide network of computer security experts, AusCERT provides computer incident prevention, response and mitigation strategies for members, a national alerting service and an incident reporting scheme.

U.S. National Computer Crime Squad, Federal Bureau of Investigation

http://www.emergency.com/fbi-nccs.htm/

The FBI's National Computer Crime Squad (NCCS) investigates violations of the Federal Computer Fraud and Abuse Act of 1986. These crimes cross multiple state or international boundaries. Violations of the Computer Fraud and Abuse Act include intrusions into government, financial, most medical, and Federal interest computers. Federal interest computers are defined by law as two or more computers involved in a criminal offense, which are located in different states. Therefore, a commercial computer which is the victim of an intrusion coming from another state is a "Federal interest" computer.

The Federal Bureau of Investigation (FBI) has a Computer Crime Squad Web page that contains contact information for the Squad.

The Purdue University Center for Education and Research in Information Assurance and Security (CERIAS)

http://www.cerias.purdue.edu/

The Purdue University Center for Education and Research in Information Assurance and Security (CERIAS) is currently viewed as one of the world's leading centers for research and education in information assurance and security. CERIAS is unique in its multidisciplinary approach to the problems, ranging from purely technical issues (e.g., intrusion detection, network security, etc) to ethical, legal, educational, communicational, linguistic, and economic issues, and the interactions and dependencies among them. The following areas summarize the research focus areas for the faculty involved with the center: Risk Management, Policies, and Laws; Trusted Social and Human Interactions; security awareness, education, and training; assurable software and architectures; enclave and network security; incident detection, response, and investigation; identification, authentication, and privacy; and cryptology and rights management.

The Computer Security Resource Center of the U.S. National Institute of Standards and Technology (NIST)'s Computer Security Division

http://csrc.nist.gov/

The Computer Security Division (CSD) is one of eight divisions within NIST's Information Technology Laboratory. The mission of NIST's Computer Security Division is to improve information systems security by: (1) Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies; (2) Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive systems; (3) Developing standards, metrics, tests and validation programs; and (4) Developing guidance to increase secure IT planning, implementation, management and operation.

The SANS Institute

http://www.sans.org/

The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, and CIOs who share the lessons they are learning and jointly find solutions to the challenges they face. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the information security community. The SANS Institute is the most trusted and by far the largest source for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system – Internet Storm Center.

Many SANS resources, such as the weekly vulnerability digest (@RISK), the weekly news digest (NewsBites), the Internet's early warning system (Internet Storm Center), flash security alerts and more than 1,200 award-winning, original research papers are free to all.

Forum for Incident Response and Security Teams (FIRST)

http://www.first.org/

FIRST is a leading organization in incident response. It brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. Membership in

FIRST enables incident response teams to more effectively respond to security incidents – reactive as well as proactive.

FIRST also provides value added services, such as access to up-to-date best practice documents, technical colloquia for security experts, hands-on classes, annual incident response conference, publications and web-services and special interest groups

At present FIRST has more than 170 members, spread over the Americas, Asia, Europe and Oceania.

ON-LINE PUBLICATIONS

Cybercrime and Cybersecurity Communication

http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html

This is a communication from the Commission of the European Communities to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on creating a safer information society by improving the security of information infrastructures and combating computer-related crime.

Perspective: The Left and Right Hands of Cybersecurity

http://news.com.com/2010-1009_3-6036384.html

This is a commentary by Eric J. Sinrod, partner at Duane Morris. A report from the National Association of State Chief Information Officers (NASCIO) criticizes the Department of Homeland Security (DHS) for failing to coordinate with state and local law enforcement against cyberthreats. The report finds that state and local agencies would rather work with DHS than with the private sector, which has proven detached from local interests. The NASCIO recommend adding cybersecurity to DHS's State Homeland Security Assessment and Strategy process. State and local governments need better training in best practices, cybersecurity, risk assessment, and continuity of operations. The report also finds that DHS needs to deliver information in a timelier manner, arguing that "more emphasis needs to be placed on external-directed attacks, and internal ineptitude and maliciousness." State and local agencies also need better academic and educational opportunities.

Convention Committee on Cybercrime (T-CY)

http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/6_Cybercrime/T-CY/

Owing the dangers of cybercrime and the need for common minimum technical and legal standards to fight such crime at a global level, the Convention on cybercrime (ETS N° 185) was prepared by Council of Europe member States and Canada, Japan, South Africa and the United States. It entered into force on 1 July 2004. Its Additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS N° 189) will enter into force on 1 March 2006.

The Convention is the only binding international instrument dealing with cybercrime. It has received widespread international support and is open to all states. The Convention provides for consultations of the parties.

Cyber Criminals Stepping up Targeted Attacks

http://news.zdnet.com/2100-1009_22-6046606.html

Symantec Internet Security Threat report says that during the second half of 2005, attackers continued to move away from broad attacks seeking to breach firewalls and routers and are now taking aim at the desktop and Web applications.

The report said threats such as viruses, worms, and trojans that can unearth confidential information from a user's computer rose to 80 percent of the top 50 malicious software code threats from 74 percent in the previous six months.

The Truth about Cyberterrorism

http://www.cio.com/archive/031502/truth.html

"Since September 11, threats once considered digital aggravations have been tagged cyberterrorist provocations. What cyberterrorism really means, according to the National Infrastructure Protection Center, is an act perpetrated through computers that results in violence, death and/or destruction, and creates terror for the purpose of coercing a government to change its policies. To qualify as cyberterrorism, an act must fulfill two criteria: a political motivation and a destructive result. Most computer attacks satisfy only the first criterion. It's far less likely than the media would have us believe that cyberterrorists could cause destruction, especially to the nation's physical infrastructure. More credible is the danger to critical data: a cyberterrorist who hacks critical computer systems to steal or irreversibly damage vital data, such as the Social Security database. The good news for CIOs is that protecting against any security threat protects against cyberterrorism."

