Collaboration for the
Detection, Prevention, Mitigation and
Response to Cyber Attacks

Presented by
Steve Lines
Chairman DIB SCC Cyber Committee
CIO
CyberIQ
The Information Sharing Analysis Centers (ISACs) were created to empower information sharing and collaboration between the specific sectors that protect our Nation’s Key Resources and Critical Infrastructures.

The Defense Security Information Exchange (DSIE) is the Defense Industrial Base ISAC. The collaboration performed by the DSIE has been one of the most effective protections against the adversary today.

What does the future of collaboration space look like and how will collaboration improve.
Cyber Threat Environment

- Political Inspired Attacks
  - Terrorism
  - Nation State Attacks
  - Destabilization
  - Hacktivism

- Economic
  - Identity Theft
  - Blackmail
  - Bank Account Attacks (Organized Crime)
Cyber Threat Environment

☐ Social Networking
  ▪ Identity Theft
  ▪ Blackmail
  ▪ Surveillance
  ▪ Cyberstalking
  ▪ Child Pornography

☐ Legal
  ▪ Regulatory Requirements
  ▪ PII, PCI, HIPPA Data Standards and laws etc
The Disappearing Boundary

- The perimeter has vanished.
  - The risks now extend outside traditional network defenses.

- Mobile Devices
  - Your mainframe in your pocket!

- Cloud Computing
  - Computing outside the boundary

- Teleworking
  - Mixing home with work
  - BYOD

- Social Networking
  - Web 2.0
What are the Bad Guys Doing?
What are the bad guys doing?

- ShadowServer.org
  - 1600 Botnets monitored on a daily basis
  - Some 10,000 computers some > 250,000
  - They talk to each other every day!

  The New China Syndrome! The Advanced Persistent Threat! (APT)

- Time Magazine August 5, 2005
  - Titan Rain (Inside the Chinese Hack Attack)

- Business Week Reports April 10 2008
  - Operation Byzantine Foothold (Chinese infiltrate private industry)

- Russian Business Network (RBN)!
  - Pornography
  - Extortion
  - Host >60% of world's Cyber criminals
    - Resale of Personal Identities
    - Botnets
    - Fake Downloads to install malicious software

- Anonymous/Lutzsec
  - Hacktivism

Attacks are becoming much more sophisticated as the stakes rise!
Fake RBN Download

Protect Yourself.
Stop Spyware and Spam infecting your PC
Is Your Computer Infected?
Find out right now with our FREE Spyware Scan.
FREE SCAN

Some of the fastest-growing and dangerous threats on the Internet are spyware, adware, dowers and browser hijackers. Simple web-page browsing can cause you a lot of PC infections. That's why the very first thing a clever user should do is to protect his computer not only with anti-virus programs but with anti-spyware applications as well. AntiVirGear has proved to be one of the most effective protection solutions. It is the most advanced Spyware detection and removal application on the Internet available.

How AntiVirGear Can Help You?
If your PC is infected with spyware all your keystrokes, visited websites and even conversations can be recorded or monitored by someone who has secretly installed spy software on your PC. This person or company can steal your banking data, make Internet access slower, change browser homepage, etc.

Usually spyware is bundled with software downloads, attached to e-mails, or transmitted through networks. That's why many antivirus programs define it as legitimate software. Once installed, it can be hard to remove, and therefore, your computer will remain infected and your privacy will be at risk for a long time. We have developed a powerful tool – AntiVirGear – to help users detect and remove spyware and malware from their PCs.

Every PC owner has valuable and confidential personal information stored on his/her computer. This can include credit card and banking details, private e-mails and documents, shopping and browsing habits, etc. All this information should be protected from software intruders snooping. Are you sure your PC is protected?

Do you want to know whether it is infected or clear? Download FREE AntiVirGear scanner and check your PC now.

Customer Feedback...

