Manhattan Cyber Project

Safeguarding Corporate America
and the
National Information Infrastructure

August 19, 1997 Overview

Manhattan Cyber Project

Contents

Manhattan Cyber Project

Project Origin

- Outgrowth of 1996 Information Systems Security Survey:
  - conducted in cooperation with the U.S. Senate's Permanent Subcommittee on Investigations; and
  - anonymity protected sources and proprietary information.
- Revealed startling findings on admitted security threats and vulnerabilities to Fortune 1000 corporations and elements of the National Information Infrastructure, to include:
  - 47% response rate (205 firms qualified);
  - 119 (58%) detected intrusions, 25 (12%) did not, and 61 (30%) didn't know;
  - 98 (82%) successful intrusions from the 119 that detected;
  - 129 (63%) of 205 firms caught insiders misusing systems;
  - 67 (41%) had losses per outsider incident over $ 500,000; and
  - probing/scanning, compromise email/documents, and introduced virus most frequent.

Manhattan Cyber Project

Project Origin (cont.)

- Ms. Jamie Gorelick, former Deputy Attorney General, Department of Justice during testimony in Senator Sam Nunn's hearings on Security in Cyberspace:
  - stressed urgency to form a public/private partnership to address the "cyber threat";
  - must engage the best and the brightest in industry, government, and academia;
  - likened the desired approach to the historic Manhattan Project; and
  - focus on public awareness and sharing of expert knowledge.
- Manhattan Cyber Project formed in early May 1997 with a Management Team representing industry and academia.
- U.S. Government jumped on board in Aug 1997 based on discussions and negotiations that began in Dec 1996.

Manhattan Cyber Project

Challenges

- Despite government and private industry studies and pronouncements, warnings about lack of security in cyberspace and risk of an electronic “Pearl Harbor” are largely unheeded.
- People are uninformed, confused, and skeptical regarding government goals, expectations, initiatives, and methodologies.
- Lack of reporting and documentation on cyber attacks obscures what is really happening.
- Broad range of dynamic threats and vulnerabilities -- Information Warfare threat is generally unknown.
- No uniform method available for measuring value of data/information and selecting appropriate safeguards.

Manhattan Cyber Project

Mission Statement

- Improve on the availability and effectiveness of people, technology, and processes that safeguard corporate America and critical infrastructure areas from the “cyber threat.”
  - PEOPLE: training, education, and collaborative forums.
  - TECHNOLOGY: firewalls, filtering routers, network management, intrusion detection, authentication, digital signatures, etc.
  - PROCESSES: requirements, configuration management, quality assurance, etc.
- Accomplish this mission by developing and facilitating a coordinated “outreach” program with industry, government, and academia.

Mission (cont.)

- Focus outreach on education, awareness, and some best practices.
- Key elements of the outreach program involve:
  - providing learning materials on threats, vulnerabilities, and security safeguards;
  - gathering of quantitative and qualitative data/information enhancing the understanding and benchmarking of the cyber threat;
  - furnishing of collected information to industry, government, and academic groups, as well as the general public; and
  - laying the foundation for the nonprofit Cyberspace Research & Education Center (CYREC™) to continue the work pioneered by the Manhattan Cyber Project.
- Empower stakeholders and the general public to be “situationally aware” and address the cyber threat.

Manhattan Cyber Project

Tasks

- Develop informative and unbiased outreach materials for the target audience that does NOT focus on individual solutions.
- Foster collaborative, self-directed Outreach Teams to present materials to the target audience.
- Initially examine the effects of the cyber threat on the critical infrastructure areas of:
  - telecommunications;
  - electrical power systems;
  - gas and oil transport and storage;
  - banking and finance;
  - transportation;
  - water supply systems;
  - emergency services; and
  - vital government services.

Tasks (cont.)

- Gather essential elements of cyber threat information by:
  - conducting robust, scientific surveys and interviews;
  - installing pilot intrusion detection and traffic analysis systems in multiple industries;
  - monitoring and tracking “open source” data/information on emerging threats and vulnerabilities; and
  - analyzing data/information on the present state of security.
- Identify a cyber threat baseline segmented by industry, threat, and vulnerability.
- Present special summary of findings to the legislative branch on critical infrastructure protection and corporate competitiveness.
- Establish the nonprofit CYREC™ as a shared resource and collaborative work environment.
- Conduct a Security in Cyberspace Summit.

