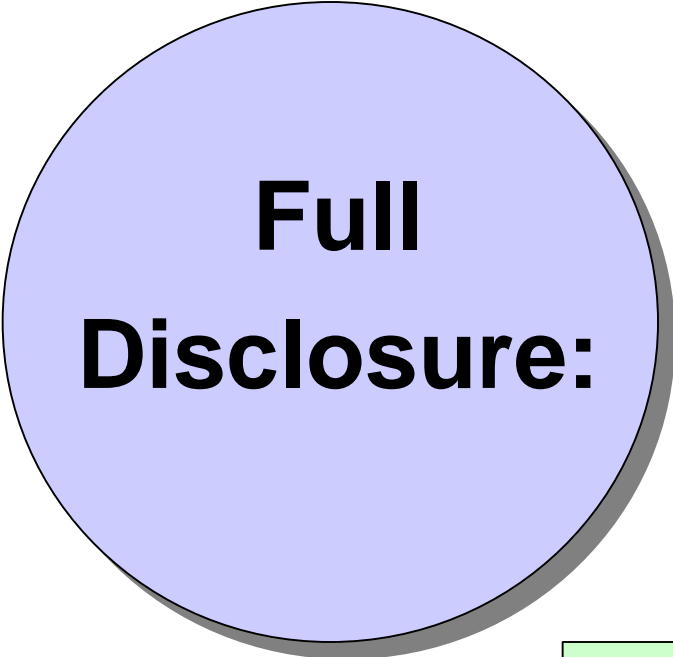# The Full Disclosure Problem:

Is Coalition a Remedy?

Dmitri Nizovtsev,
Ph.D. candidate

Marie Thursby,
Burton D. Morgan Chair of
International Management and Policy

*CERIAS sponsored project

Full Disclosure:

- Why disclose?

- Why the controversy?

- What is socially desirable?

- Feasible solutions?

2

Commonly believed motives for full disclosure:

- fame (reputation building);
- educating other end users;
- putting pressure on vendor.

Our explanation:

Self-interest (minimizing expected loss)

The Model

Three types of "agents":

Black Hats — attack other users when they can

White Hats — choose whether to disclose or not

Vendors — choose when to issue a fix

Independent discoveries of the same bug are possible.

Methodology

- **Game theoretic approach**
- **Agents minimize their expected losses**
- **Society minimizes the damage from attacks**