Cybersecurity for the Homeland

http://hsc.house.gov/files/cybersecurityreport12.06.04.pdf

This report discusses the activities and findings of the Chairman and Ranking member of the House Subcommittee on Cybersecurity, Science, and Research & Development of the Select Committee on Homeland Security. This report addresses the following areas: case for action, role of the Department of Homeland Security, subcommittee oversight, and cybersecurity roadmap for the future.

VerySign's White Paper on Cybersecurity

http://www.verisign.com/static/005567.pdf

Today, national security and the concomitant need to protect the nation's critical infrastructure and maintain the continuity of government and financial services are equally important drivers. To meet the requirements for protecting national security and to address internal business requirements for online security, cyber systems must be able to share data securely; ensure the continuous availability of critical services; interoperate across federal, state, and local systems; and comply with federal consumer-privacy regulations. All this has been discussed in VerySign's white paper on cybersecurity.

Creating a National Framework for Cybersecurity: An Analysis of Issues and Options

http://www.thecre.com/pdf/secure/20050404_cyber.pdf

This Congressional Research Service (CRS) report (February 2005) discusses: (1) what is Cybersecurity; (2) where are the major weaknesses in cybersecurity; (3) what are the major means of leverage; and (4) what roles should government and the private sector play.

Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems (May 2005)

http://www.au.af.mil/au/awc/awcgate/gao/d05231.pdf

This report by the Government Accountability Office (GAO), United States, discusses (1) the potential risks to federal information systems from emerging cybersecurity threats such as spam, phishing, and spyware; (2) the 24 Chief Financial Officers Act agencies' reported perceptions of these risks and their actions and plans to mitigate them; (3) government and private-sector efforts to address these emerging cybersecurity threats on a national level, including actions to increase consumer

awareness; and (4) government-wide challenges to protecting federal information systems from these threats.

Guide for Developing Performance Metrics for Information Security

http://csrc.nist.gov/publications/drafts/draft-sp800-80-ipd.pdf

NIST's Computer Security Division has completed the initial public draft of Special Publication 800-80, Guide for Developing Performance Metrics for Information Security. This guide is intended to assist organizations in developing metrics for an information security program. The methodology links information security program performance to agency performance. It leverages agency-level strategic planning processes and uses security controls from NIST SP 800-53, Recommended Security Controls for Federal Information Systems, to characterize security performance. To facilitate the development and implementation of information security performance metrics, the guide provides templates, including at least one candidate metric for each of the security control families described in NIST SP 800-53.

Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities

http://www.gao.gov/new.items/d05434.pdf

This report by the Government Accountability Office (GAO), United States, discusses (1) Department of Homeland Security (DHS)'s roles and responsibilities for cyber critical infrastructure protection, (2) the status and adequacy of DHS's efforts to fulfill these responsibilities, and (3) the challenges DHS faces in fulfilling its cybersecurity responsibilities.

Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats

http://www.shaneland.co.uk/ewar/docs/dissertationsources/institutionalsource1.pdf

This is a report by James A. Lewis, published by the Center for Strategic & International Studies (CSIS). The author discusses issues related to cyber-terrorism and cyber attacks on critical infrastructure and their implications for national security.

Special Issue on Cybercrime of the International Journal of Communications Law and Policy (IJCLP)

http://www.ijclp.org/Cy_2004/index.html

The International Journal of Communications Law and Policy and the Yale Journal of Law and Technology published in autumn 2004 Issue 9 on Cybercrime in two parts. It features the following articles:

- Architectural Regulation and the Evolution of Social Norms (by Lee Tien)
- Transborder Search: A New Perspective in Law Enforcement? (by Nicolai Seitz)
- The Fourth Amendment Unplugged: Electronic Evidence Issues & Wireless Defenses - Wireless Crooks & the Wireless Internet Users Who Enable Them (by Tara McGraw Swaminatha)
- Launch on Warning: Aggressive Defense of Computer Systems (by Curtis E. A. Karnow)
- Real World Problems of Virtual Crime (by Beryl A. Howell)
- Distributed Security: Moving away from Reactive Law Enforcement (by Susan W. Brenner)
- The Price of Restricting Vulnerability Publications (by Jennifer Stisa Granick)
- Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd (by Kim A. Taipale)
- Surfing While Muslim: Privacy, Freedom of Expression & the Unintended Consequences of Cybercrime Legislation (by Jason M. Young)
- Privacy vs. Piracy (by Sonia K. Katyal)
- Characteristics of a Fictitious Child Victim: Turning a Sex Offender's Dreams into His Worst Nightmare (by James F. McLaughlin).

Defending against Cybercrime and Terrorism: A New Role for Universities

http://www.fbi.gov/publications/leb/2005/jan05leb.pdf
http://www.fbi.gov/publications/leb/2005/jan2005/jan2005.htm#page14

This is an article by Tony Aeilts, published in FBI-Law Enforcement Bulletin, Washington, vol. 74, no.1 (January 2005), p.14-20. The article discusses the need to include college and university resources in the fight against cybercrime and the threat of terrorism.

Reducing Opportunities for e-Crime

http://www.eurim.org.uk/activities/ecrime/reducingops.doc

"The paper focuses on the need for industry and law enforcement to work together to produce practical, plain English guidance for users at all levels, but most especially small firms and consumers, on what to do to protect themselves and what to do when they suspect they have been victimized. That guidance needs to include material on identifying and assessing risk and what to do about it. Similar guidance is needed for large organizations because un-prioritized governance paperchases, to meet the demands of regulators, can serve to increase vulnerability by diverting resources and attention from practical action."