SAND2011-6020C

Cybersecurity Challenges and Opportunities

Edward B. Talbot

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.
SAND Number : XXX-XXXX X

Outline

- A Thought Experiment
  - Evidence
- The Exemplar Threat: The Insider
- Full-scope Cybersecurity
- Effective Cybersecurity

Analyst, Administrator or Adversary?

- "To do my job, I need the following for all web traffic entering or leaving your site:
  - I need ***access*** to every packet.
  - I need the ***time-history*** of the traffic.
  - I need ***tools*** so I can analyze the data."

- Analysts, administrators, and adversaries require the ***same*** resources.

- Analysts, administrators, and adversaries pose ***similar*** threats to cybersecurity.

Are we doing cybersecurity wrong?

Probability of compromise increases with each "monitor" (program, administrator, analyst,…) that is added to the communication path.

Detection and protection are mutually exclusive.

- Increased **detection**:
  - ***may*** increase the probability that a bad guy will be discovered and caught.
  - ***will*** increase the probability that data will be compromised.

- Improved user **protection**:
  - ***will*** decrease the probability that data will be compromised.
  - ***may*** enable compromise without detection.

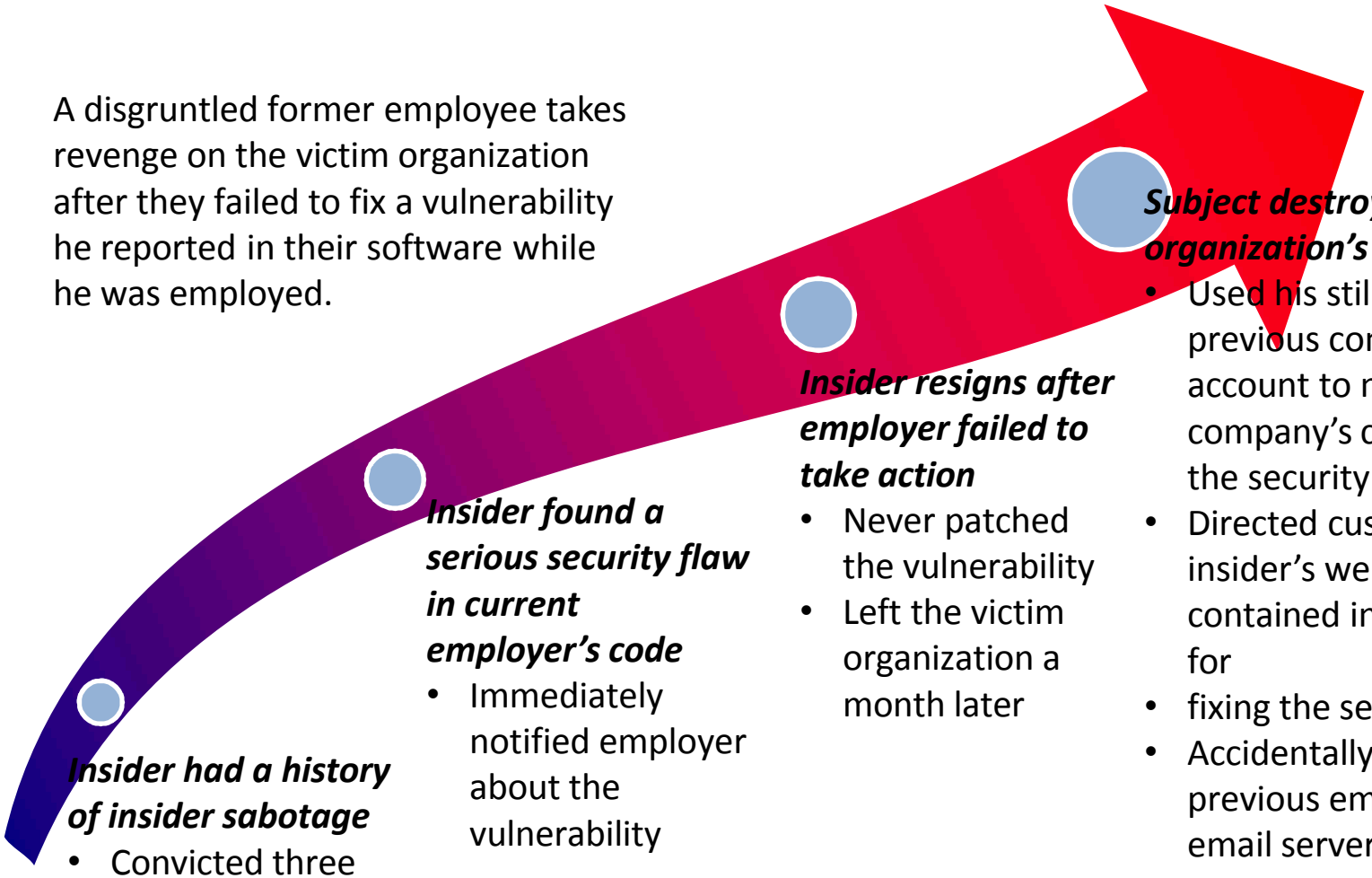
Any system that is capable of ***detecting*** all that is going on inside of it is capable of ***revealing*** all that is going on inside of it.

