Above My Pay Grade:
Incident Response at the National Level

Jason Healey
Atlantic Council
Traditional Incident Response
But at the national level, incident response is a different game

Implications for
- Misunderstandings between geeks and wonks
- Attribution
- Decision making
- Large-scale response (or miscalculations about response)
EXAMPLE:

LARGE SCALE ATTACK ON FINANCE
Large-scale Attack on Finance Sector

Who Is Their First External Call To?

- Bank A
- Bank B
- Exchange
- Clearing House
First: Call a Law Firm!
Then Mandiant or CrowdStrike!
After That: Tell the Cops...

- Bank A
- Bank B
- Exchange
- Clearing House

FBI
USSS
Then Share within the Sector

- **Operational** sharing and crisis management
  - Shared with *all* financial institutions
  - Sector-wide incident response via audioconfernce ‘bridge’ line
  - Typically heard:
    - “What’s the vulnerability?”
    - “Is there a patch?”
    - What IP addresses?
    - “What works to mitigate?”
When More than Tech Discussions Are Needed...

Policy-Level Incident Response

- Senior company and government executives across all sector and regulators
- Management response via audio bridge
- Typically heard:
  - “How healthy is the sector?”
  - “What do we do if it gets worse?”
  - “Can markets open as normal tomorrow?”
If Markets are Melting...

Within Treasury
- Escalate to the senior leadership, especially political appointees

Bank A
Bank B
Exchange
Clearing House

Treasury
FSSCC
FBIIC
FS/ISAC
Other ISACs
Water, Energy, Telecom...
If Markets are Melting...

Highest Level of Financial Decision-making

- No different than any other financial crisis!
- Secretary, Chairs of FRB, SEC, CFTC
The *Cyber* Response...

- Bank A
- Bank B
- Exchange
- Clearing House
- President’s Working Group on Financial Markets
- Treasury
- FSSCC
- FBIIC
- FS/ISAC
- Other ISACs: Water, Energy, Telecom...
- DHS

Department of Homeland Security

- *But what does that actually mean?*
- *And what then?*
The Cyber Response...

National Cybersecurity and Communications Integration Center
- 24/7 operations floor
- Includes US-CERT, ICS-CERT, NCC

- Bank A
- Bank B
- Exchange
- Clearing House
- FS/ISAC
- Other ISACs Water, Energy, Telecom...

- FSSCC
- FBIIC

- President’s Working Group on Financial Markets
- Treasury

- DHS
- CIA
- DoD
- Treasury
- FBI
- USSS
- State & Local
- FS-ISAC
- Justice
- NSA
- Others
- State
A “Significant Cyber Incident ... requires increased national coordination” as it affects

- National security
- Public health and public safety
- National economy, including any of the individual sectors that may affect the national economy or
- Public confidence

Cyber Unified Coordination Group
Cyber UCG IMT

FS/ISAC

Other ISACs
Water, Energy, Telecom...

DHS
NCCIC

Operational Response

President’s Working Group on Financial Markets

Treasury

FBIIC

FSSCC

Bank A

Bank B

Exchange

Clearing House

NTOC
USCC

Telcos

black hat
USA 2013
Who Coordinates Above DHS?
Who Coordinates Above DHS?
Who Coordinates Above DHS?
If Incident Needs Escalation

- Bank A
- Bank B
- Exchange
- Clearing House

President’s Working Group on Financial Markets

Treasury

FSSCC <-> FBIIC

FS/ISAC

Other ISACs
Water, Energy, Telecom...

National Security Council
- Cyber Directorate
  - ICI-IPC
  - Cyber Response Group

Policy Response

DHS NCCIC
- Operational Response

DHS, CIA, DoD, FBI, NSA, State, Others

“The Interagency”
If Incident Needs Escalation

President’s Working Group on Financial Markets

Treasury

FSSCC

FBIIC

Bank A

Bank B

Exchange

Clearing House

FS/ISAC

Other ISACs
Water, Energy, Telecom...

NCCIC

DHS

ICIC-IPC

Cyber Response Group

Deputies Committee

Cyber Directorate

National Security Council

DHS

CIA

DoD

FBI

NSA

State

Others

“The Interagency”
If Incident Needs Escalation

Policy Response

Principals Committee
Deputies Committee
Cyber Directorate
ICI-IPC Cyber Response Group

Operational Response

DHS NCCIC

Other ISACs
Water, Energy, Telecom...

Bank A
Bank B
Exchange
Clearing House

President’s Working Group on Financial Markets
Treasury
FSSCC
FBIIC

President of the United States

DHS
CIA
DoD
FBI
NSA
State
Others

“The Interagency”
Why This Works

• Since
  – Worst-impact cyber conflicts generally caused by nations, not individuals and
  – Cyber conflicts tend not to be “network speed”

• Process translates “cyber crisis” out of technical channels

• Into the time-tested traditional national security crisis management

• Countries with NSC equivalents have natural edge to those without ... like China
Why This is a Good Thing:
Provides Process for Tough Decisions

- Enables national-level technical response options
- Commitment of additional resources to help private sector response
  - Money, personnel, intelligence
- Determine “what nation is responsible?”
- Enables response using levers of national power:
  - Diplomatic, economic and yes, military
Why the Process Might Not Work or Otherwise Suck:

• It doesn’t always work even for physical crises!
• When government wants to control the response
• The “Katrina” of something on the edges of the system
• The “Six-Day War”
• True Cyber War
Why the Process Might Not Work:

If We Are At Cyberwar!

- President's Working Group on Financial Markets
- Treasury
- FBIIC
- FSSCC
- FS/ISAC
- Director FBI
- DHS
- NCCIC
- UCG
- Operational Response
- Military Response
- NTOC
- Regional COCOM
- SECDEF, CJCS
- President
- Principals Committee
- Deputies Committee
- Cyber Directorate
- ICI-IPC
- Cyber Response Group
- Governors
- Bank A
- Bank B
- Exchange
- Clearing House
- President's Working Group on Financial Markets
- FBIIC
- FSSCC
- FS/ISAC
- Director FBI
- DHS
- NCCIC
- UCG
- Operational Response
- Military Response
- NTOC
- Regional COCOM
- SECDEF, CJCS
- President
- Principals Committee
- Deputies Committee
- Cyber Directorate
- ICI-IPC
- Cyber Response Group
- Governors
- Bank A
- Bank B
- Exchange
- Clearing House
Inside the Beltway, they forget the real response, the *real* battle isn’t in DC but at the banks under attack and in the private-sector networks.
QUESTIONS?

Cyber Statecraft Initiative

• International conflict, competition and cooperation in cyberspace
• Publications (all at our website, acus.org)
• Public and Private Events

jhealey@acus.org  Twitter: @Jason_Healey