NATIONAL INTELLIGENCE UNIVERSITY

EDUCATION RESEARCH OUTREACH

Supply Chain Risk Management: Viewing ICT Supply Chains as Complex Adaptive Systems

Christopher M. Hines
Dr. Michael W. David

Overview

- Introduction
- Methodology
- Concepts
- Cases / Analyses
- Conclusions
- Recommendations
- Questions?

Introduction

- Supply chain risk management (SCRM) issues - addressed by USG for decades
- Simple supply chains have become very intricate:
  - Multiple contracts are needed to design, run, maintain ICT networks
    - Has led to increased risk
      - SCRM must therefore become more resilient and secure
        - **Use of complexity theory can serve as a possible tool kit for control of risk**

Introduction (contd.)

Methodology - Case Study Format

- Recent examples
- Lack of scholarly work on complexity theory applied to ICT SCRM
- Three case studies:

1. Public/Private Survey of global cybersecurity climate (Vanson Bourne and CrowdStrike)
2. “Air Force Space Command Supply Chain Risk Management of Strategic Capabilities” (DoD OIG review)
3. “The Big Hack” and its implications for motherboard and server security (Bloomberg)

Background - Concepts

- **“Operational Complexity”**
  - Direct result of WWII combat
  - “Mixed Teams” – Group of specialized analysts (SMEs)
- **Complexity** - a function or process where the number of interactions between components increases dramatically causing things to become quickly unpredictable.

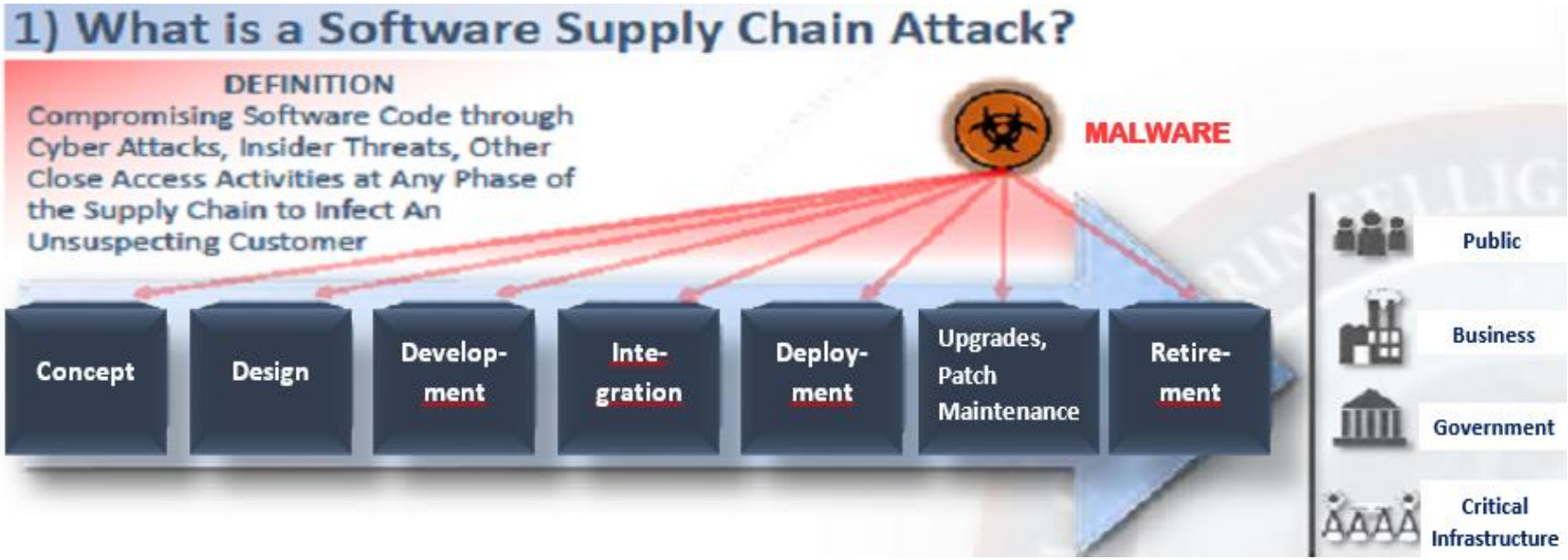
Background – Concepts (contd.)

