Global Aggregation of Cyber Risks:  
“Finding Cyber Sub-Prime”

2nd International Conference on Cyber-crisis Cooperation and Exercises  
23-24 September 2013 | Athens, Greece
“Cyber” just means interconnected IT, but that increasingly means *everything*

**Common Terms:**
- Intrusion, hack
- Cybercrime
- Carders
- Russia, East Europe
- Stolen identity, credit cards, records
- Extortion

**Internet**

**Criminals**
- Hactivists
- Spies
- Militaries

**Steal individual records with personal info to sell**

---

September 2013

Global Aggregation of Cyber Risk
Zurich and Atlantic Council
Traditional Cyber Threats

Common Terms:
- Intrusion, hack
- DDoS (distributed denial of service)
- Anonymous
- Patriotic hackers

Disrupt network or steal sensitive or embarrassing info

Internet

Criminals
Hactivists
Spies
Militaries

Corporation X
Traditional Cyber Threats

Common Terms:
- Intrusion, hack
- IP Theft
- China
- Advanced Persistent Threat

Internet

Criminals
Hactivists
Spies
Militaries

Steal R&D, business plans or negotiating strategies

Corporation X

September 2013
Global Aggregation of Cyber Risk
Zurich and Atlantic Council
Traditional Cyber Threats

Common Terms:
- Stuxnet
- Shamoon
- Iran, US, China
- Cyber war, cyber conflict

Disrupt network or systems or even upstream Internet – very rare

Criminals
Hactivists
Spies
Militaries

September 2013
Global Aggregation of Cyber Risk
Zurich and Atlantic Council
Non-Traditional Cyber Threats

The Cloud

Wireless Implantable Medical Devices

Deep Brain Neurostimulators

Cochlear Implants

Gastric Stimulation

Cardiac Defibrillators/Pacemakers

Foot Drop Implants

Insulin Pumps

Smart Grid

The Internet of Things
But This is All at the Level of Individual Organization

What About the Systemic Risks?

Mainstream cyber risk management is markedly similar to that for financial prior to 2008!
Cyber Sub-Prime

• Cyber is in the same place finance was prior to 2008
• Examination of cyber risk pools
• Analysis of key factors
• Recommendations
Cyber Sub-Prime

Cyber is in the same place finance was prior to 2008

• Risk only examined one organization at a time
• Risks passed outside organization into unknown pools
• Little if any governance of the system as a whole and complex interdependencies ignored
• Led to catastrophic global failure, even for those organization which handled internal risks correctly!
• We are heading for similar fate with global aggregation of cyber risk
Overlapping Pools of Systemic Cyber Risk

**Outsourced and Contract**
- China, India
- Manufacturing
- Professional: HR, legal, accounting, consultancy
- Defense industrial base

**Upstream Infrastructure**
- Electrical, finance
- Bandwidth and Internet infrastructure like IXPs, submarine cables, security tokens
- Embedded devices: ICS, SCADA
- Some key companies: MSFT
- Networking standards like BGP and DNS
- Internet governance

**External Shocks**
- Conflicts, malware pandemics
- States: China, Russia, US
- Non-states: Activists, Anonymous, organized crime
- Intrusion, disruption, theft of IP, espionage

**Counterparties and Partner**
- Trusted interconnections
- Dependence

**Supply Chain**
- China
- Counterfeit components, software
- Global logistics chain

**Disruptive Tech**
- Internet of everything and digital economy largely w/o human intervention
- Embedded medical, human enhancement, driverless cars, etc

**Internal Enterprise**
- Desktop, server, data centers, networks, security
- Software: in-house, legacy, custom, commercial, open source,
Every year, technology and business processes push us further up and to the right!

Mitigated by risk management, resilience contracts, SLAs, MOUs

Mitigated government action, resilience, standards, regulations

Global Aggregation of Cyber Risk
Zurich and Atlantic Council

September 2013

Most Control
Least Control
Notional Chart of Upstream Risks
Three Zones of Risk (?)

**Distant**
- **Mitigated by**
  - Government actions
  - Resilience
- **External Shocks**
  - Causal
  - Upstream of all else

**Everywhere**
- **Mitigated by**
  - Standards
  - Regulations
  - Governance
  - Resilience
- **Disruptive Tech**
  - Upstream Infrastructure
  - Tight linkages
  - More so over time

**Near**
- **Mitigated by**
  - SLAs
  - Contracts
  - MOAs/MOUs
  - Resilience
- **Outsourced and Contract**
  - Counterparties and Partner
  - Internal Enterprise
  - Info only

Over time, more business critical functions move upstream...

September 2013
Analysis: The Upside

• Few if any single shocks could affect cyberspace in any way that could transfer into a strategic shock to the global economy
  • Defenders are excellent at responding
  • System has been extremely resilient day-to-day and year-to-year
Analysis: The Downside

- Three separate vulnerabilities: interconnectedness and complexity, lack of transparency, and lack of either local control or system-wide governance
  - Everything increasingly interdependent in unknowable ways
  - Tech and business models continue to push major risks away from management understanding and control
  - No system-wide governance
  - In the face of catastrophic failures, not clear who would be in charge or what levers they could use
  - Few backup paths for crisis communication or manual workarounds
Therefore

- Main concern is a failure of multiple key elements could lead to cascading failures
  - Where is the next Lehman? The next sub-prime?

Expected future: Organizations will suffer ever more frequent shocks like natural disasters ... too severe to ever be able to sufficiently protect
How?

• Either one shock that cascades completely out of control or multiple shocks which cascade and reinforce one another

• Examples: California earthquake, large cloud provider goes bust (Enron-style fraud, Lehman-style misunderstanding of risk, etc), major routing protocol failure or attack, slow deterioration of resilience and defenses over time, major GPS outage takes out global precision navigation and time signals
Three Recommendations for Companies

1. Organizations can take **basic and advanced mitigations**, depending on their maturity and resources.
2. However, since so much risk is external, complex, and interdependent then **resilience is the main hope for companies**.
3. Board-level **strategic risk management** including insurance and other risk transfer options.
Two Recommendations for Governments and System-Wide Organizations

1. Far more focus on systemic rather than organizational risk
2. Eventual goal for defense to be better than offense
Need for Strategic Exercises

• Many exercises look only to the technical or organizational levels for solutions
• Private sector companies are unaware of what strategic decisions are being made until it is too late
• Event non-cyber disasters can cause unknown threats
Global Aggregation of Cyber Risks: “Finding Cyber Sub-Prime”

2nd International Conference on Cyber-crisis Cooperation and Exercises
23-24 September 2013 | Athens, Greece