Outline

- A Thought Experiment
  - Evidence
- The Exemplar Threat: The Insider
- Full-scope Cybersecurity
- Effective Cybersecurity

"Generic" Insider Threat Model

A disgruntled former employee takes revenge on the victim organization after they failed to fix a vulnerability he reported in their software while he was employed.



Insider had a history of insider sabotage

- Convicted three years earlier at a previous employer

Insider found a serious security flaw in current employer's code

- Immediately notified employer about the vulnerability

Insider resigns after employer failed to take action

- Never patched the vulnerability
- Left the victim organization a month later

Subject destroyed organization's reputation

- Used his still-active previous company email account to notify the company's customers of the security flaw
- Directed customers to insider's website, which contained instructions for
- fixing the security hole
- Accidentally crashed previous employer's email servers
- Victim organization went out of business

The content of this slide was collected strictly from publicly available information

Insider Threat Observations

- Intent is the only certain way to distinguish between benign and malicious insiders.
  - Intent is devilishly hard to determine.
  - A manipulated insider is equivalent to a malicious insider.
- In cyberspace, smart and/or well-resourced people will always be able to redirect attribution to the not-so-smart or well-resourced.
  - Any conclusion reached based solely on cyber data is subject to deception.

"Beyond a Reasonable Doubt:

The standard that must be met by the prosecution's evidence in a criminal prosecution: that no other logical explanation can be derived from the facts except that the defendant committed the crime, thereby overcoming the presumption that a person is innocent until proven guilty."

Source: http://legal-dictionary.thefreedictionary.com/Beyond+a+Reasonable+Doubt

The insider threat is out-of-scope for current cybersecurity thinking.

7.) Application
6.) Presentation
5.) Session
4.) Transport
3.) Network
2.) Data Link
1.) Physical

- Example: Mao (card game)
  - The game forbids its players from explaining the rules, and new players are often told only "the only rule you may be told is this one."
  - The ultimate goal of the game is to be the first player to get rid of all the cards in their hand.
  - Specifics are discovered through trial and error.
  - A player who breaks a rule is penalized by being given an additional card from the deck.
  - The person giving the penalty must state what the incorrect action was, without explaining the rule that was broken.
- User frustration and confusion are unintended consequences of using limited scope rules to address an out-of-scope problem.

"…unintended consequences are outcomes that are not the outcomes intended by a particular action. The unintended outcomes may be positive or negative."

Source: http://en.wikipedia.org/wiki/Unintended_consequences

Outline

- A Thought Experiment
  - Evidence
- The Exemplar Threat: The Insider
- Full-scope Cybersecurity
- Effective Cybersecurity

Full-scope cybersecurity addresses all systemic vulnerabilities *and* the insider threat.

