JANUS Associates

Cyber Warfare
The Reality Is We Are All Under Attack

Presented to: 2013 NYS Cyber Security Conference
Presented by: Matthew J. Lane, CIO
About JANUS Associates

Focused on Information Security and Business Continuity consulting since 1988

- Founded 1988, the oldest IT Security consultancy in the nation
- Privately held, woman-owned small business
- 25 Years serving government and business
- Locations in Stamford, Boston, Baltimore, Hartford
JANUS Areas Of Expertise

- Risk Management
- Information Security & Privacy
- Risk/Vulnerability Assessments
- Cloud Assessment and Security Services
- Smart Grid Assessment and Security Services
- Information Assurance
- Business Continuity and Disaster Recovery Planning
- Regulatory Compliance
- Security Awareness & Training
- 3rd Party Vendor Assessments
- Policy and Procedures
- Computer Forensics
“An integral part of warfare, the Peoples Liberation Army identifies Electronic Warfare as a way to reduce or eliminate U.S. technological advances.”
Annual report to congress, May 2013, Office of the Secretary of Defense

“I stand back in awe of the breadth, depth, sophistication, and persistence of the Chinese espionage effort against the United States of America.”
Former CIA and National Security Agency director Michael Hayden

“Well, there’s no question that if a cyber-attack, you know, crippled our power grid in this country, took down our financial systems, took down our government systems, that that would constitute an act of war.”
Secretary of Defense Leon Panetta
Definitions

- Hacker
  - Made innovative modifications to electronics
  - Modified Software
  - Broke into Phone Systems
  - Circumvents Computer Security
Definitions

- Hacker
- **Hacktivist**
  - Political Motivation
  - Social Motivation
  - Non-violent
  - Independent
Definitions

- Hacker
- Hacktivist
- Cyber Terrorist
  - Political Motivation
  - May be Violent
  - May be state sponsored
Definitions

- Hacker
- Hacktivist
- Cyber Terrorist
- **Cyber Criminal**
  - Financially Motivated
  - Ties to Organized Crime
  - Majority in Eastern Europe
Definitions

- Hacker
- Hacktivist
- Cyber Terrorist
- Cyber Criminal
- **Cyber Warrior**
  - State Sponsored
  - Traditional war activities
What is a Cyber War?

- A political mechanism to force another group of people to change and act differently
What is a Cyber War?

- A political mechanism to force another group of people to change and act differently
- An organized, prolonged, military conflict between sovereign entities
What is a Cyber War?

- A political mechanism to force another group of people to change and act differently
- An organized, prolonged, military conflict between sovereign entities
- It effects violence, aggression, and mortality
What Are Cyber Warriors After?

In the past the bad guys were after financial gain.

Today they are after everything

- Log On Information (User ID’s & Passwords)
- Credit Card Information
- Intellectual Property
- Corporate Confidential Information
- Documents, Spreadsheets, Email, Images
- Access to Manufacturing Process Control
The Components of Cyber Warfare

- Reconnaissance
The Components of Cyber Warfare

- Reconnaissance
- Espionage
The Components of Cyber Warfare

- Reconnaissance
- Espionage
- Arms Proliferation
The Components of Cyber Warfare

- Reconnaissance
- Espionage
- Arms Proliferation
- Aggression
Cyber Warfare Distribution of Targets

Distribution Of Targets
March 2013

* Source: hackmageddon.com

Industry Fragmentation
March 2013

Organization Fragmentation
March 2013

* Source: hackmageddon.com
Cyber Warfare Distribution of Attack Techniques

Distribution of Attack Techniques
March 2013

- DDoS: 50.6%
- SQLi: 13.5%
- Targeted Attack: 9.3%
- Unknown: 8.6%
- Account Hijacking: 6.8%
- Defacement: 5.6%
- Unspecified Malware: 4.3%
- CCTV Hack: 1.2%
- DNS Hijacking: 0.6%
- iFrame Infection: 0.6%
- Proxy Misconfiguration: 0.6%
- Vulnerability in ASP page: 0.6%
- XSS: 0.6%
- N/A (Botnet): 0.6%

* Source: hackmageddon.com
So Easy: A Six Year Old Can Do It!
Properly Responding To A Cyber Attack

- First Step – Plan in Advance
  - Update Your Plan on a Regular Basis
  - Do a Table Exercise and Test Your Plan
- Notify the Proper Authorities
- Isolate and Protect Compromised System
- Document Everything
- Discuss on a Need to Know Basis
How NOT To Respond To A Cyber Attack

- Hack-Back-Attack

---

**Israeli Elite**
@IsraeliElite

We are the Israeli Elite Force. BOW DOWN! Wanna join? #IEF @ efnet
(for email browse the tweets)
How NOT To Respond To A Cyber Attack

- Hack-Back-Attack
- Escalate to traditional warfare
How NOT To Respond To A Cyber Attack

- Hack-Back-Attack
- Escalate to traditional warfare
- Buy more bandwidth
How NOT To Respond To A Cyber Attack

- Hack-Back-Attack
- Escalate to traditional warfare
- Buy more bandwidth
- Move to the Cloud
How To Tell If Your Safeguards Are Effective

- Internal Testing
How To Tell If Your Safeguards Are Effective

- Internal Testing
- 3rd Party Testing
How To Tell If Your Safeguards Are Effective

- Internal Testing
- 3rd Party Testing
- Cost Benefits
How To Tell If Your Safeguards Are Effective

- Internal Testing
- 3rd Party Testing
- Cost Benefits
- What Should be Tested?
Test Sample: Spear Phishing

- Purchase a similar looking domain
Test Sample: Spear Phishing

- Purchase a similar looking domain
- Set up an email for the domain
Test Sample: Spear Phishing

- Purchase a similar looking domain
- Set up an email for the domain
- Identify suspect classes of users
Test Sample: Spear Phishing

- Purchase a similar looking domain
- Set up an email for the domain
- Identify suspect classes of users
- Craft e-mail messages to each class of user
Test Sample: Spear Phishing

- Purchase a similar looking domain
- Set up an email for the domain
- Identify suspect classes of users
- Craft e-mail messages to each class of user
- Create Click Based attacks
Test Sample: Spear Phishing

- Purchase a similar looking domain
- Set up an email for the domain
- Identify suspect classes of users
- Craft e-mail messages to each class of user
- Create Click Based attacks
- Create attachment based attacks
Test Sample: Spear Phishing

- Purchase a similar looking domain
- Set up e-mail for the domain
- Identify suspect classes of users
- Craft e-mail messages to each class of user
- Create Click Based attacks
- Create attachment based attacks
- Generate statistics to improve process
Questions and Answers

JANUS Associates
1055 Washington Blvd.
Stamford, CT 06901
www.janusassociates.com

Matthew J. Lane, CIO
Office: 203-251-0229
matthewl@janusassociates.com

Lyle A. Liberman, COO
Office: 203-251-0236
lylel@janusassociates.com