"When I realised that my home computer was infected I tried a lot of anti-spyware programs. However, I was satisfied by AntiVirGear only. I want to say a huge thank you to the developers of such a brilliant program."
Megan N. Canada

"I was excited when I saw that annoying"
Anatomy of an Attack: The Advance Persistent Threat

- On September 13\textsuperscript{th}, a Defense Company discovered a critical “0” day vulnerability in Adobe’s Flash product. This issue was reported to US-CERT as well as Adobe.

- On September 17\textsuperscript{th}, 2011 several Defense Security Information Exchange (DSIE) members began seeing a dramatic increase in the number of targeted phishing attacks.

- The number of attacks reported to the DSIE from member companies increased on September 20\textsuperscript{th} and September 21\textsuperscript{st} to over 20 per day.

- The number of attacks for two days resulted in over 25 pages of different attack vectors and over 200 separate indicators.
Campaign Scale Attacks

- Phishing campaigns consist of multiple waves of targeted emails
  - Different senders and different attachments, but same campaign
Targeting

- Advanced threats targeted industry websites and portals
  - Compromise “Waterholes” – Places where members of a particular industry tend to browse regularly
  - Send links to spoofed websites to collect credentials/data
  - Send links to web pages hosting malware

- Same approach used in phishing email attacks
  - Command & Control Functionality
  - Exfiltration Capability
  - Modified to be undetectable by Anti-Virus
Other Attack Vectors

- **Botnets**
  - Mariposa (13 million computers)
  - Zeus
  - Botnets use distributed computing and resources
  - Excellent delivery mechanism for Warez or illegal software
  - Creates a buffer between the attacker and their victims
  - Shadowserver.org

- **Botnet Uses:**
  - Distributed Denial of Service (DDoS)
  - Spam/Phishing
  - Ad-ware
  - Click Fraud
  - Others...(malware distribution, Spyware, Rent a Bot!)

- **SCADA Attacks** *(supervisory control and data acquisition)*
  - Stuxnet
  - [Project Aurora](#)
Mobile Security Matures

We are now seeing attacks against all layers of mobile infrastructure:

- Applications
- Platform
- OS
- Baseband
- Network

*Mobile devices must be treated as fully fledged computers.*

*Do not assume they are "special".*
What are we doing about it?

Keeping a Secret
(While Sharing Broadly)

1 10 100 \cdots 10^9

Number of People With Access
Information Security Program

Links in the Security Chain: Management, Operational, and Technical Controls

- Risk assessment
- Security planning
- Security policies and procedures
- Contingency planning
- Incident response planning
- Security awareness and training
- Physical security
- Personnel security
- Certification, accreditation, and security assessments
- Access control mechanisms
- Identification & authentication mechanisms (Biometrics, tokens, passwords)
- Audit mechanisms
- Encryption mechanisms
- Firewalls and network security mechanisms
- Intrusion detection systems
- Security configuration settings
- Anti-viral software
- Smart cards

Adversaries attack the weakest link…Our Goal is not to be that link…..
Information Security Architecture
Weakest Link in the Chain

Clem the “Clicker”
User Awareness

- Do not share passwords.
- Do not open suspicious attachments
- Do not click on links in emails that you were not expecting
- Protect sensitive information.
  - For Official Use Only (FOUO), Sensitive But Unclassified (SBU), Personal Identifiable Information (PII), law enforcement sensitive, etc.
- Protect proprietary and customer information from disclosure.
- Secure all portable hardware and storage devices in desks, cabinets, etc.
- Report lost or stolen computer hardware and software to a local security manager, Corporate IT security and the Corporate legal department as soon as possible.
- Follow security procedures and policies as directed
Creating Partnerships
Simplify the Process

• Collaboration is cheap

• You can use other people’s money

• The Return on Investment is high

• You’re not admitting you were compromised, just that you found something

• Share the ‘known bad sites’, ip-addresses, malware

• Sharing should be voluntary and without attribution
Creating Partnerships

Homeland Security Presidential Directive 7
December 17, 2003

...To the extent permitted by law, Federal departments and agencies with cyber expertise, including but not limited to the Departments of Justice, Commerce, the Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support the organization in accomplishing its mission. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems...