HMI
Perception
Cognition
Experience

Authorities
Expectations
Incentives

15	Human
14	Cultural Norms
13	Social Norms
12	Organizational Roles
11	7.) Application
10	6.) Presentation
9	5.) Session
8	4.) Transport
7	3.) Network
6	2.) Data Link
5	1.) Physical
4	System Hardware (Motherboard, etc.)
3	Component (ICs…)
2	Semiconductor Physics
1	Atomic

Less predictable
Larger Error Bars
Less Deterministic

Example Layer 12-15 Vulnerabilities:
- Spear-phishing
- Social engineering

Traditional, *limited-scope* cybersecurity

More Certain
Smaller Error Bars
More Deterministic

Example Layer 1-4 Vulnerabilities:
- Supply Chain

Full-scope cybersecurity acknowledges that insiders can be *hired*, *ordered* or *created*.

Hired

Paycheck

Hiring and Recruiting

Benign

Poor Treatment and Incentives

Created

Poor Business Processes, Support, and Training

Deliberate Malicious Insider (Intentional)

Manipulated Malicious Insider (Unknowing)

Ordered

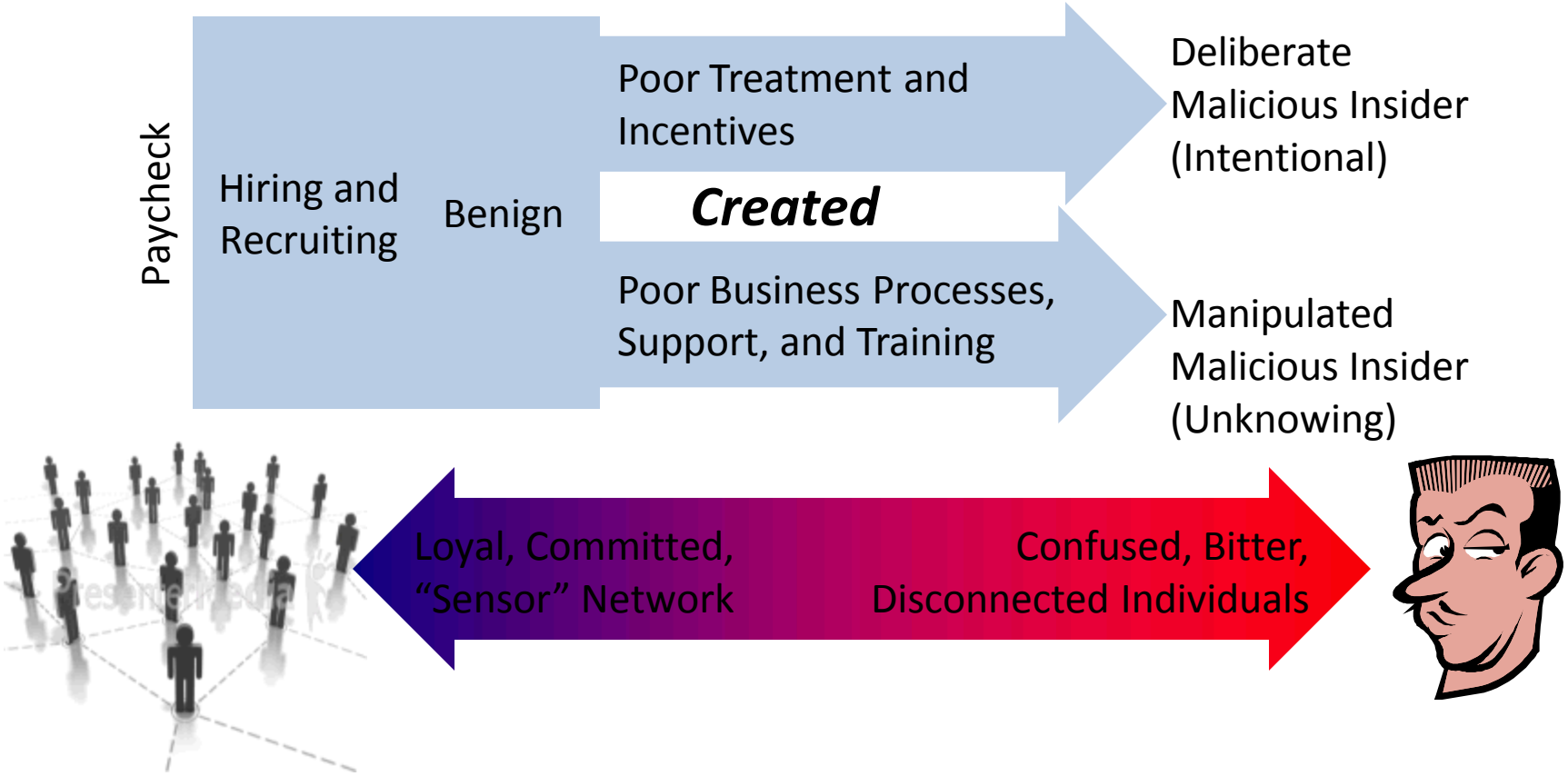
Purchase Order

Requisitions and Contracts

Service, Supplies, and Equipment

Solutions to the insider threat problem may lie predominantly OUTSIDE the purview of traditional cybersecurity practice.

Limited scope strategies transform a loyal and committed workforce to a confused and/or bitter set of vulnerabilities.



"The *self-fulfilling prophecy* is, in the beginning, a *false* definition of the situation evoking a new behavior which makes the original false conception come 'true'."

- *Social Theory and Social Structure*, Robert K. Merton

Outline

- A Thought Experiment
  - Evidence
- The Exemplar Threat: The Insider
