



Calhoun: The NPS Institutional Archive
DSpace Repository

Acquisition Research Program

Acquisition Research Symposium

2015-05-01

Acquiring Secure Systems Through Information Economics

Dacus, Chad

Monterey, California. Naval Postgraduate School

<http://hdl.handle.net/10945/53652>

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



Acquiring Secure Systems Through Information Economics

Chad Dacus
Research Professor of Defense Economics
Air Force Research Institute

Dr. Pano Yannakogeorgos
Research Professor & Deputy Director
Air University Cyber Research Task Force



Introduction



“For all future weapons systems that DoD will acquire or procure, DoD will mandate specific cybersecurity standards for weapons systems to meet. Acquisition and procurement policy and practice will be updated to promote effective cybersecurity throughout a system’s life cycle.”

- **DOD moving toward holding contractors liable**
- **Is now the best time to add contractor risk?**
- **Is this enough?**
 - **Minimum standard**
 - **Dynamic adversaries**





Dynamic Adversaries



Foreign
Intelligence

Traditional
Military



Criminal

Ad Hoc

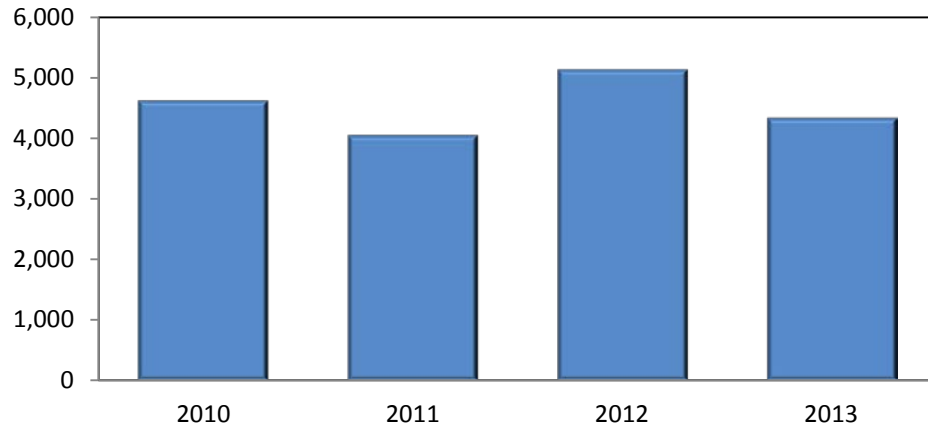




Cyber Risk to Military Missions



Known Software Vulnerabilities



- If adversary can hack into mission essential software/hardware, then mission is compromised
- Mission assurance requires materiel solutions, educated personnel (acquisition & operators), and TTPs



Duration of compromise may range from seconds to days, months, or years



Spectrum of Cyber Operations



Access Operations

- Digital intelligence (e.g., stealthy implant)

Disruption

- Interrupt the flow of information or function of information systems without physical damage or injury

Attack

- Use of force
- Physical damage or destruction
- Physical injury or death

Very stealthy

Less stealthy



Motivating Contractor Efforts



- Contractors have different priorities than the DOD when it comes to cybersecurity
 - Classic example
 - Manager's huge office
 - In another defense context
 - Cost-reimbursement contracts
- Why is this the case?
 - Contractor can satisfy client through other achievements
 - DOD has not clearly communicated importance



Motivating Contractor Efforts



- Government's problem: Outcomes to avoid?
 - Minimize:
 - Expected payments to contractors plus
 - Expected cost of hacking
 - Subject to:
 - Contractor participation constraint
 - Contractor chooses government's favored level of effort
- Results
 - Fee for successful protection
 - Penalty for breach





Motivating Contractor Efforts



- Implications
 - Incentives Depend on:
 - Probability of success
 - Marginal cost of effort
 - Marginal benefit of effort
 - How to administer incentives?
 - Incentive fees
 - Award fees
- Need a more functional way to set incentives





Choosing the Right Contractors



- Less expensive contractors likely to win contract over those with strong cybersecurity commitment and practices
 - Classic example:
 - “Market for Lemons”
 - In another defense context:
 - Sealed bids
- Why is this the case?
 - Cybersecurity is considered a constraint
 - Cybersecurity is costly to provide





Choosing the Right Contractors



- What to do about it?
 - Screening
 - Actively consider cybersecurity when awarding contract
 - Difficult when you have so many objectives
 - Encourage signaling
 - Foster metric development





Choosing the Right Contractors



- More specifically
 - Screen by system sensitivity
 - Boost incentives
 - Require higher quality scores
 - Quality scores
 - Historical system protection
 - Vulnerability Assessment/Penetration Testing
 - Weakness and Vulnerability scores
 - How to aggregate?



Effectiveness of Incentives?



- Long history of incentives in DOD
- Empirical results
 - GAO (1999-2003)
 - Incentives not particularly helpful
 - Recommendations
 - 2014 Performance of DOD Acquisition System
 - Incentive contracts performed at least as well



Concerns



- Detection Lag and Uncertainty
 - Alternate signals
- Adversarial behavior
- Setting appropriate fee
 - Budget buster
 - Tradeoffs





Conclusions



- Move beyond a compliance mindset
- Economic theory calls for cybersecurity incentives
 - Truly makes cybersecurity a priority
 - Size based on system sensitivity
 - Monitor profit margins/perverse behavior
- Lack of metrics is an obstacle
 - Encourage creativity through rewards
 - Information sharing important



Questions?

Dr. Chad Dacus
Research Professor & Chief Economist
Air Force Research Institute
Chad.Dacus@us.af.mil

Dr. Pano Yannakogeorgos
Research Professor & Deputy Director
Air University Cyber Research Task Force
Panayotis.Yannakogeorgos@us.af.mil