



Security in knowledge

Cyber Attacks

The Call for Retaliation and the Legal Ramifications

Moderator:

John E. Jorgensen, CEO
The Sylint Group, Inc.

Panelists:

Ms. Stacy Arruda, Special Agent
Federal Bureau of Investigation

Steven Tepler, Esq.
Kirk-Pinkerton, PA

Charly Shugg, BG USAF Ret.
VC Air Force Cyber Command
The Sylint Group, Inc.

Serge Jorgensen, CTO
The Sylint Group, Inc.

Session ID: LAW-R33

Session Classification: Intermediate

Agenda

- ▶ Cyber Attacks
 - ▶ Source & Sophistication
 - ▶ International Intelligence Operations
 - ▶ Anonymous
 - ▶ Sophisticated Organized Crime
 - ▶ Targets and Costs
 - ▶ Intellectual Property
 - ▶ PII, PCI and PHI
 - ▶ Malicious
 - ▶ The “Unwitting” Proxy
 - ▶ Major Corporations
 - ▶ Small Companies

Agenda (Continued)

- ▶ The Call For Retaliation
 - ▶ Who is Responsible?
 - ▶ What Can Be Done?
 - ▶ Legal Consequences?
- ▶ The Future Litigation
 - ▶ Aiding and Abetting
 - ▶ Damages Through Ignorance
 - ▶ The International Flavor
 - ▶ Cyber Warfare
- ▶ What is Your Proposal
 - ▶ How Will That Happen?
 - ▶ Who Will Make It Happen?

Applied Results

- ▶ Understanding the Cyber Security issues of responsibility
- ▶ Can litigation be pursued with positive results
- ▶ The legal ramifications of retaliation
- ▶ What the legal process might be
- ▶ The potential pitfalls

Cyber Attacks The Call for Retaliation



Security in knowledge