- **<u>Complex Adaptive Systems (CAS)</u>**:
  - *Emergence:* all life forms feed off one another and make a system that is greater than the sum of its parts. (non-linear, i.e. "A+B+C ≠ D"; similar to complexity)
  - *Adaptability*: adaptive interaction where interacting agents modify their strategies in diverse ways as experience accumulates, i.e., they learn.
  - *Self-organization*: complex systems exhibit qualities of self-organization into patterns, e.g. flocks of birds or schools of fish
  - **Holism (Mixed-teams): Synthetic thinking - learn and apply new ideas to understand CAS**

Concepts – ICT as CAS

- **<u>ICT Supply Chains are similar to CAS:</u>**
  - Emergent: small changes can lead to drastic impacts
    - ➢ Non-linear: prime contractors face unannounced changes
  - Adaptable: especially unannounced or unanticipated changes
  - De-centralized: no central executive (or no enforcement)
  - ❖ **Holism (Mixed-teams): Synthetic thinking - to understand ecosystem**

Case One – Public/Private Survey



- Resource all IT functions
- Technology is good; a strategy for how to fit it in larger business concept is better.
- Comprehensive and adaptable response plans.
- Budgetary priorities and IT security priorities should be more compatible.

Case Two – DoD IG Report

- Criticality analysis, not complete
- Supplier threat assessment
- Non-accredited sources
- No parts test or validation and verification
- Take aways:
  - No adaptability (no learning)
  - No holism (no SMEs or mixed teams)
  - SCRM weak for high-value target

Case Three – 'The Big Hack'

- The case
- The skeptics
- Take aways:
  - Supply chain is fungible, living, self-organizing organism.
  - Small change could lead to wave of failure; emergent failure.
  - Make changes – harden defenses

Summary

	Case One Public/Private Survey	Case Two DoD IG Report	Case Three 'The Big Hack'
Emergence	Malware in trusted software may affect whole system/Streamline IT	No criticality analysis: whole system compromised	Microchip inserted in server can affect whole system
Adaptability	Adversaries adapted their attack vector/Orgs need plans	Not adaptable (no learning) - high risk	Chips adapted by locating required information
Self-organization	Malware makes system behave in unanticipated manner/small teams, new ideas for defense	Could change supply chain alter function, allow control/Self-organization - doubtful	Adversarial hardware makes system behave in unanticipated manner
Holism (Mixed Teams)	Make business and IT goals compatible & IT seamless	No holistic approach, though possible (SMEs)	Adversary (possibly)/Targets (damage control)

Conclusions

- Supply chain is “complex” and needs holistic thinking:
  - Every organization needs a holistic SCRM strategy that recognizes supply chains as complex adaptive systems.
  - 12/2018: Federal Acquisition Supply Chain Security Act
  - Section 909 of FY ‘18 NDAA – DoD CIO powers

Recommendations

- Empower managers at all levels (Adapt, self-organize)
- Engage mixed teams: Each member may propose risk management tools from different angles, that benefit the system as whole. (holism – people)
- Enforce continuous monitoring of all parts of the system to increase chance of identifying risk. (holism - technology)
- Vetting of all suppliers (“counter” – emergence)
- Question your readiness (self-organize)
- A framework to develop own tools


NATIONAL INTELLIGENCE UNIVERSITY
EDUCATION
RESEARCH
OUTREACH
NATIONAL INTELLIGENCE UNIVERSITY
SCIENTIA EST LUX LUCIS
1962

QUESTIONS?

Figures - Sources

- Slide 4: RSA Conference 2015, SF, USA, April 20-24, Session ID: STR-F03, Slide 9, “Supply Chain as an Attack Chain: Key Lessons to Secure Your Business,” https://www.rsaconference.com/writable/presentations/file_upload/str-f03_supply-chain-as-an-attack-chain.pdf, accessed 29 Oct 2018.

- Slide 9: Excerpt from Figure 6. Software Supply Chain Attacks, National Counterintelligence Security Center, 30 October 2017.

- Slide 11: Microchips found on altered motherboards in some cases looked like signal conditioning couplers. Source: Bloomberg Businessweek, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies, photographer, Victor Prado, accessed 7 Feb 2019