The Risk of Risk Analysis

And Its Relation to the Economics of Insider Threats

Christian W Probst
Technical University of Denmark

Jeffrey Hunker
Carnegie Mellon University

The 8th Workshop on the Economics of Information Security
June 25, 2009 London

Insider Threats

- Considered the most serious security problem by many
  - Also most difficult problem to deal with
- High-level cases are well publicised (eventually)
  - Jerome Kerviel, Societe Generale
  - US District of Columbia tax fraud
- Minor cases and lesser damages are covered up
  - if discovered at all

Insider Threats

- Organisations are aware of insider threats
- But take only limited steps to prevent them
  - Even though the consequences can be severe
- **Shouldn't it be topmost priority to prevent these threats in the first place?**
  - Ignoring these severe threats is often described as distinct choice

Why do organisations choose to be so vulnerable?

Outsider Threats

- Organisations rarely choose to leave open vulnerabilities that might be exploited by outsiders
  - As these attacks might severely damage the organisation
- Only “excuses”
  - limited resources
  - sloppiness

This Work

- Insiders and Outsiders
- Investigate
  - The organisation's risk analysis
  - Assessment of trust in insiders
    - Their development over time
- Combined view of the economics of
  - The organisation, insiders, and elements of mitigation

Who is an Insider?

An insider is a person that has been legitimately empowered with the right to access, represent or decide about one or more assets of the organisation's structure. (Dagstuhl, 2008)

- Factors of a "good" insider
  - Knowledge, intent, motivation
  - Power to act as agent for the organisation
  - Knowledge of IT platforms and security controls
  - Ability to incur liability

Outsiders vs. Insiders

- Organisations usually does whatever possible to prevent threats from the outside
  - Easily identify outsiders and the necessary access to an organisation's assets
  - Control interactions (access control, policies, ...)
- Insiders have a special role
  - Malicious/disallowed actions hard to separate from useful actions

Insider Threats

- Emanate from insiders whose actions place the organisation at risk
  - Motivation
    - Maliciously motivated, result of accident or error, caused by deception
  - Actors
    - Single insider or combination of insiders, outsiders, etc.

Kinds of Insider Threats

- No violation of trust
  - Accidents or stupidity, Fulfilment of duty
- Violation of trust
  - "Simple"
    - System facilitates the damage
    - Losses caused are not too high (can be ignored) or potential harm is considerable but the threat could have been prevented easily

High Profile Insider Threats

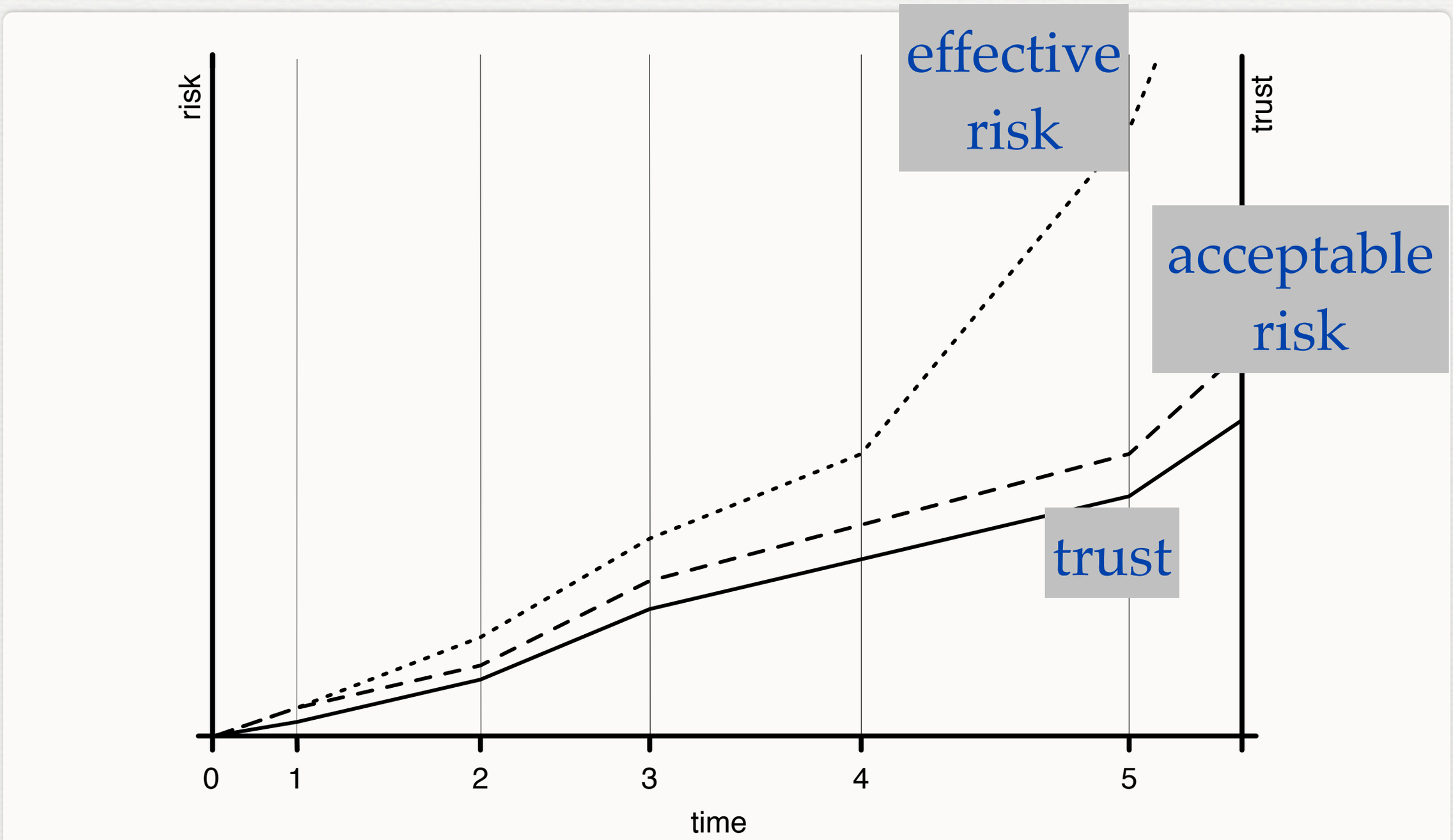
- The type of threat that is (eventually) reported in press
- Devastating consequences
- The actor causing them often has even better information than the “regular” insider
- Challenge risk analysis, which is based on
  - Policies directed towards a risk
  - Losses due to risks, and
  - Probabilities of risks taking place.