Led to the establishment of the National Infrastructure Protection Plan (NIPP)
Creating Partnerships

National Infrastructure Protection Plan (NIPP) 2006

“The effective implementation of the NIPP is predicated on active participation by government and private sector security partners in robust multi-directional information sharing. When owners and operators are provided with a comprehensive picture of threats or hazards to critical infrastructure and key resources (CI/KR) and participate in ongoing multi-directional information flow, their ability to assess risks, make prudent security investments, and take protective actions is substantially enhanced.”
Creating Partnerships

The NIPP Framework and CIPAC

Critical Infrastructure Partnership Advisory Council (CIPAC): CIPAC is a partnership between government and private sector CI/KR owners and operators that facilitates effective coordination of Federal CI/KR protection programs. CIPAC engages in a range of CI/KR protection activities such as planning, coordination, NIPP implementation, and operational activities, including incident response, recovery, and reconstitution. DHS published a Federal Register Notice on March 24, 2006, announcing the establishment of CIPAC as a Federal Advisory Committee Act (FACA)-exempt body pursuant to section 871 of the Homeland Security Act
Summary of Information Sharing Organizations

- **DoD**
  - NII Cyber Task Force DCISE
  - Government Coordinating Council
  - Cyber Command
  - Service Commands
  - Defense Cyber Crime Center (DC3)
  - Defense Critical Infrastructure Program (DCIP)

- **DHS and the National Infrastructure Protection Plan**
  - Sector Coordinating Councils (SCC)
  - Critical Information Partnership Advisory Council (CIPAC)
  - Defense Security Information Exchange (DSIE)
  - Network Security Information Exchange (NSIE)
  - Information Sharing Analysis Centers (ISAC)
  - National Security Telecommunications Advisory Council (NSTAC)
  - Office of the Protected Critical Infrastructure Information (PCII)

- **FBI**
  - InfraGard
  - Domain

- **USSS**
  - Electronic Crimes Task Force
Summary of Information Sharing Organizations (more)

- Global Justice Information Sharing Initiative
- National Criminal Intelligence Sharing Plan
- Markle Foundation Task Force: Creating A Trusted Network For Homeland Security
- 9/11 Commission Report and Recommendations
- Law Enforcement Regional Data Exchange
- Intelligence Community Information Sharing Working Group
- Community Interoperability and Information Sharing Office Policy Board
- DOJ-DHS Ad Hoc Working Group on SBU-level Information Sharing Systems
- National Virtual Pointer System Coordinating Committee
- Justice Intelligence Coordinating Council
- Homeland Security Advisory Council Working Group
- National Association of State Chief Information Officers
- Joint Terrorism Task Force
- Etc, Etc, Etc
Who’s in Charge?

- National Cyber Security Division (NCSD)
- National Cybersecurity and Communications Integration Center (NCCIC) (*combined NCS with US-CERT*)
- National Security Agency
- Defense Cyber Crime Center (DC3)
- Cyber Command
- US Service Commands
- Etc, Etc...

With all of these organizations, effective sharing between private industry and government still does not exist today!
Why can’t we all just get along?

Barriers to Information Sharing

These include:

- **Trust**
  - Let’s share our most embarrassing moments…You first!

- **Information is power**

- **Culture differences**

- **Legal barriers**

- **Classified programs**
  - Need to know vs. need to share

- **Liability issues**

- **Contractual obligations**

- **Stockholder value**
Legal Barriers to Information Sharing

- Restrictions of sharing intel information to law enforcement led to 9/11*
  - Differences in missions, cultures and legal authorities
  - Foreign Intelligence Surveillance Act (FISA) 1978

- Need to share
  - Bremmer’s National Commission on Terror 2000
    “Law enforcement agencies are traditionally reluctant to share information outside of their circles so as not to jeopardize any potential prosecution.”