Manhattan Cyber Project

Target Audience

- CEO’s, CIO’s, CFO’s, CKO’s, CTO’s -- owners and operators of critical infrastructure areas
- Senior managers of state and local governments
- Law enforcement agencies
- Information security personnel
- Physical security personnel
- Business continuity personnel
- Strategic planners
- General public
- Kids and young adults

Manhattan Cyber Project

Schedule

- Manhattan Cyber Project initiated in early May 1997.
- Follow-up press announcement in Aug 1997 to announce updated Management Team and Outreach Team members, government coordination, and event schedule.
- Outreach events held from Jun to Dec 1997.
- Establish CYREC™ in late 1997 with limited operations underway in Jan 1998.
- Security in Cyberspace Summit to be held in Feb 1998.

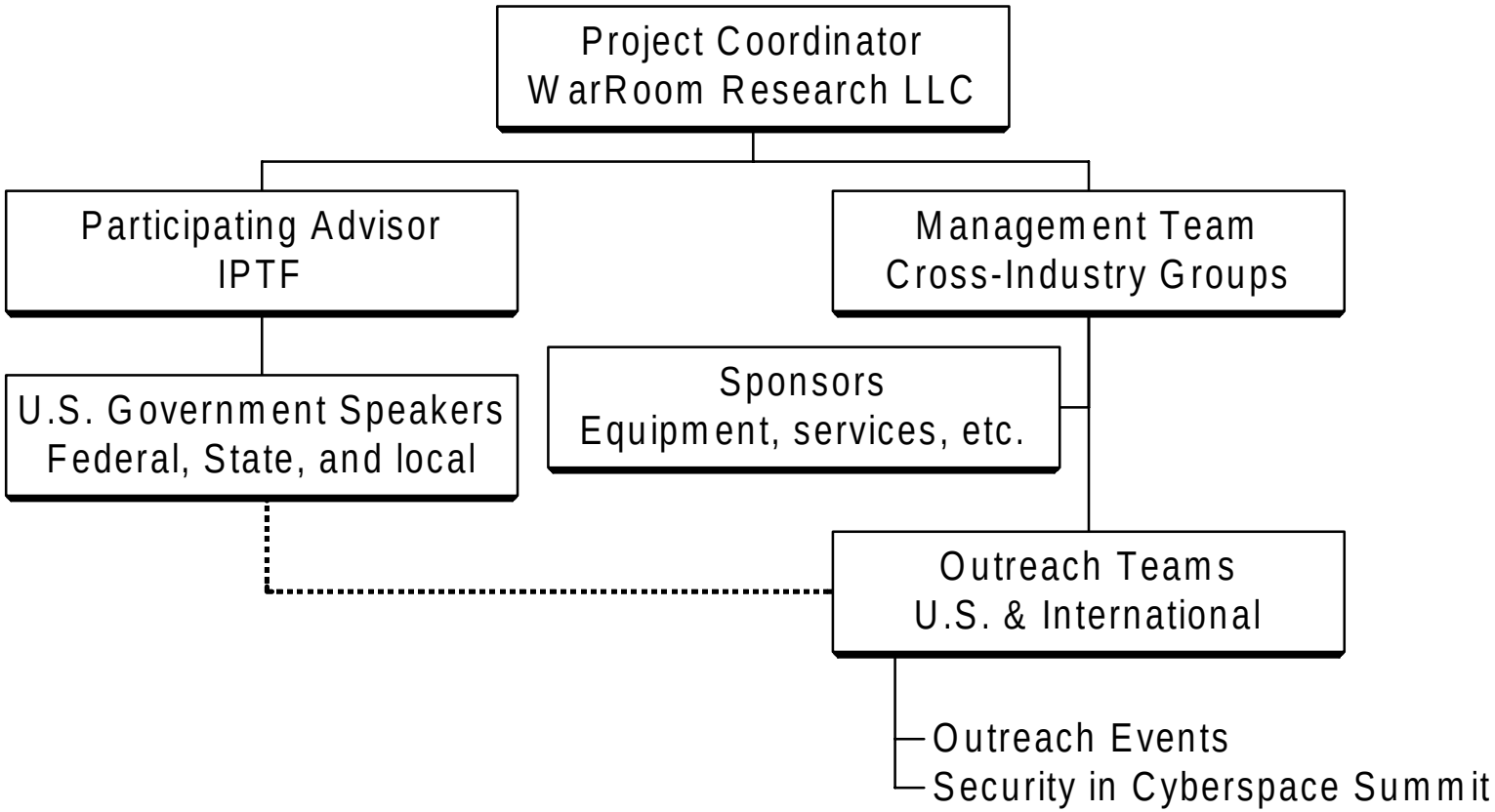
Manhattan Cyber Project

Organization

- Creative collaboration of leaders assembled to address challenges.
- WarRoom Research handles day-to-day administration as Project Coordinator.
- Infrastructure Protection Task Force proposed to handle government coordination as a Participating Advisor.
- Management Team assists in planning and overseeing project implementation.
- Sponsors provide equipment, services, etc.
- Outreach Teams provide educational programs and collect survey and other data/information -- estimated at 125+ organizations.

Manhattan Cyber Project

Operational Structure



Refer to http://www.WarRoomResearch.com/MCP for updated information.

Manhattan Cyber Project

Management Team & Sponsors

AXENT™

Bell Atlantic

ENRON

ERNST & YOUNG LLP

Georgia Tech Research Institute

IBM®

KING & SPALDING

SecurityDynamics

WarRoom Research

WheelGroup corporation

DELL

Refer to http://www.WarRoomResearch.com/MCP for updated information.

Manhattan Cyber Project

Outreach Events

- Employ an extended, security awareness outreach program that affects industry and government alike.
- Vehicle is an Outreach Team (U.S. and International) comprised of noted executives, practitioners, academics, and other professionals from diverse disciplines.
- Appearances include conferences, trade association meetings, online sessions, and special events -- estimated at 30 to 40 internationally.
- Themes or topics will vary and include an informative lecture, seminar, workshop, and hands-on demonstration -- war room.
- Security surveys and interviews will be conducted and later analyzed by various indicators -- war room.
- Team members are under Manhattan Cyber Project aegis -- project logo displayed with respective organizational logos.

War Room Facility

- Monitor and track project activities.
- Demonstrate and visualize cyber threat scenarios by:
  - displaying the critical junctures which vulnerabilities and threats exist to information and telecommunication systems; and
  - modeling cybercrime incidents and develop situational alarms.
- Maintain an executive action/issues management status board for an immediate team response.
- Coordinate cybercrime incidents with law enforcement -- option for anonymous reporting if desired.
- Link to portable war rooms used by Outreach Teams at events and “hands on” demonstrations.

Manhattan Cyber Project

Proposed Outreach Topics

- Access Control
- Antivirus & Malicious Logic
- Applications Program Security
- Business Continuity Planning
- Competitive Intelligence
- Computer and System Security
- Computer Emergency Response Team (CERT)
- Cryptography
- Data Classification
- Electronic Commerce
- Enterprise Security
- Financial Crimes
- Firewalls/Virtual Private Networks
- Information Ethics
- Information Warfare
- Internet Security
- Investigations/Computer Forensics
- Legal/Regulatory Issues
- Operations Security
- Organization Architecture
- Policy Development
- Risk Assessment/Management
- Security Awareness
- Telecommunications Security
- Year 2000
- Youth Programs

Manhattan Cyber Project

Outreach Team Criteria

- Candidates are selected on a first-come-first-serve basis and must be majority approved by the Management Team.
- Choose U.S. Team or International Team -- based on organization's ownership.
- Satisfy ONE of the following resource areas:
  - provide a leading edge technology or process that can help mitigate the cyber threat;
  - offer knowledge on a recognized, quality security program and how to implement it successfully;
  - demonstrate adverse effects of the cyber threat either in terms of security or competitiveness; or
  - share some “sanitized” data relating to intrusions and penetrations that can be added to the project’s database.
- Select a topic or theme that reflects the expertise and knowledge of the organization -- create one if not found.

Manhattan Cyber Project

Outreach Team Criteria (cont.)

- Choose to lead a single team and/or participate on single or multiple teams under the selected topic.
- Assist the chosen team on developing 2-3 products such as seminars, interviews, articles, data collection/analysis, etc.
- Develop a presentation for Security in Cyberspace Summit to include research papers, hands-on demonstrations, informative workshops, etc.
- Share in the project's development by contributing some degree of funding (value determined by candidate) -- small business and academia excluded.
- Agree NOT to market products or services while under the aegis of the Manhattan Cyber Project -- consequence is immediate removal from project.