Christian W Probst & Jeffrey Hunker * The Risk of Risk Analysis * WEIS 2009 * June 25, 2009

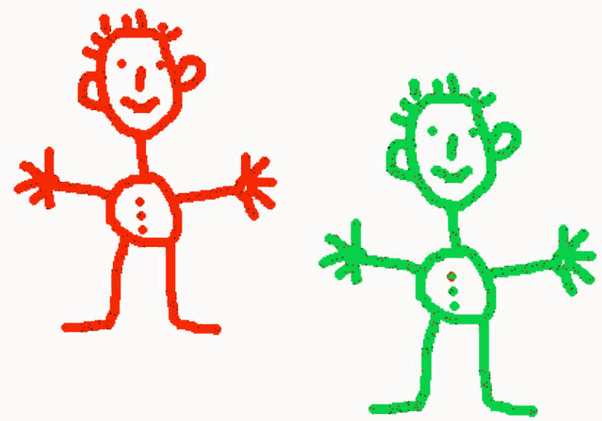
Trust and Risk

- Trust is essential whenever we have to take a risk
  - Be it a marriage, an organisation, or a nation.
- As time goes by, trust into actors and the likelihood to accept risks increases (usually)
- Two aspects
  - How do trust and risk evolve over time?
  - How effective are mitigating factors?

Trust and Risk



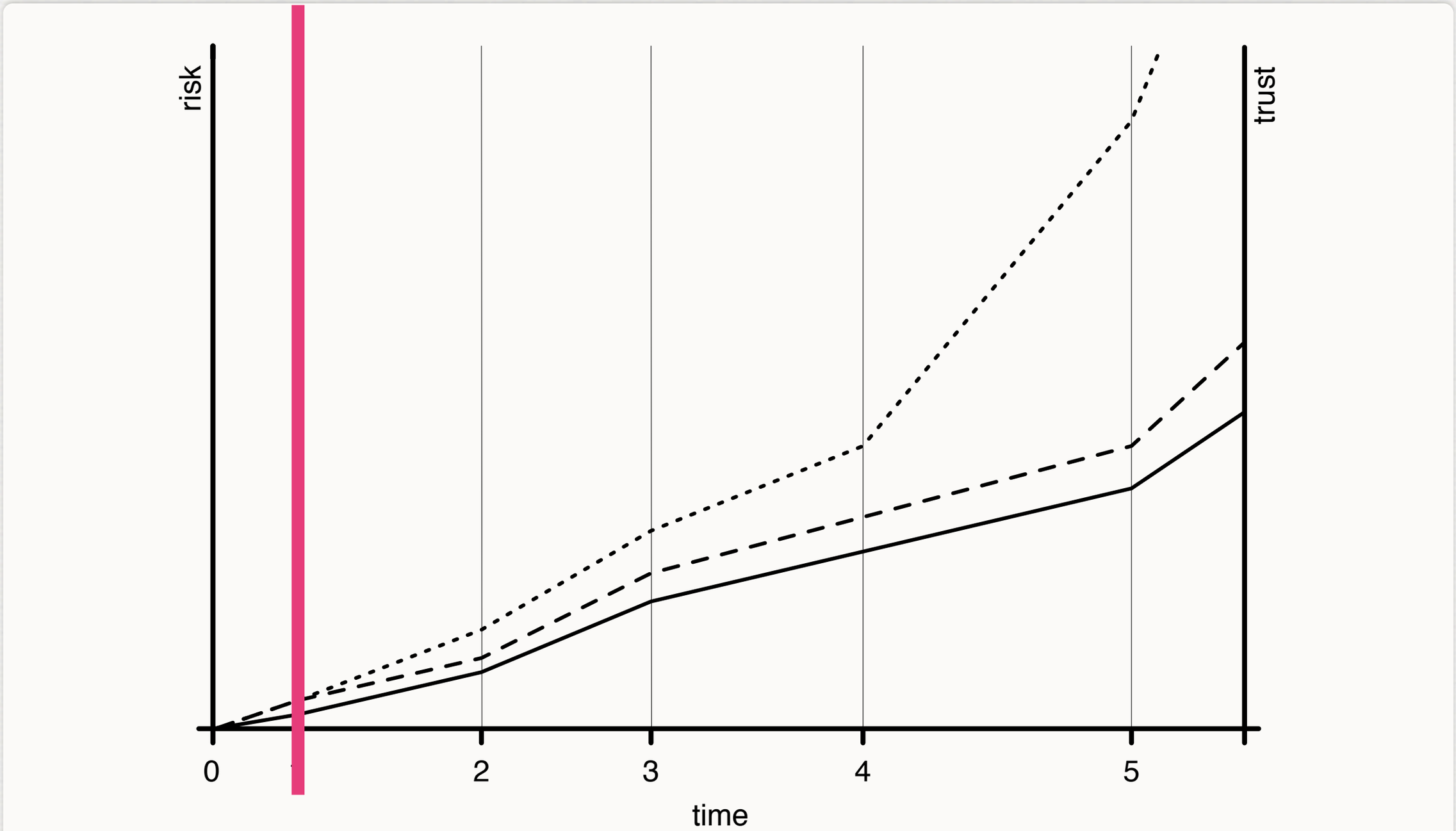
- Actors
  - Bob, a young boy, and
  - His mother Alice