- Full-scope Cybersecurity
- Effective Cybersecurity

Absolute Certainty is Unobtainable

Loyal, Committed, "Sensor" Network

Confused, Bitter, Disconnected Individuals

No Certainty

Know Little

Know "Everything"

Know Trust

No Trust

"We can have all the records in the world and if somebody wants to trade outside them or something, you know, they're not going to tell us they're trading in their cousin's name," [Warren Buffett's partner Charlie] Munger said. "I think your best compliance cultures are the ones which have this attitude of trust and some of the ones with the biggest compliance departments, like Wall Street, have the most scandals."

- http://articles.economictimes.indiatimes.com/2011-05-03/news/29499643_1_charlie-munger-warren-buffett-berkshire-hathaway

Effective Cybersecurity

Are the processes we are putting in place to *detect* this…

…inadvertently resulting in the *creation* of this?

- What doesn't work (by itself):
  - Enforcement/compliance/oversight/governance…
  - Physical controls (guards, gates, guns,…)
  - Cyber controls (access controls, IDS,…)
- What works – every employee is a sensor:
  - Develop and cultivate trust, loyalty and accountability.

What if we are doing cybersecurity wrong?

Opportunity: Refocus cybersecurity on user ***protection.***

A Notional User Protection System

- Anonymous – predictably unlikely to extract useful data.
- Non-attribution – forensics pushed to the endpoints.
- Non-persistence – no trace remains of data transferred.
- Strong authentication – at all endpoints, as certain as the real world (endpoint and real world equivalence).