Exogenous parameters

- **Size of the population**
- **Share of black hats in the population**
- **Damage from each attack**
- **Difficulty of developing a fix**
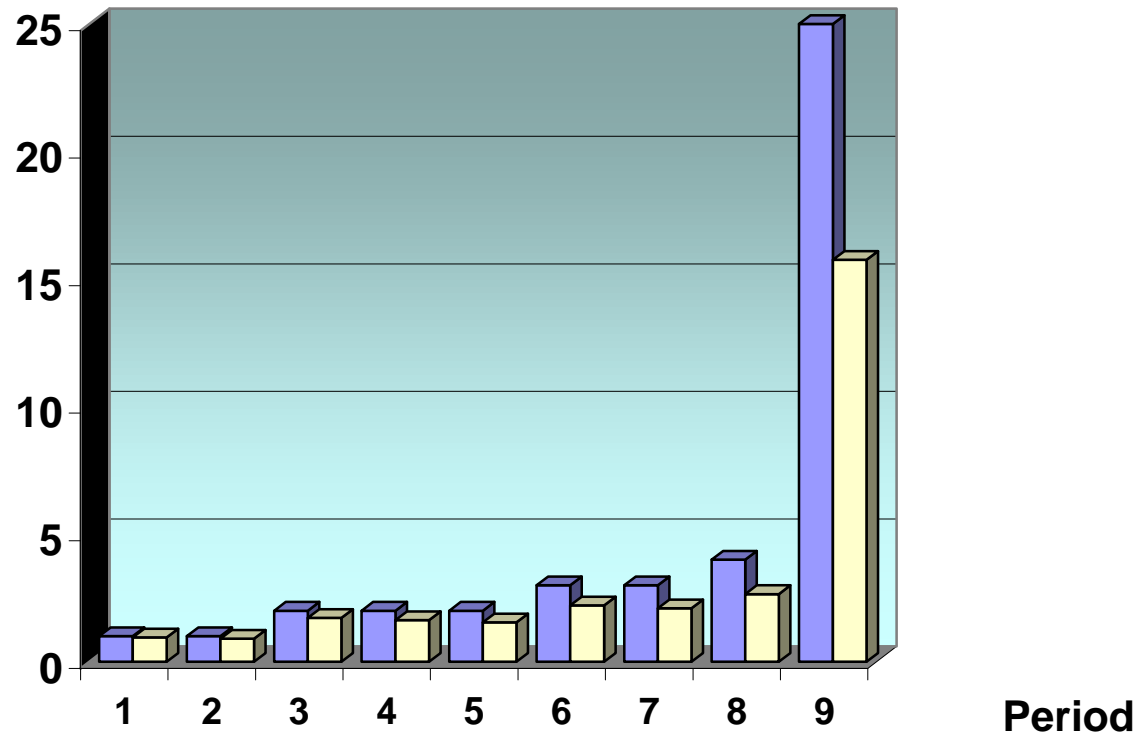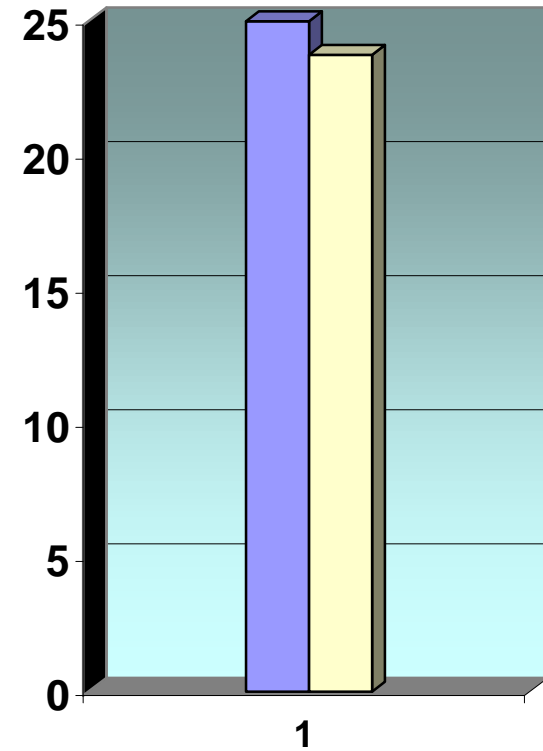- **Chances of independent discovery**