- His mother opens a bakery, and hires Bob to help

- Simple Trust, Low Risk
  - Newly hired employees should be background-checked
  - Control to assets easy to establish

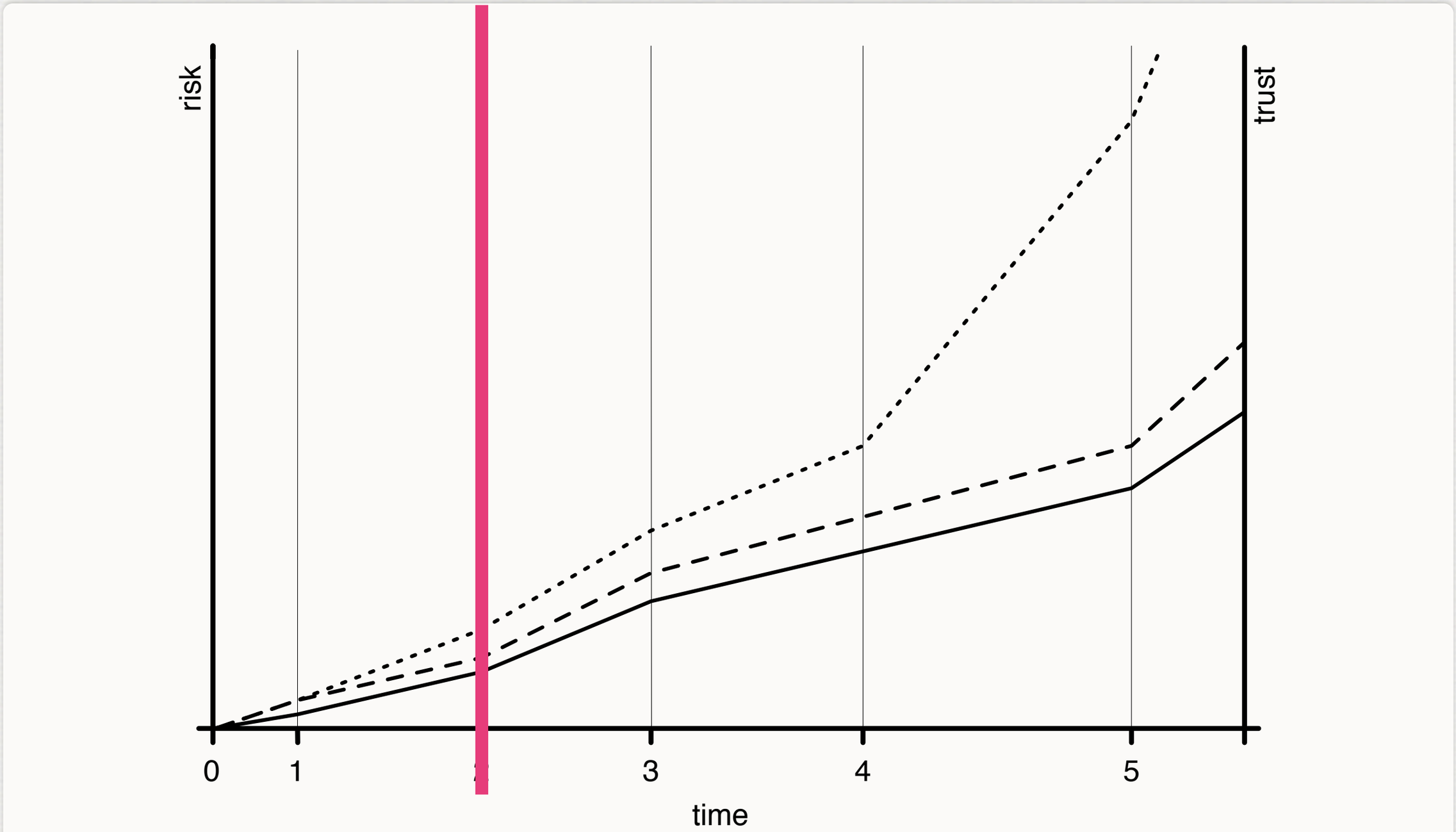
Trust and Risk



- After some time, Bob is entrusted to program a web interface and since he trains for a marathon, he is no risk to the precious cookie dough

- Medium Trust, Elevated Risk