Summary: Cybersecurity Challenges and Opportunities

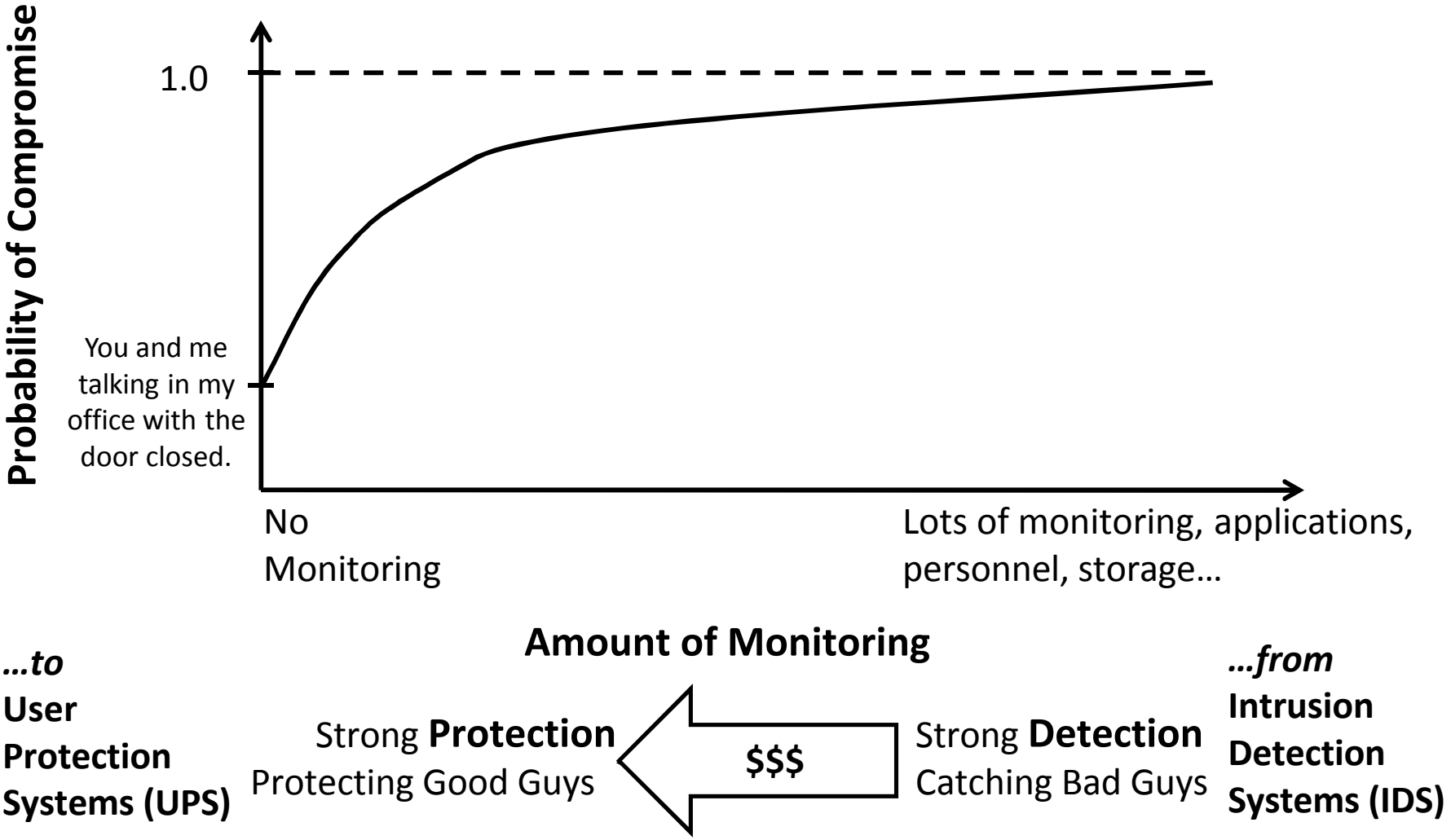
- The assumptions underlying cybersecurity as it is practiced today are delusions.
  - Evidenced by experience with incidents.
- We need cybersecurity approaches architectures based on what people (and systems) actually do.
  - Not what we wish they did.
  - A focus on cybersecurity protection supports users.
- People respond favorably to positive incentives and being treated well.
  - **Effective** cybersecurity develops a culture of trust, loyalty and accountability through positive incentives and fairness.

"We cannot solve our problems with the same thinking we used when we created them."