Decision Tree
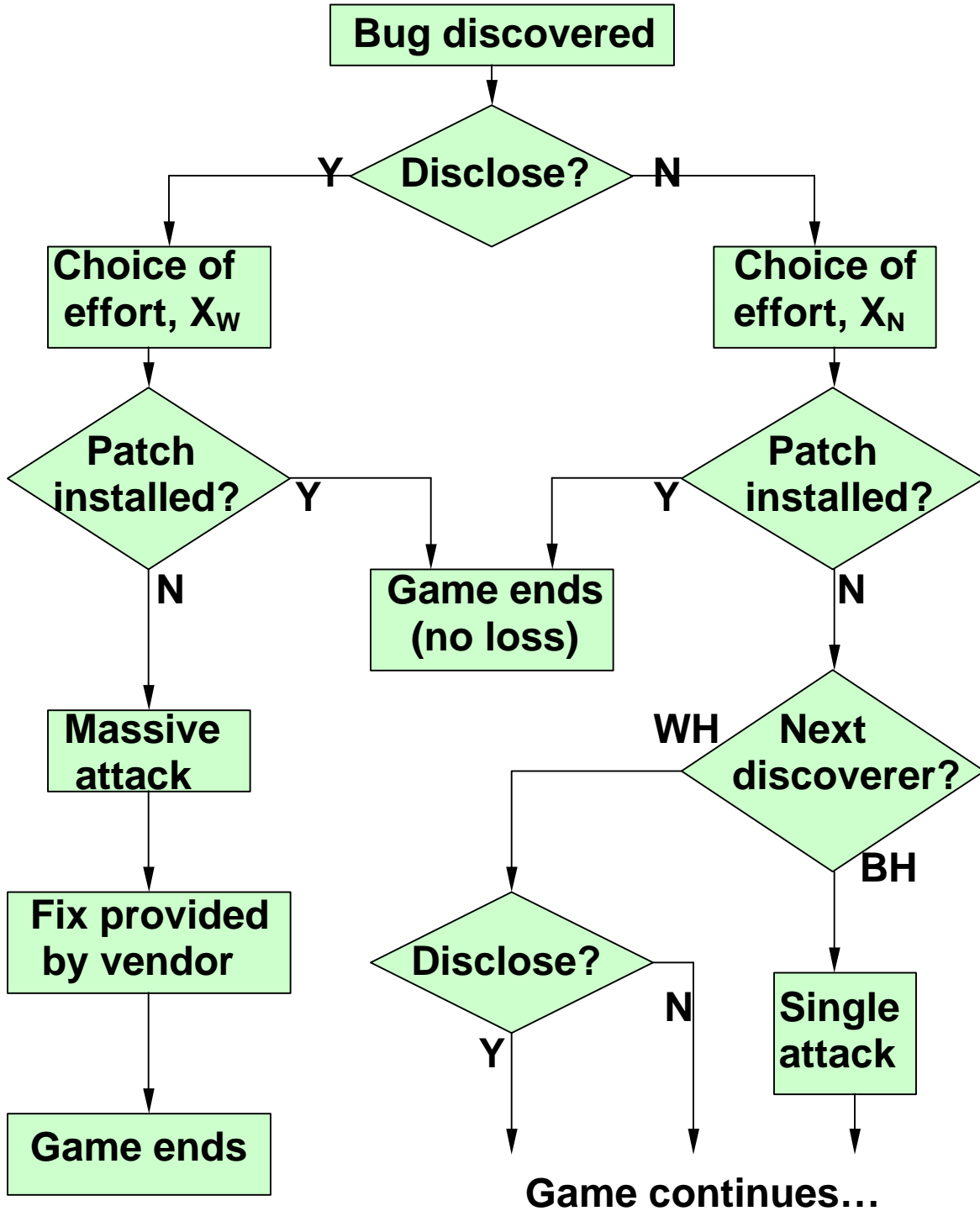
Loss Structure

NON-DISCLOSING AGENT
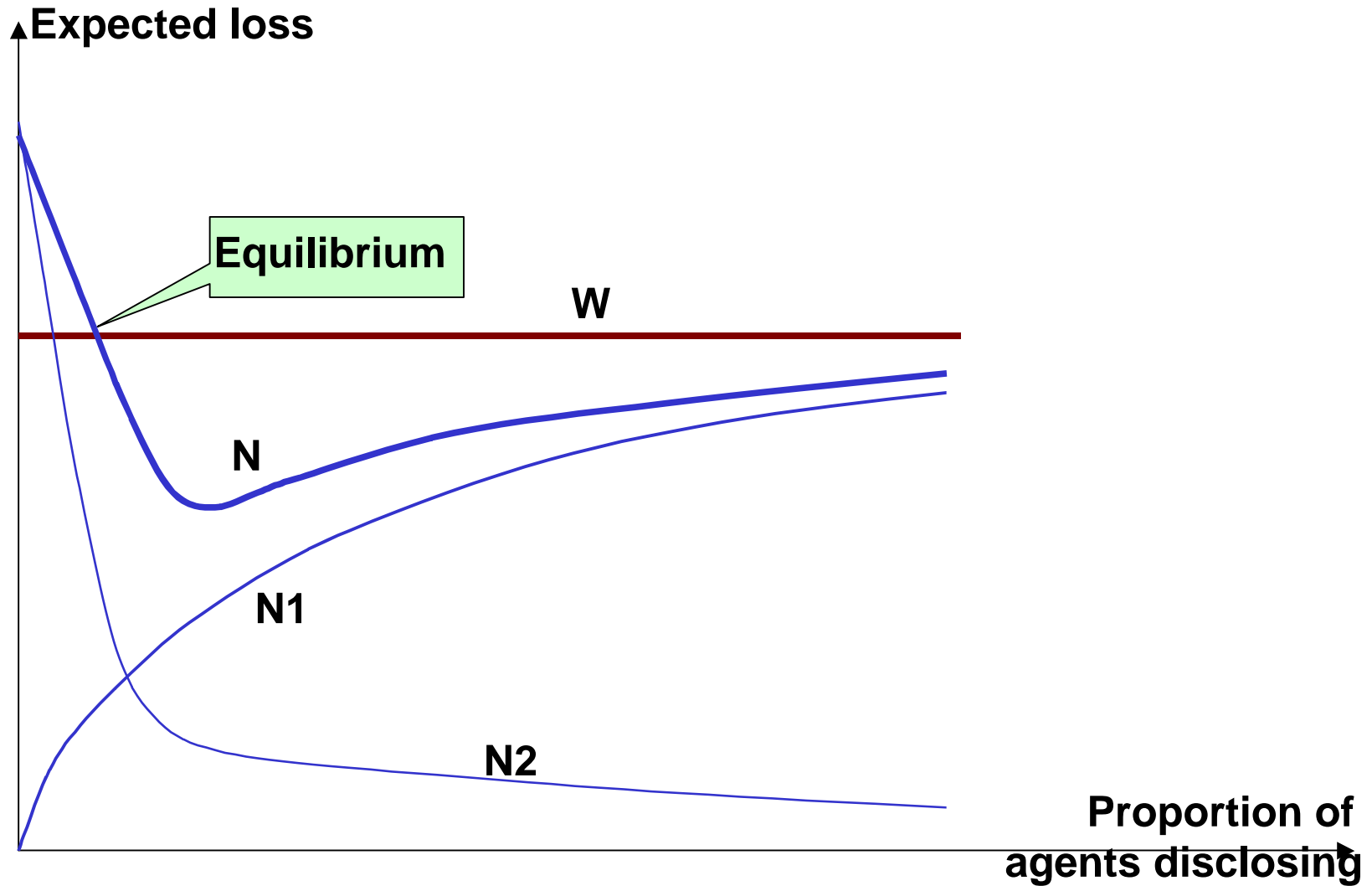
DISCLOSING AGENT

Period

■ Absolute Loss
□ Discounted Loss

7

W – agents disclosing to the World
N – agents Not disclosing
N1 – loss from massive attack (result of FD)
N2 –loss from occasional attacks (result of discoveries)

Results

There are cases (and we may deal with one) when

Full Disclosure is
- *Inevitable*
- *Desirable*

Comparative statics:

Full disclosure occurs more often as
- Bugs become easier to discover
- Population increases
  - It *possibly* occurs more often as
    - Software gets more complex
    - Average damage from an attack decreases
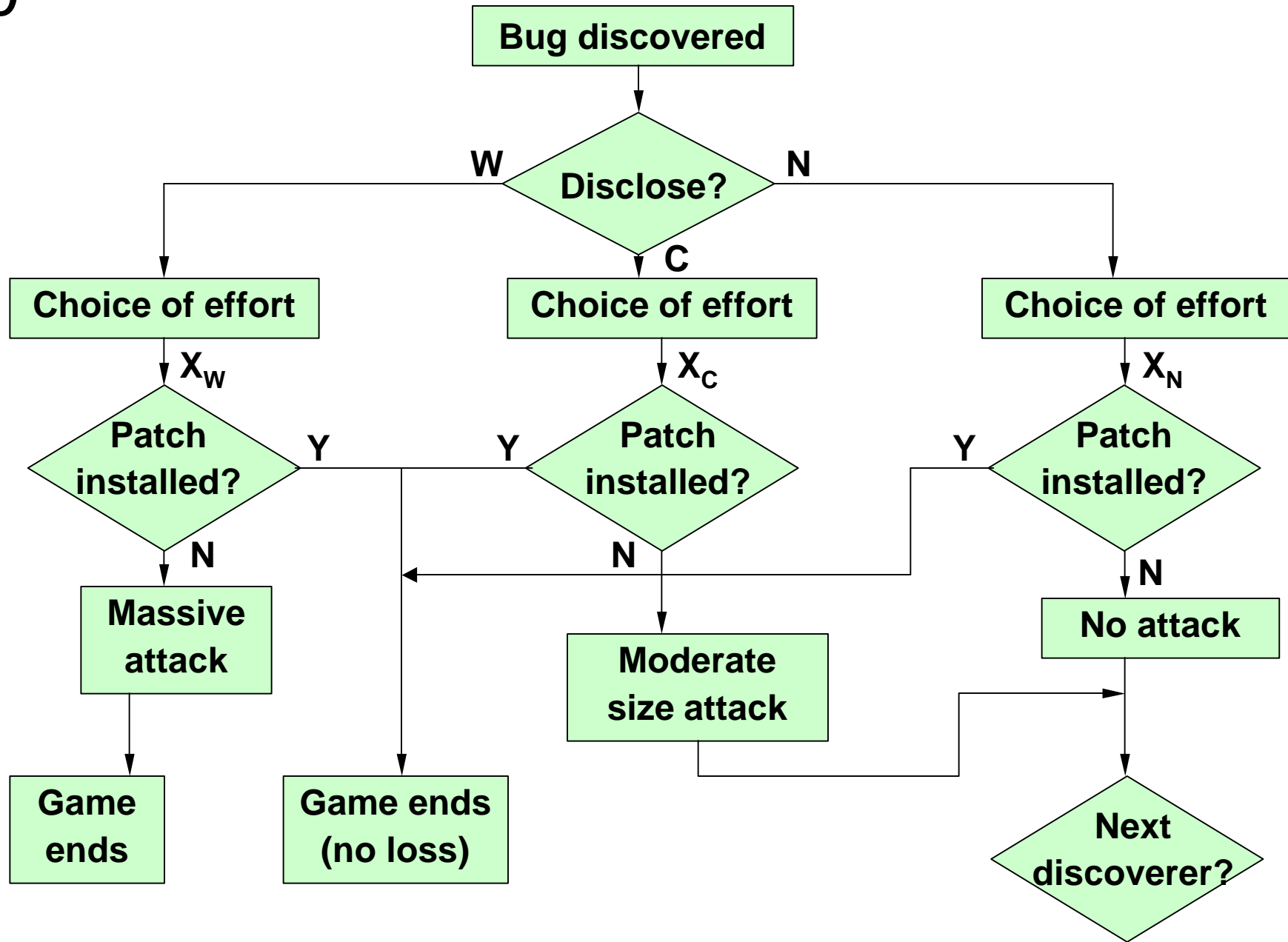   - Portion of black hats in the population decreases

Suppose we have a coalition of agents anyone can disclose information to.
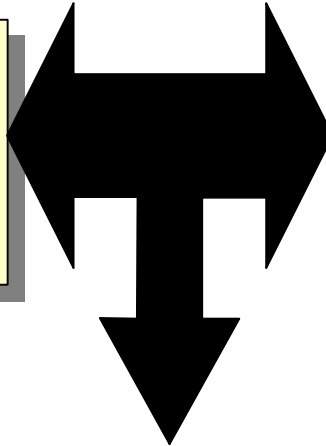
- **Does it change incentive structure?**

- **What happens to aggregate damage from attacks?**

10

Bug discovered

Disclose?