  - Promotion, otherwise increased trust
  - In lockstep risk increases due to more detailed knowledge

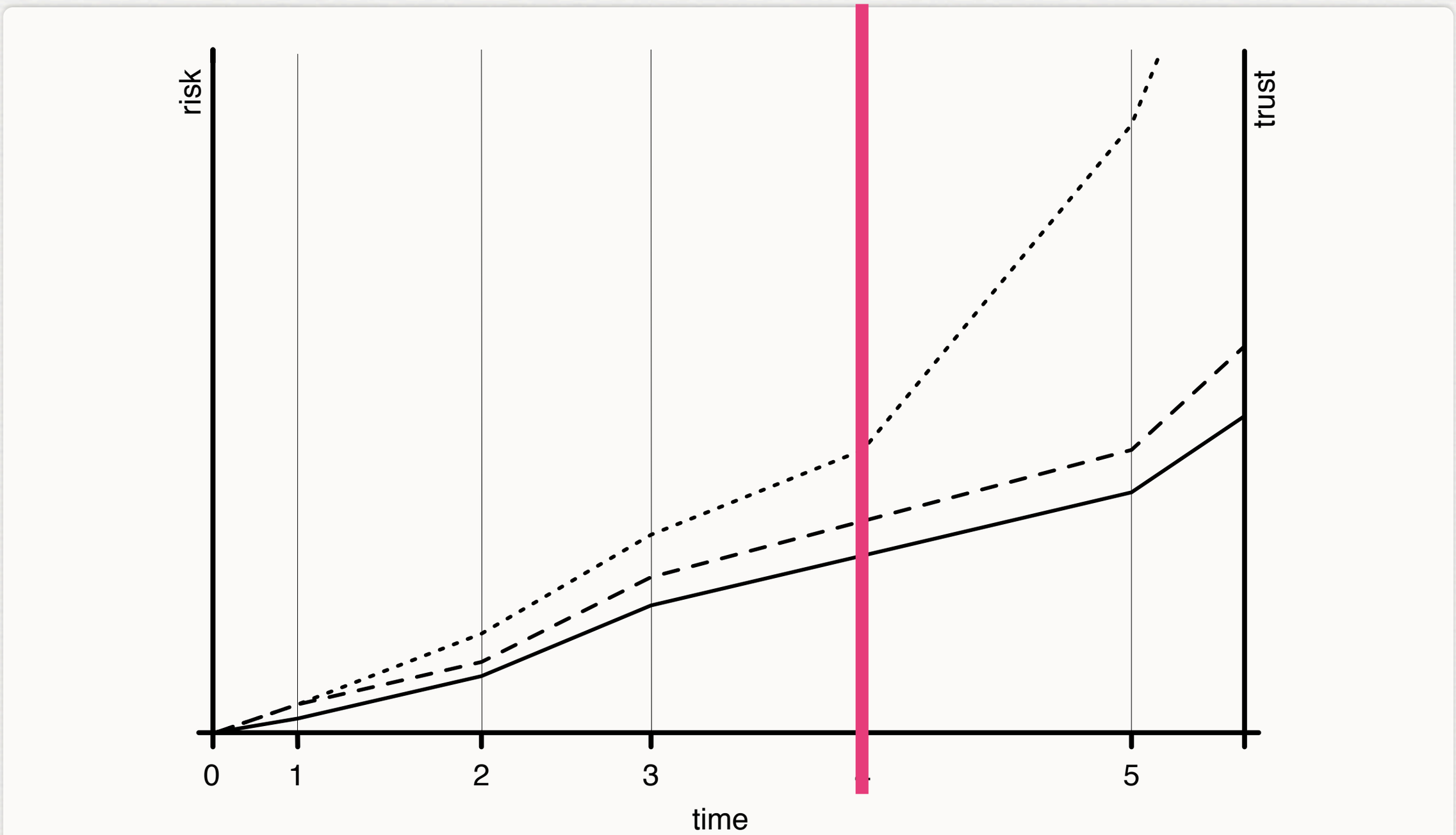
Trust and Risk



- Again some time goes by, with Bob spending time in the bakery, and eventually he stops running
  - Suddenly, he has quite some interest in cookies...
- Andnd he still knows how to access the web interface, so he can ensure his orders are free and can not be traced