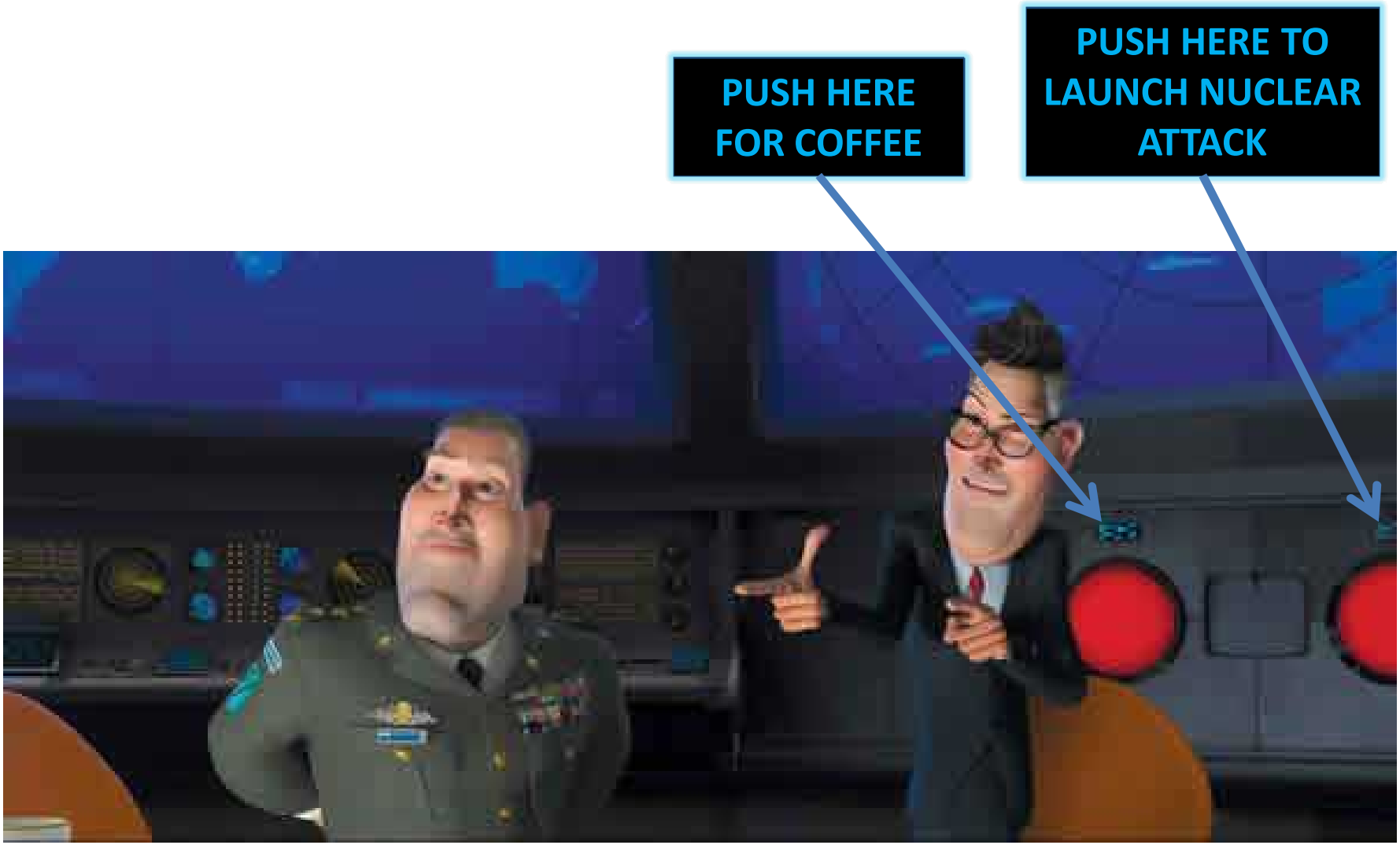
- Albert Einstein

Back-ups

A Thought Experiment: What if we're doing cybersecurity wrong?



Limited-scope solutions confuse users.



