Anti-Virus Strategies – Preventing an Epidemic

Panel Chair
Christine M. Orshesky
Telos Corporation
P.O. Box 46677
Washington, DC 20050
christine.orshesky@telos.com

Mark Jesmer
Federal Bureau of Investigation
10th and Pennsylvania Avenue, NW
Room 4282
Washington, DC 20535

Donald Phipps
Kaiser Permanente
1 Kaiser Plaza
Suite 5 Lakeside
Oakland, CA 94612
Donald.Phipps@kp.org

Jimmy Kuo
Network Associates
3415 S Sepulveda Blvd., Suite 700
Los Angeles, CA 90034
Jimmy_Kuo@nai.com

Erika Langerman
Joint Staff
9300 Joint Staff Pentagon
Washington, DC 20318-9300
langereh@js.pentagon.mil

According to the 1998 Annual Industry Survey published by the International Computer Security Association (ICSA), viruses and other types of malicious logic are the most prevalent forms of security breaches experienced. Given the current state of technology and resulting evolution of computer viruses, all organizations processing information must take active virus protection seriously.

The panelists represent major sectors of industry and government that utilize computing technologies. The panelists will highlight the differences and similarities as well as the potentially unique issues that their respective sectors possess. By describing the operating environments and anti-virus strategies used in each sector, it is the aim of the panel to provide insight into the types of protection available for various forms of computing resources and information including national security, intellectual property, trade secrets, and privacy data.

The anti-virus strategies presented will include the operating systems in use as well as policy, procedures, awareness, and software implementation for protecting the computing environment from viruses using anti-virus software and other techniques. Each panelist will also identify the rationale for the strategy implemented and the means for determining its effectiveness. In conclusion, each panelist will identify both lessons learned and any open issues that remain to be resolved.

Panelist Information

Ms. Orshesky, as a member of the Telos Corporation's Information Protection Solutions team, provides Malicious Logic Incident Management support and program development for the Single Agency Manager, Directorate of Security at the Pentagon. Additionally, Ms. Orshesky has over 8 years experience providing various information security and systems engineering support including: intrusion detection, access control mechanisms, key escrow, security assessments, penetration testing, application security requirements, security awareness, communications security, system certification and accreditation, application development methodologies, and quality assurance. Ms. Orshesky has achieved professional recognition through publication and participation in international virus prevention and national information system security conferences. Ms. Orshesky has obtained professional certification as a Certified Information Systems Security Professional (CISSP) and a Certified Quality Analyst (CQA).

Mr. Jesmer has over 15 years of experience in physical and computer security. He has conducted risk analysis on several hundred systems and facilities for federal, state and commercial operations. Mr. Jesmer has provided risk analysis and risk management training to over 1,000 participants. Presently, Mr. Jesmer is an Automated Data Processing and Telecommunications (ADPT) Security Specialist for the Federal Bureau of Investigations. The ADPT Security Specialist is responsible for all aspects of information system security for the FBI. Mr. Jesmer is responsible for administering the virus prevention, detection and reporting program.

Donald Phipps has been involved actively in the computer industry for nine years working in the areas of network installation, system configuration, application testing and setup and Anti-virus research and virus prevention in a heterogeneous LAN environment spanning the globe. Don has been a presenter at Virus Bulletin's International Conference on Computer Viruses in Brighton, England as well as the National Computer Security Association's International Virus Prevention Conference in Arlington, Virginia. Don also consults with individuals and non-profit organizations in the areas of system configuration and virus security.

Jimmy Kuo has a BS degree from California Institute of Technology in Pasadena. He worked with IBM on the PS/2 development team. Later, he was manager of the virus laboratory at Symantec's Peter Norton Product Group where he also worked on Norton Anti-Virus. Currently he is Director of Anti-virus Research at Network Associates.

Mrs. Langerman has over 15 years of experience in the computer security field within the DOD. Her experience includes the Naval Supply Systems Command, Naval Data Automation Command, Headquarters US Marine Corps, and 9 years with the Joint Staff. She has a wide perspective on computer security issues having worked at local command, headquarters, and components level agencies. She is currently the Chief of the Information Systems Security Division on the Joint Staff and is responsible for the corporate information assurance security program. Mrs. Langerman has implemented numerous "security in-depth" virus strategies for Joint Staff networks and seen significant reductions in virus proliferation.