- Complex Trust and Risk
  - Dangerous combination of knowledge and access rights

Trust and Risk



Phases

- Simple Trust, Low Risk
  - New employees should be background-checked
  - Fine-grained control over which assets the actor may access
- Medium Trust, Elevated Risk
  - Promotion, otherwise increased trust
  - Risk increases due to more detailed knowledge
- Complex Trust and Risk
  - Dangerous combination of knowledge & access rights

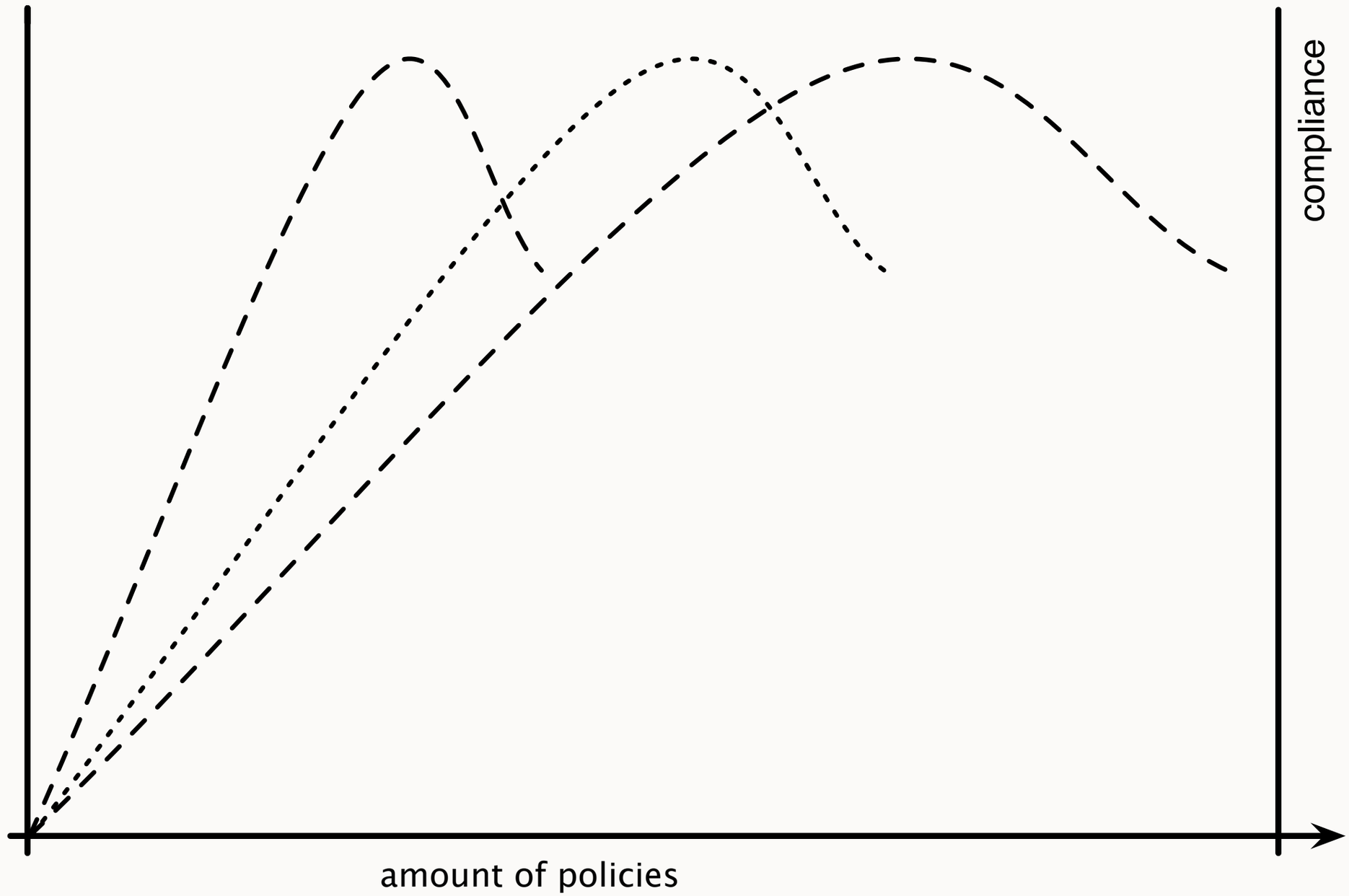
Problems

- Gap between effective risk and acceptable risk is often not measurable
  - Needed to judge how effective mitigation is
  - Gap must be bridged by willingness to trust, or by policies
- Hard to maintain a “global” vs “local” viewpoint
  - “Previous” knowledge of an insider?
  - External events that influence the whole system?