Assumptions

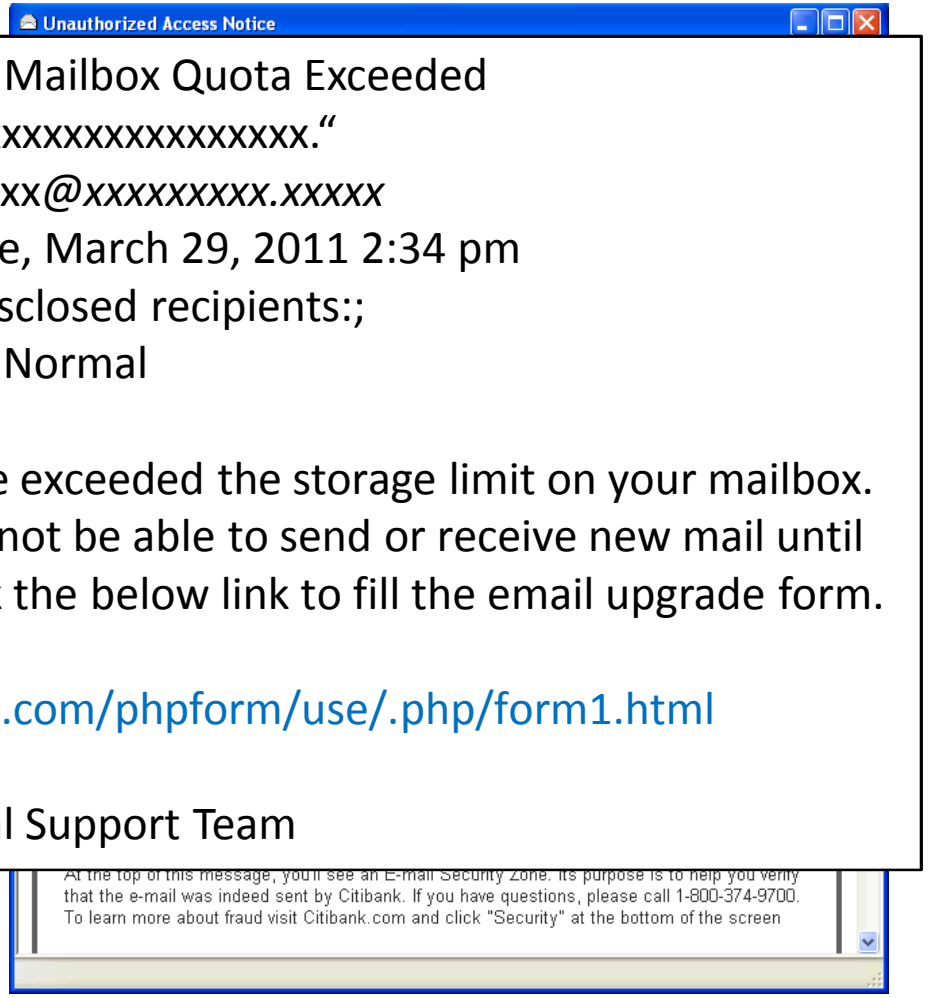
- Correctness
  - Components reasonably work as designed
- Policy
  - Effective operating policies are practiced
- Monitoring
  - Timely situational awareness of reasonable fidelity available
- Response
  - Effective coordinated mitigation of breaches

A Thought Experiment

"Basic cybersecurity practices" are increasingly inadequate.

