Deterrence

Is it effective and how to make it better

Matthew Merzbacher

/ November 15, 2016 /

WHY ME?

- **Does Security Work?**
  - Initial Conclusion: Of course it works!
- **Why does Security work? Is this Detection or Deterrence (or both)?**
  - Is Deterrence effective?
  - Ask a Social Scientist… So I did!
- **Outline:**
  - Understand Deterrence
  - Learn from it
  - Improve it
- **Deterrence**
  - Structured openness needed in processes
  - Continuous forward-looking Gap Analysis
  - Improve top-down information flow and bottom-up performance flow
  - Audit

WEIGHT GAIN ANALOGY

➔Remediation – response to gained weight

- The longer gain goes unnoticed, the worse it gets

➢Detection

- Scale (to measure performance)
- Detects nothing if no gain
- Only detects after the fact

➢Deterrence

- Reduce unhealthy food & habits
- Increase awareness

➔We need all three

➔Let's talk about Deterrence

CRIMINAL DETERRENCE

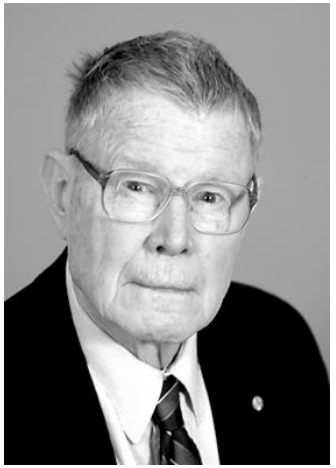
- **Specific Deterrence and General/Indirect Deterrence**
- **Extensive reviews … with conflicting assessments**

- Despite numerous studies using a variety of data sources, sanctions, crime types, statistical methods and theoretical approaches, **there remains little agreement** in the scientific literature **about whether**, how, under what circumstances, to what extent, for which crimes, at what cost, for which individuals, and perhaps most importantly, in which direction do various aspects of contemporary **criminal sanctions affect subsequent criminal behavior**.

- **Interesting, but not really what Security is about**
  - Preventative, not punitive

NUCLEAR DETERRENCE

- **Game Theory (Schelling)**
- **Strategy intended to dissuade an adversary from taking an action not yet started**
  - An inferior nuclear force, by virtue of its extreme destructive power, could deter a more powerful adversary



- **Kissinger, Perry, Shultz, Nunn (WSJ '07)**
  - **Reversed** their previous position and asserted that far from making the world safer, nuclear weapons had become a source of extreme risk.
    - Nuclear deterrence is a **far less persuasive strategic response to a world** of potential regional nuclear arms races and nuclear **terrorism** than it was to the cold war.

- **Closer, but…**

FRAUD DETERRENCE

- **Sarbanes Oxley**
  - The intent of the U.S. Congress… was attempting to proactively **deter** financial misrepresentation (Fraud) **in order to** ensure more accurate financial reporting to **increase** investor **confidence**.
- **Premise: Fraud is not random – conditions must be right**
- **Proactive identification and removal of causal & enabling factors**
  - Remove root causes and enablers, possibly revealing other opportunities
  - Improved procedures are the best defense
- **Deterrence != Detection**
  - Detection: identify non-conforming transaction
  - Deterrence: analyze conditions and procedures
- **Short term (procedural) and Long term (cultural) initiatives**

HOW DOES IT WORK? COSO MODEL

- **Control Environment**
  - Top-Down culture of ethics in Management
- **Risk Assessment**
  - Look forward to identify gaps
- **Control Activities**
  - Do (only) what you intend – no more, no less
- **Information & Communication**
  - Information flows Down to line
  - Performance flows Up (informally & formally) – Objective Feedback
- **Monitoring**
  - Audit

WILL/DOES COSO WORK FOR SECURITY?

➔ Control Environment

- How do we control society from top-down?

➔ Risk Assessment

- Opportunity for improvement: Gap analysis

➔ Control Activities

- Strict ConOps in place
- Danger: Impediment to innovation

➔ Information & Communication

- Information flows Down, Performance flows Up

➔ Monitoring

- Audit, Audit, Audit!

OTHER KINDS OF FRAUD

Laboratory

- Environmental / Laboratory
  - Deliberate falsification of analytical and quality assurance results... historically been detected either by reports from disgruntled employees or electronic data audits. In both of these circumstances the laboratory is **already performing fraudulent work and the damage is done**.
    - *Best Practices for the Detection and Deterrence of Laboratory Fraud*, California Military Environmental Coordination Committee [1997]

Academic

- Replication study – 36%
- Do terrorists need to replicate? Can we use this? (perhaps not for deterrence)

HOW CAN WE USE THIS IN SECURITY?

➔ Detection

- Keep improving scales
- Invent new scales
- By the time we detect, the damage may be done

➔ Deterrence

- Structured openness needed in processes
- Must have **continuous** forward-looking Gap Analysis
- Improve top-down information flow and bottom-up performance flow
- Audit

➔ Ultimate Deterrence – ban travel!

- Balance controls against Freedom

QUESTIONS?

- **Thank You**