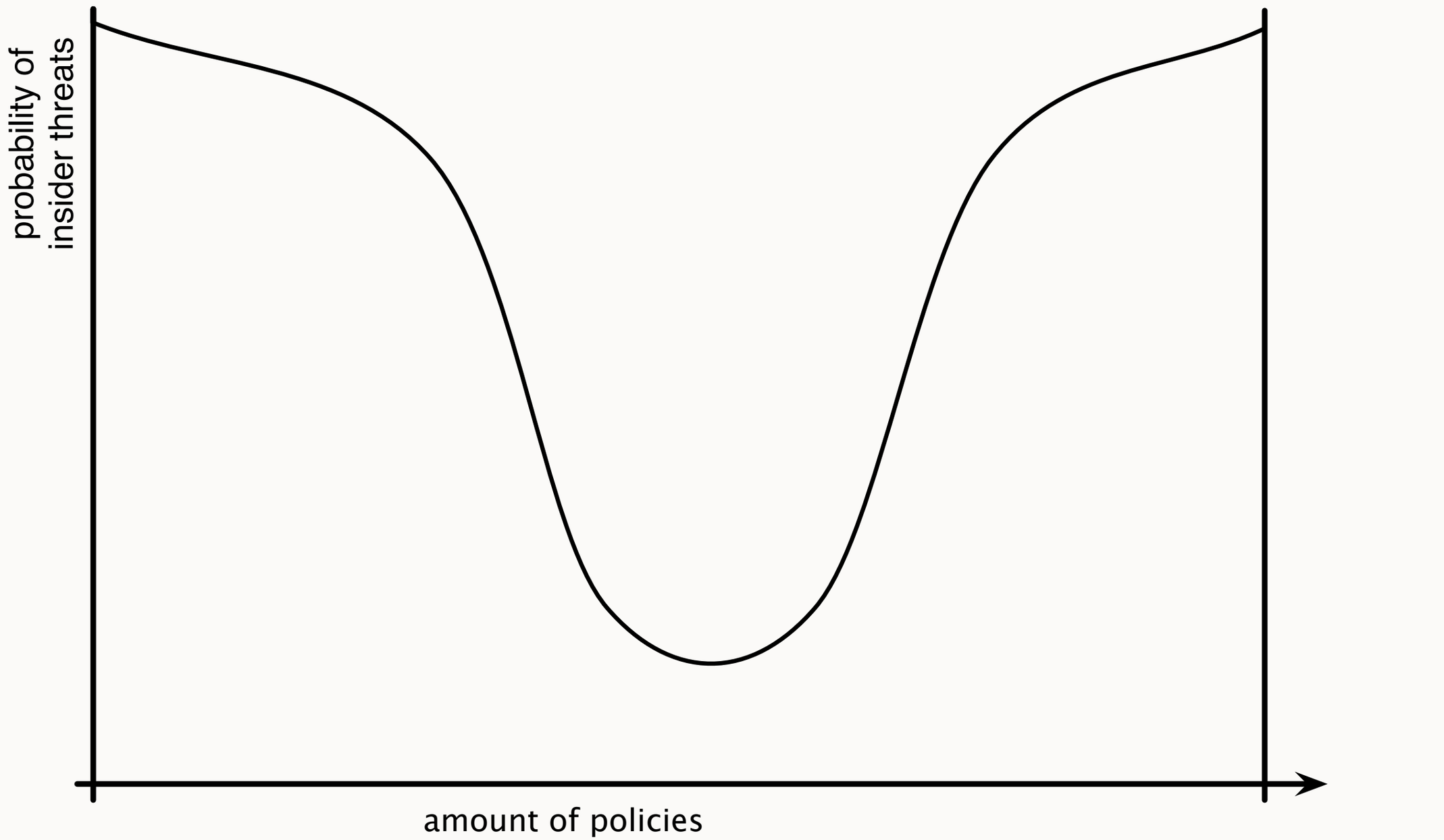
Policies

- The "natural" reaction to gap between acceptable and effective risk
  - Add more policies
- More policies might no do more good
  - Compliance with policies will peak, then decline
  - Point where policies more often than not prohibit useful work, or employees feel too controlled

