
COLLEGE OF
INFORMATION
STUDIES

# Incentives

## Sociotechnical Cybersecurity Workshop 2
## August 8 – 9, 2017 San Diego
## Scripps Seaside Forum

Timothy Summers, Ph.D.

Cybercriminals compete - for **money and fame** – and this makes them **fast to adapt** and **innovate faster than defenders**.

Center for Strategic & International Studies, 2017

CSIS

CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

**Incentives are misaligned** – both within organizations and between attackers and defenders.

A recent study of 800 companies across five major sectors revealed **three key misalignments**:

| | |
|---|---|
| Attackers versus defenders | Attackers' incentives are shaped by a fluid, decentralized market, making them agile and quick to adapt, while defenders are constrained by bureaucracy and top-down decision making. |
| Strategy versus implementation | While more than 90% of organizations have a cybersecurity strategy, less than half have fully implemented their strategies. |
| Executives versus implementers | Senior executives designing cyber strategies measure success differently to those who put strategies into practice, limiting their effectiveness. |

**54% of executives** say that their organizations **are most concerned about reputational effect** rather than actual breaches.

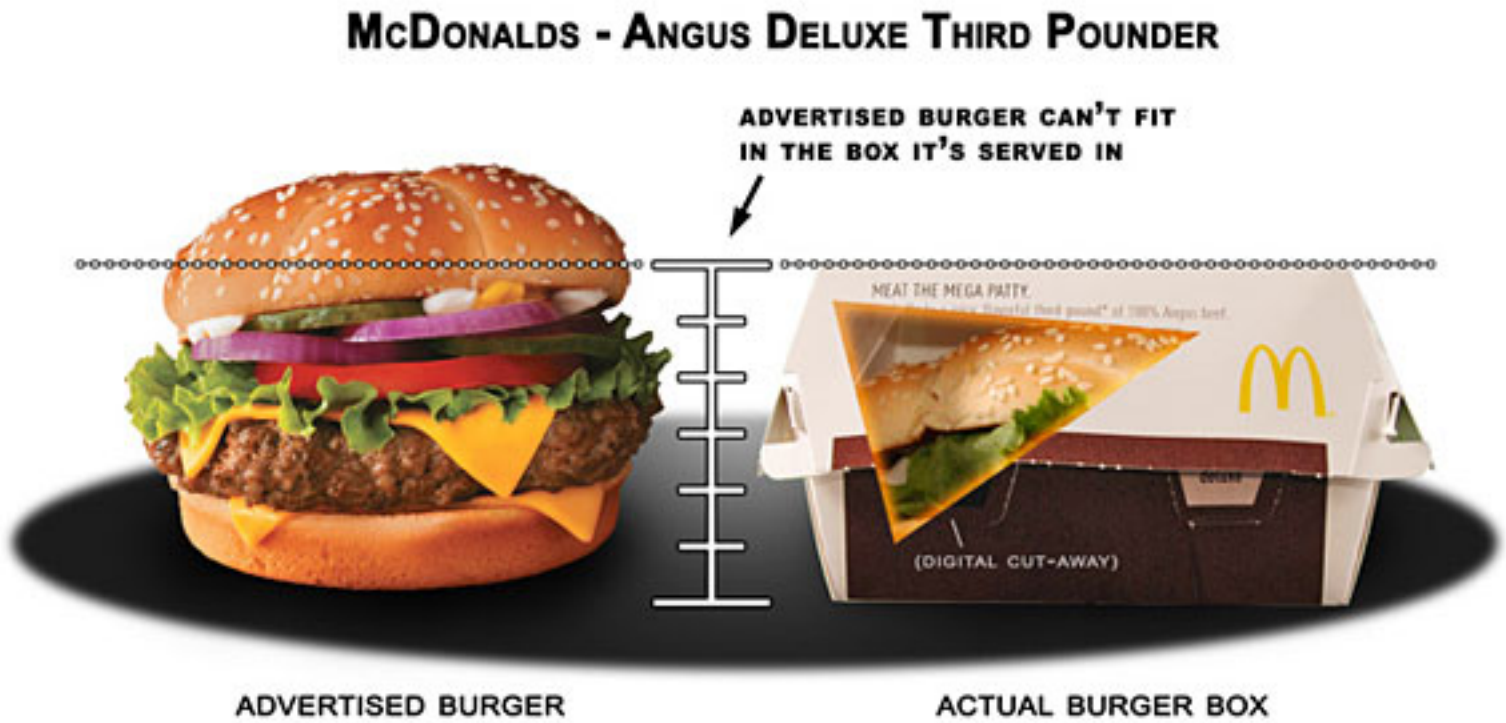
What does it mean for an organization to have an **adequate** level of cybersecurity?

# Issues to be Considered

- **Overcoming barriers of information failures**: The nature of cyber threats means that there is hidden information such that organizations do not know enough about the threat and which measures will offer the most effective protections.
- **Overcoming barriers of external costs**: Cybersecurity can protect three key areas of organizational interest from attack: personal information, other sensitive data (e.g. intellectual property, financial and commercial information), and an organization's reputation.
- **Identifying mechanisms of government, FFRDCs, and consumer protection intervention**: The combination of lack of information and external costs is likely to lead to organizations investing in asymmetric levels of cybersecurity which can have consequences to the economy as consumers and other organizations are harmed via breach.
- **Overcoming the misalignment of incentives**: There are three levels of misaligned incentives that put organizations and their cyber defenders at a disadvantage.

**Perfect World**
What we're proposing

**Normal Chaos**
How it'll actually look


McDONALDS - ANGUS DELUXE THIRD POUNDER
ADVERTISED BURGER CAN'T FIT
IN THE BOX IT'S SERVED IN
MEAT THE MEGA PATTY.
(DIGITAL CUT-AWAY)
ADVERTISED BURGER
ACTUAL BURGER BOX

# Additional Topics to be Considered

- **Environmental instability**: How can incentives appropriately reflect the normal chaos that occurs in cybersecurity?
- **Operational instability**: How can incentives be organizationally agnostic? Should they be?
- **Types of Incentivization**: How can incentivization be reflective of the practices of sociotechnical cybersecurity?
- **Entity Interdependencies**: What are interdependencies that must be understood in order to create effective incentives?
- **Incentivization Flexibility**: What kind of flexibility must exist in the incentivization structures?
- **Autonomous operation**: Are some tasks not within the view of incentivization structures?
- **Alignment rules**: What are the alignment rules necessary to create effective incentives in sociotechnical cybersecurity?