Manhattan Cyber Project

Government Participation

- Government contact is the Infrastructure Protection Task Force created by Presidential Executive Order 13010, Jul 15, 1996.
- Act as a Participating Advisor to the project's Management Team and coordinate government involvement.
- Important and unique undertaking requiring many policy and legal reviews -- began in Dec 1996.
- Core IPTF talent is reflective of what government can bring to bear against the cyber threat -- real world threat briefings and liaison to law enforcement and other entities.
- More information on the IPTF is available on the Internet at http://www.fbi.gov.

IPTF Members

IPTF member agencies include:

- Federal Bureau of Investigation (Chair);
- Department of Defense;
- Defense Information Systems Agency;
- National Security Agency;
- Central Intelligence Agency;
- National Communication Systems;
- Department of Energy;
- Department of Justice;
- Department of Transportation;
- Department of Treasury;
- National Institute of Standards & Technology; and
- Federal Emergency Management Agency.

Manhattan Cyber Project

IPTF Disclaimer

Nothing in this briefing is intended to establish or imply the existence of any contractual relationship between WarRoom Research LLC (WRR) and the Infrastructure Protection Task Force (IPTF). The role of the IPTF will, at all times, be limited to the facilitative functions enumerated in Executive Order 13010, and IPTF conduct will be governed by that Order and other applicable federal authority. Similarly, nothing in this briefing is intended to imply that IPTF's participation in this project constitutes an endorsement by IPTF of any commercial product or service offered by WRR or any other participant in this project. The IPTF does not necessarily endorse the opinions of WRR and access to the IPTF is not limited to WRR or participants in the Manhattan Cyber Project initiative.

Manhattan Cyber Project

CYREC™

- Provide on-going organizational support to continue the work pioneered by the Manhattan Cyber Project.
- To be formed in late 1997 as a nonprofit education center to address the cyber threat and related cyberspace issues.
- Shared resource amongst industry, government, and academia.
- Operations limited to core education and research areas until infrastructure is established in 2nd Quarter 1998 to kick-off CERT and other operational activities.
- CYREC™ membership opened 2nd Quarter 1998 to non-Manhattan Cyber Project participants.
- Relevant Outreach Teams under the Manhattan Cyber Project will be offered corresponding CYREC™ positions.

CYREC™(continued)

- Objectives of this nonprofit center include:
  - sponsor technical and educational programs on a variety of cyberspace issues;
  - develop an accessible clearinghouse for open source data/information on the cyber threats and vulnerabilities;
  - offer CERT services incorporating a confidential reporting mechanism for high risk profiles;
  - foster emerging technologies and best practices;
  - outsource center activities such as research projects and technology transfer initiatives (cycled to ensure objectivity);
  - establish a backbone security team to counter cyber threats to corporate America and critical infrastructure areas; and
  - become a reliable source for expert opinion and testimony available to government, law enforcement, and industry.

Manhattan Cyber Project

Security in Cyberspace Summit

- Occurs as the last outreach event in Feb 1998.
- Three day, invitation only program.
- Leaders from industry, government and academia will identify and develop sessions as well as chair positions.
- Objectives are:
  - create a forum in which to analyze and present the findings of Manhattan Cyber Project;
  - designed for both business and technical mindsets;
  - review the mission of CYREC™ and its management structure, to include how government can actively participate; and
  - establish a semi-annual, private retreat for decision-makers to plan for future collaborations.
- Press conference held on final day to release findings to the public and announce next steps.

Manhattan Cyber Project

Anticipated Outcome

- Educate owners and operators of critical infrastructure areas and the general public to the cyber threat.
- Empower stakeholders through available and effective solutions -- technology, people, and processes.
- Raise the bar of pragmatic security to a higher level through realistic expectations of products and services.
- Enhance cooperation and understanding between industry, government, and academia -- sharing of data/information.
- Provide a shared resource in CYREC™ for continued collaborations to engage the cyber threat.

Manhattan Cyber Project

More Information...

Mark Gembicki
Project Coordinator for the Manhattan Cyber Project
Cofounder & Executive Vice President
WarRoom Research LLC
1134 Veranda Court
Baltimore, MD 21226-2211 USA

+1 410-437-1110
+1 410-437-1118 fax
info@WarRoomResearch.com
http://www.WarRoomResearch.com