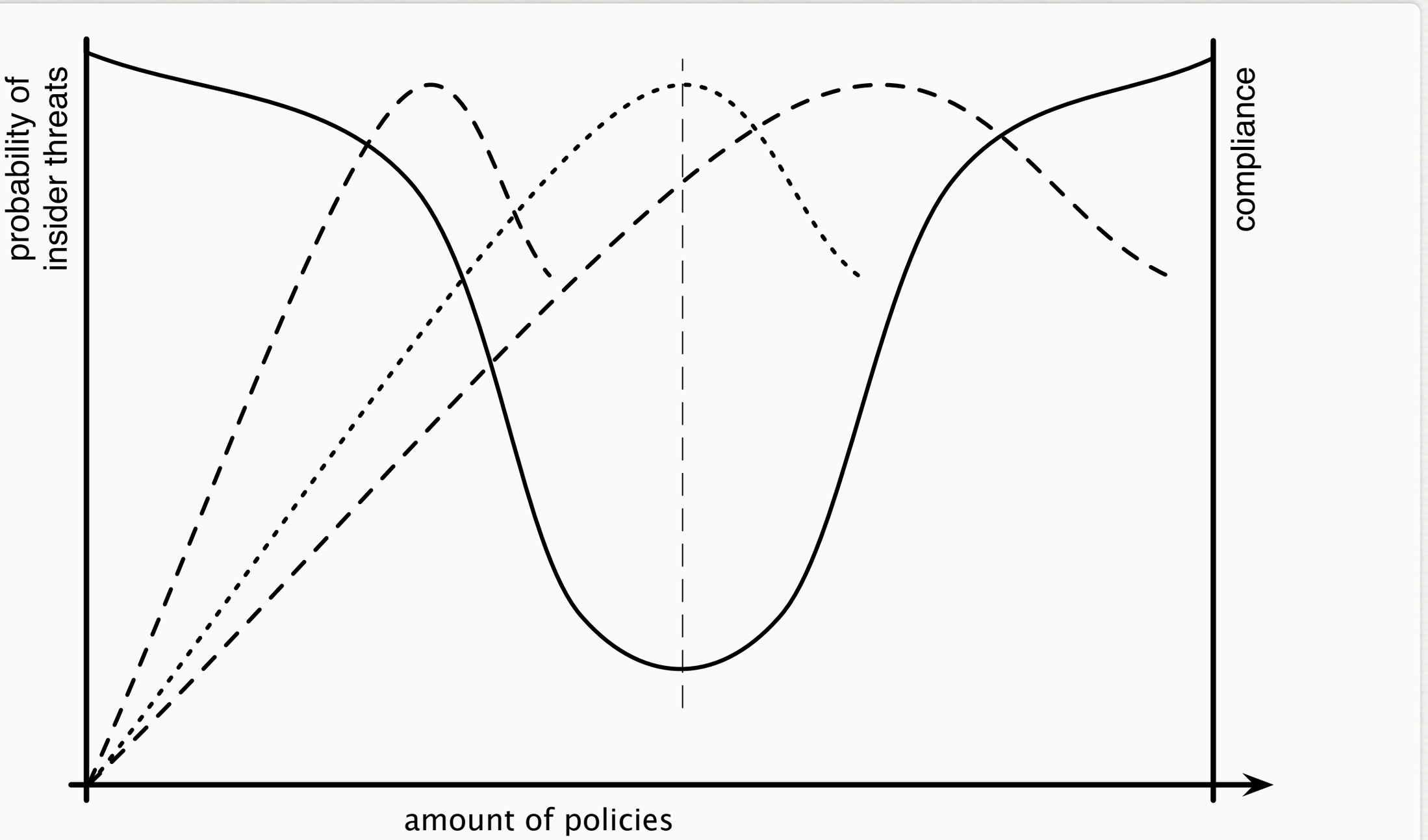
Compliance vs. Policies



Probability of Attack vs. Policies



Ideal: Sweet Spot
(Maximal Compliance, Minimal Risk)

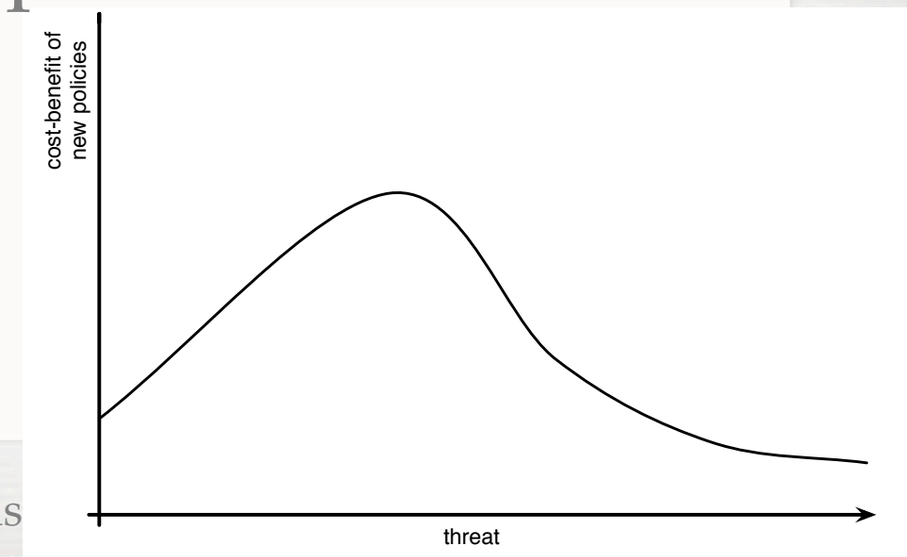


Policies and Compliance

- Two kinds of policies
  - control or monitor behaviour
  - motivate insiders to act in an appropriate way
- Costs (hidden and real) can be high and difficult to measure
  - These costs include the cost of enforcing them as well as that caused by (negatively) influencing staff time and motivation

Enforcing Simple Trust

- Mostly access control and monitoring
- Commonly accepted cost/benefit ratios
- Beneficial in preventing or discouraging large set of activities
  - Question is how much mitigation is acceptable
- However, only beneficial up to a point



Managing Complex Trust

- Same problems faced by simple relations, plus
  - When does complex behaviour signal an insider threat (as opposed to creative behaviour)?
- How real are the threats a policy targets--will it ever materialise?
  - This is hard to measure
- What is the cost of yet another policy?

