Cyber-Security and the Need for Strategic Collaboration

March 2, 2016
On June 6, 2012, Secretary Napolitano announced the formation of a Task Force on CyberSkills with a two-part mandate:

First, to identify the best ways DHS can foster the development of a national security workforce capable of meeting current and future cybersecurity challenges; and

Second, to outline how DHS can improve its capability to recruit and retain that sophisticated cybersecurity talent.
The numbers of professionals with cybersecurity mission-critical skills are so limited that government contractors and federal agencies compete with one another and the private sector to hire them.

DHS Homeland Security Advisory Council’s Cyberskills Task Force Report (Fall 2012)
Competition for Resources

- Washington Post report (May 2012) forecasted 50,000 cyber security jobs in the near future in the federal government and private industry.
- Career Builder (August 2013) reflected 973 openings (using Cyber Security in a keyword search)
- The demand for skilled workers and training professionals by the government and private sectors are expected to remain high

Cybersecurity is Getting More Complex

  - “gear up for accelerated change and complexity in 2014, especially in cybersecurity, data privacy and big data.”
Cyber Attacks are known in particular for their anonymity.

- Since cyber-attackers are known for their anonymity, understanding ‘who’ conducts an attack often requires a deeper examination of ‘why’ the attack was conducted and then ‘how’ it was conducted.

Consider your vulnerability to cyber-attacks from the perspective of why, how, & who.

- Objectives
- Methods
- Actors
Objectives

- Confidentiality
- Integrity
- Availability
- Destruction
Actors

- Criminal
- Nation-States
- Terror Groups
- Hacktivists
- Insider Threats*
How are “Cyber Attacks” conducted?

- Social Engineering
- Spearphishing
- Malware
- Distributed Denial of Service (DDoS)
- Advanced Persistent Threat (APT)
- Mobile Applications
- Accidental Data Spills
- Insider Threat
Diagnosing your Vulnerability

Objective
- Confidentiality
- Integrity
- Availability
- Destruction

Method
- Spearphishing
- Insider Threat
- DDoS
- Malware
- APT

Actor
- Criminals
- Hacktivists
- Terror Group
- Nation-State
Can you provide me with an example of an Accidental Data Spill?
Super Bowl XLIX

Broadcasting the SSID and password on national tv for the Super Bowl security command center is probably bad. ow.ly/i/4t9f9

 hide photo
 reply 3 retweeted favorite more

CBS MORNING
SUPER BOWL SECURITY INSIDE SECRET, FIRST-OF-ITS-KIND COMMAND CENTER TAKES ON OLD-FASHIONED EYE ON THE BALL

view on web

retweets favorites
123 27
Cyber Security: Layered Defense

**User**
- Training
- Anti-Virus
- Authentication
- Protect Social Media Content

**Network**
- Firewall
- Proxy Servers
- Secure Socket Layer
- DDoS Protection
- Load Balancers
- Multi-factor Authentication
- Intrusion Detection
- Log Audits
Multi-Factor Authentication

- Something you know
- Something you have
- Something you are
Physical Security is Getting More Complex
Complexity

Rate of Change

# of Factors That Change

COMPLEXITY

R of C # of Factors That Change
Information Needs

Rate of Change

# of Factors That Change

Information needs are not known
Cooperation v. Collaboration

- Cooperation
  - Need to

- Collaboration
  - Want to
Solving Problems and Conflicts

Diagram:
- Assertive: Competing, Collaborating
- Passive: Avoiding, Accommodating
- Uncooperative to Cooperative
- Compromising at the center
Cybersecurity, Complexity, and Strategic Collaboration

- The cybersecurity challenge facing entities is too complex to be tackled by superstars and individual blue-chip players.

- Cooperation and simple collaboration can not increase the U.S. cybersecurity capacity needed for a secure existence in the information/communication world.

- The need for strategic collaboration is the only way to approach cybersecurity.
An intentional, collective approach to address public problems or issues through building shared knowledge, designing innovative solutions, and forging consequential change.

(Norris-Tirrell & Clay, 2010, p. 2)
Strategic Collaboration Yields...

- More knowledge and innovation
- Accelerated maturity of cybersecurity capabilities
- Less learning costs / less trial-and-error
- Optimal partners for strategic needs
- Stronger relationships amongst partners
- More competitive grant/funding applications
- Focus
- Increased cybersecurity capacity
Positive, sustainable impacts

Long-term stakeholder commitment to policy or program change

Increased capacity of individuals and organizations to effectively work together

...LETS TALK CAPABILITIES AND CAPACITY BUILDING
Today will make you ask more questions
Dr. William M. Toms
732-851-4824

bill@thetomsprofessionalgroup.com