*107th U.S. Congress, Select Committee on Intelligence
Trust

It has to be true!
I saw it on the Internet!

On the Internet, no one knows you’re a dog.

Risk = Threat x Vulnerability x Cost
Risk x (Threat + Vulnerability) = Compromise
Trust

Not everyone is a good person…

Risk x (Threat + Vulnerability)= Danger
Trust

Not everyone is a good person…

Risk x (Threat + Vulnerability) = Danger
Defense Security Information Exchange (DSIE)

Cyber Sub-Council of the DIB SCC
History of Partnerships

DSIE Concept was developed from the Network Security Information Exchange (NSIE)

• National Communication System (NCS) founded in 1962
• National Security Telecommunications Advisory Committee (NSTAC) was formed in 1989
• Government and NSTAC Network Security Information Exchanges (NSIE) were established in 1991
• Four DIB members of the NSIE started the formation of DSIE in 2007
• DSIE was formed in 2008 as a Sub-Council of the DIB Sector Coordinating Council
• Currently the DSIE consists of over 60 companies with over 300 security engineers sharing information daily
<table>
<thead>
<tr>
<th>Kill Chain</th>
<th>Detect</th>
<th>Deny</th>
<th>Disrupt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Acquisition</td>
<td>Define objectives &amp; establish targets</td>
<td>Minimize attack surface</td>
<td>Target Shielding</td>
</tr>
<tr>
<td>Reconnaissance</td>
<td>Probing attempts to external web sites and firewalls</td>
<td>Pattern recognition detection</td>
<td>Misdirection</td>
</tr>
<tr>
<td>Weaponize</td>
<td>Determine which vulnerability to exploit “0” day if possible</td>
<td>Intelligence on tools and techniques</td>
<td>Dark fiber and CI Operations</td>
</tr>
<tr>
<td>Delivery</td>
<td>Which method, malicious web site? phishing email?</td>
<td>Prevention through predictive analysis</td>
<td>Spoofed pathways</td>
</tr>
<tr>
<td>Exploit</td>
<td>Redirect black hole/honeynet</td>
<td>Mitigation</td>
<td>In line disruption of attack traffic</td>
</tr>
<tr>
<td>Compromise</td>
<td>Reverse engineer malware</td>
<td>Effectively block compromise</td>
<td>Honey Pot/net spoofed target</td>
</tr>
<tr>
<td>C2</td>
<td>Intelligence network of Big Data</td>
<td>Active list to prevent exfiltration/malware</td>
<td>Encrypt traffic with new key</td>
</tr>
<tr>
<td>Exfiltration</td>
<td>Data loss &amp; prevention</td>
<td>Pattern recognition</td>
<td>Encrypt spoofed data</td>
</tr>
</tbody>
</table>
Government at the federal, state, and local level must actively collaborate and partner with the private sector, which controls 85 percent of America’s infrastructure. . . . the nation’s infrastructure protection effort must harness the capabilities of the private sector to achieve a prudent level of security without hindering productivity, trade, or economic growth.

—The President’s National Strategy for Homeland Security
Responsibility

In the end, it all comes down to this:

- Cyber Security is everyone’s responsibility
- Be Informed!
- Get involved!
- Develop a Plan!
- Partnership works!
Responsibility

“The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.”

Sun Tzu
The Future

- Cyber Security is still in its infancy
- Most solutions focus on endpoints and not a comprehensive mature process
- Cyber programs tend to be ad hoc focusing on compliance rather than security (C&A= CYA)
- Reactive rather than Proactive
- Need to focus on the attacker, not the technique
- We need more dedicated Cyber Security research professionals
QUESTIONS?

What did he say?

Why did he take so long?

Could you repeat everything after "good morning"?

Could you talk a little longer?
Still catching up on emails.
For More Information

Steve Lines, CISSP, CISA, CISM, CBCP
CIO CyberIQ
Phone 703-344-4522
slines@cyberiq.com