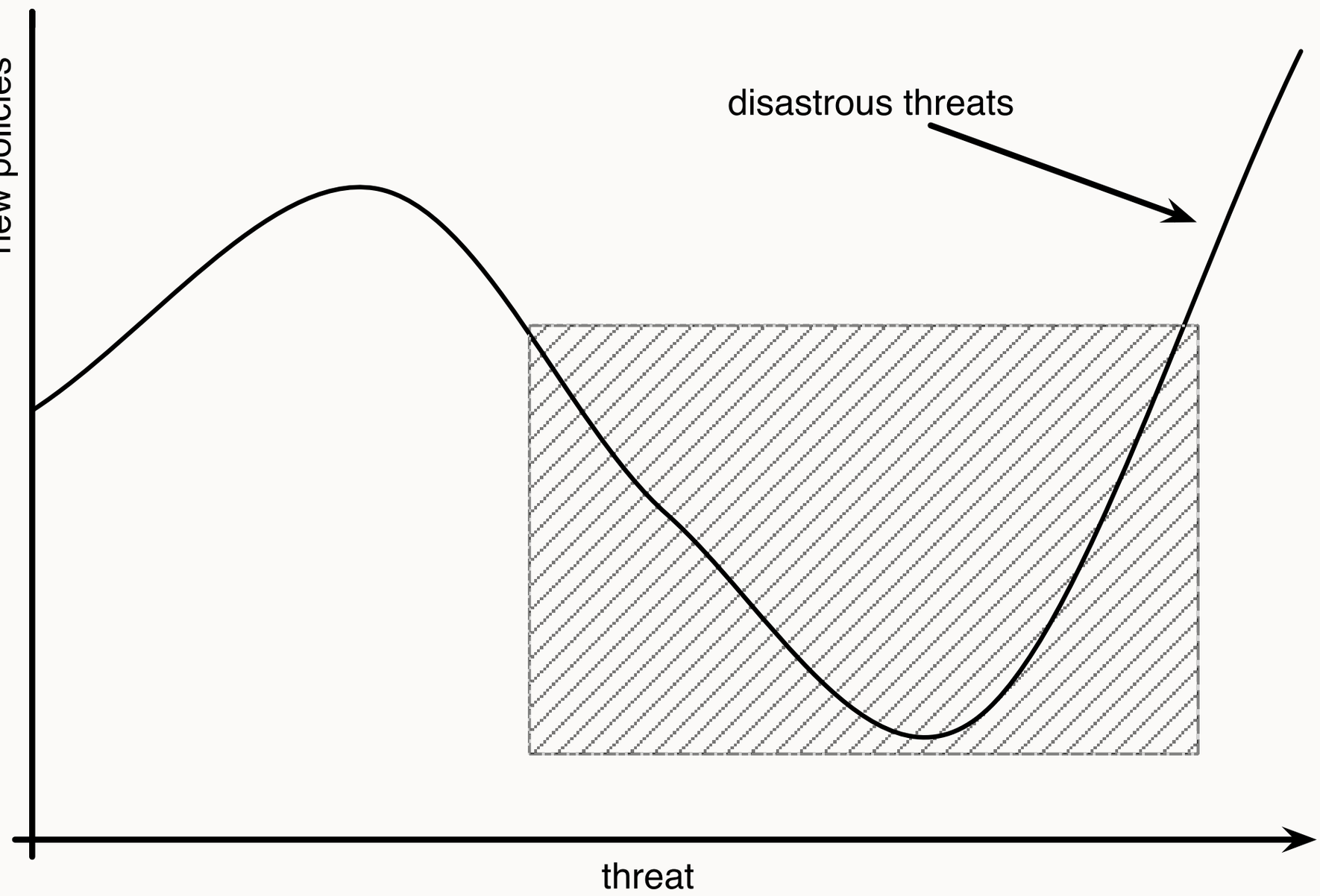
Goals

- Organisations have complex, potentially conflicting goals
  - Maximise gain function
  - Minimise risk of (inside and outside) attacks
  - Maximise compliance
- Malicious insiders have complex goals, too
  - Maximise personal gain or harm to a member of the organisation (or the whole organisation)
  - Minimise risk of being caught

The Risk of Risk Analysis

- Complex trust relationships are associated with complex behaviour
  - Complicates understanding nature of threats, the potential loss, and probabilities of both
- Major, complex insider threats seem to be rare
  - But have devastating consequences, which should be part of the risk analysis

Value Function



Conclusions

- Organisations should choose to behave economically rational for all but high-level threats
  - Pick those threats that can be handled
    - For the rest, mitigate after the fact
- Try to ensure successfulness of mitigation after the fact
- Change behaviour of employees
  - Establish a trusting relationship between employees and organisation