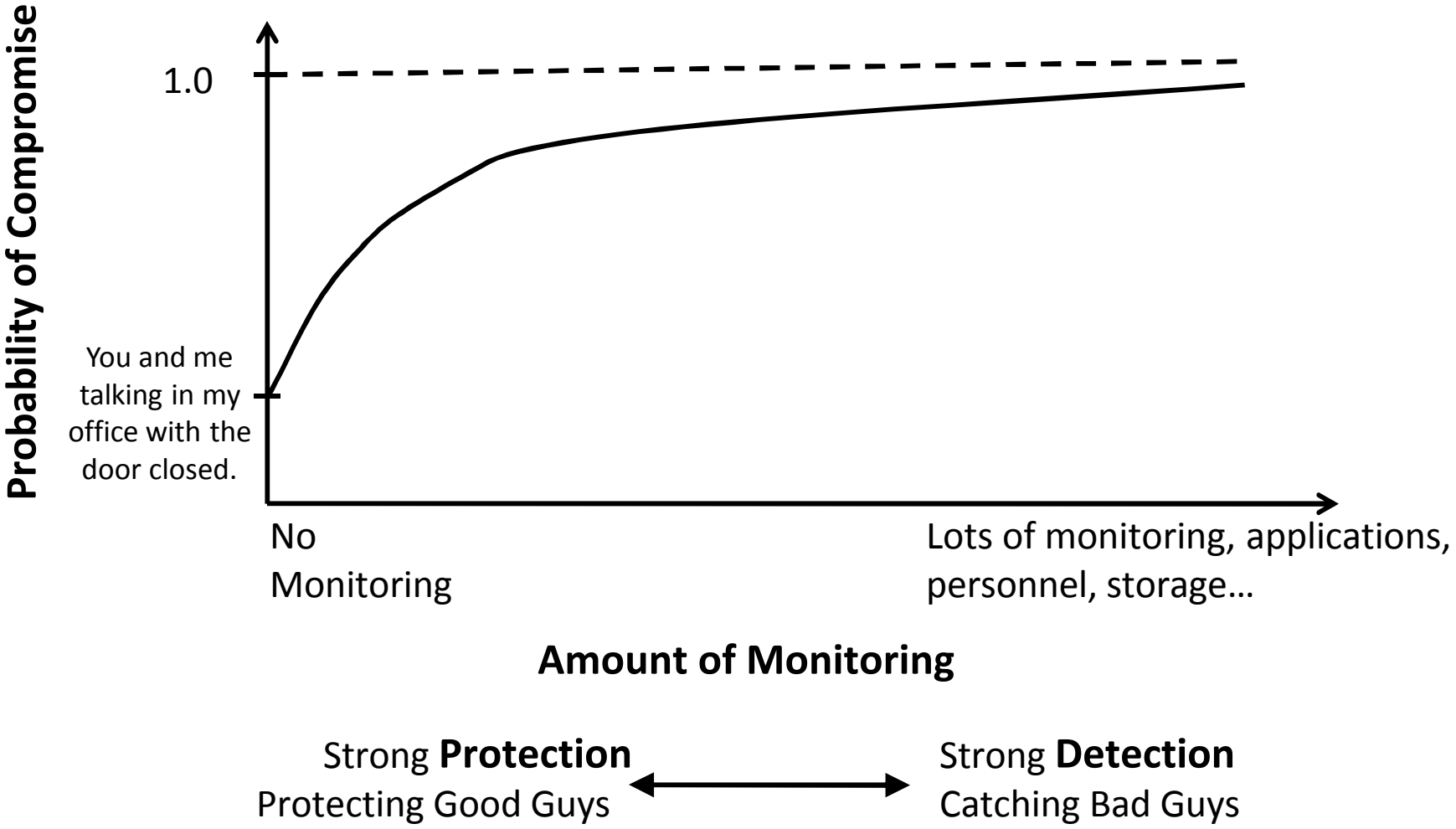
"Everyone should make basic cybersecurity practices as reflexive as putting on a seatbelt – using antivirus software, being careful which websites you visit, not opening emails or attachments that look suspicious."

- Janet Napolitano, UC Berkeley, April 2011



A Thought Experiment

What if we're doing cybersecurity wrong?



(CNN) -- A few years ago a disgruntled employee for a large multinational automotive firm left the company -- but when he walked out the door, he also walked out with plans for a new car model under development on a cheap USB drive.

When the plans were leaked, the cost to the company was an estimated $1 billion in lost sales and increased research and development costs, according to a security expert who worked on the case.

http://edition.cnn.com/2011/BUSINESS/06/06/cybercrime.cost/index.html?hpt=hp