W → **Choice of effort**
C → **Choice of effort**
N → **Choice of effort**

X_W → **Patch installed?**
X_C → **Patch installed?**
X_N → **Patch installed?**

Patch installed? — Y

Patch installed? — N → **Massive attack** → **Game ends**

Patch installed? — Y → **Game ends (no loss)**

Patch installed? — N → **Moderate size attack**

Patch installed? — Y

Patch installed? — N → **No attack**

Moderate size attack → **Next discoverer?**

No attack → **Next discoverer?**

A coalition may improve the situation
only if…

Software is not too complex
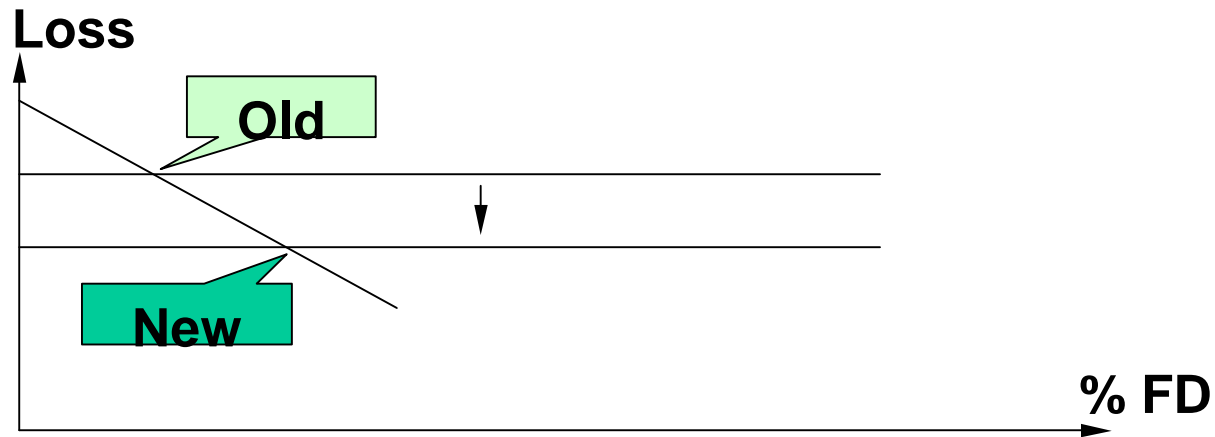
Coalition members are willing to work on a patch

Otherwise,
a coalition has no effect!

We recommend:

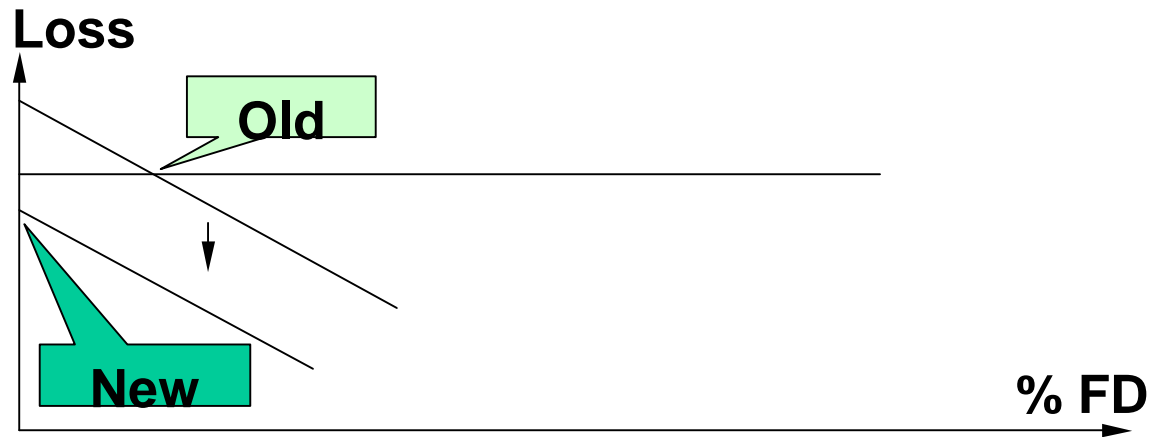**Target the cause, NOT the effect!!!**

Approach A

Loss

% FD

- Reduce average size of damage from an attack
- Reduce portion of black hats in the population

Approach B

Loss

Old

New

% FD

- Improve quality of software products
- Accelerate the fixes

Towards a perfect model

Issues deserving further study:

- **Mechanism of vendors' decisions**
- **Different schemes of disclosure**
- **End users' reluctance to patch**
- **Heterogeneous population**
- **Data available, anyone?**