A Comparative Analysis of Software Liability Policies

Terrence August
Rady School of Management
University of California, San Diego

Introduction

In the current network environment, there are serious incentive problems among various actors whose decisions impact the overall security of the cyber infrastructure; the risks associated with attacks on this infrastructure are growing in number and potential impact; and the importance of the role of regulation is increasingly understood and debated.

However, answering *how* regulation can actuate a shift toward preferable outcomes, such as an increasingly secure cyber infrastructure and higher social surplus associated with these public resources, is not well understood and requires formal analysis. We begin to explore this important question by analyzing an economic model that captures both security interdependence and the primary underlying incentives of actors.

One corrective means to address the underlying incentive problems which has received intense debate in the security community is the ownership of liability for network security losses. We investigate how liability policies can be used to increase Internet security considering the effects of interconnectivity and the resulting interdependence of users' security actions on one another.

Research Questions

1. In the short run, when the security level of a software product is fixed, what role should software liability play? What form of liability is most effective?
2. Given significant negative externalities associated with software patching and security attacks, what shapes vendor incentives to invest in software security?
3. In the long run, with vendor investment, can security liability be effective? If so, what is the best approach to vendor liability?
4. How do other policies such as software security standards compare to traditional liability?

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. CNS-0954234.

Model

- Consumer valuation space: $v \in \mathcal{V} = [0,1]$
- Security losses: αv
- Cost of patching: $c_p > 0$
- Probability of security attack on *patchable* vulnerability: π_a
- Probability of security attack on *zero-day* vulnerability: π_z

Consumer Strategy Set: $S = \underbrace{\{B, NB\}}_{\text{Buy / Not Buy}} \times \underbrace{\{P, NP\}}_{\text{Patch / Not Patch}} - (NB, P)$

Consumer's Problem:

Security Externality

$$C(v,\sigma) \triangleq \begin{cases} \pi_a u(\sigma)\alpha v + \pi_z b(\sigma)\alpha v & if \quad \sigma(v) = (B, NP)\,; \\ c_p + \pi_z b(\sigma)\alpha v & if \quad \sigma(v) = (B, P)\,; \\ 0 & if \quad \sigma(v) = (NB, NP)\,. \end{cases}$$

$$u(\sigma) = \int_{\mathcal{V}} 1_{\{\sigma(v) = (B,NP)\}}\, dv$$ Size of unpatched population

$$b(\sigma) = \int_{\mathcal{V}} 1_{\{\sigma(v) \in \{(B,NP),(B,P)\}\}}\, dv$$ Size of user population

$$\begin{aligned} \max_{s} \quad & (v - p)\cdot 1_{\{s \neq (NB,NP)\}} - C(v, \sigma_{-v}) \\ s.t. \quad & \\ & s \in S \end{aligned} \qquad [\dagger]$$

Consumers solving $[\dagger]$ yields an equilibrium strategy profile:

$$\sigma^*(v) = \begin{cases} (NB, NP) & if \quad 0 \le v < v_b\,; \\ (B, NP) & if \quad v_b \le v < v_p\,; \\ (B, P) & if \quad v_p \le v \le 1\,. \end{cases}$$

v_b | Valuation threshold above which consumers purchase

v_p | Valuation threshold above which consumers patch

- Vendor's share of zero-day losses: λ_z
- Vendor's share of patching costs: λ_p
- Policy in question: $\tau \in \{p, z\}$
- Security losses:

$$L_\tau \triangleq \begin{cases} \int_{v_p}^{1} c_p \, dv & if \quad \tau = p\,; \\ \int_{v_b}^{1} \pi_z \alpha (1 - v_b) v \, dv & if \quad \tau = z\,, \end{cases}$$

- Security investment cost: $C(\beta)$

Vendor Profit: $\Pi(p, \beta, \lambda_\tau) \triangleq p(1 - v_b) - \lambda_\tau L_\tau - C(\beta)\,,$

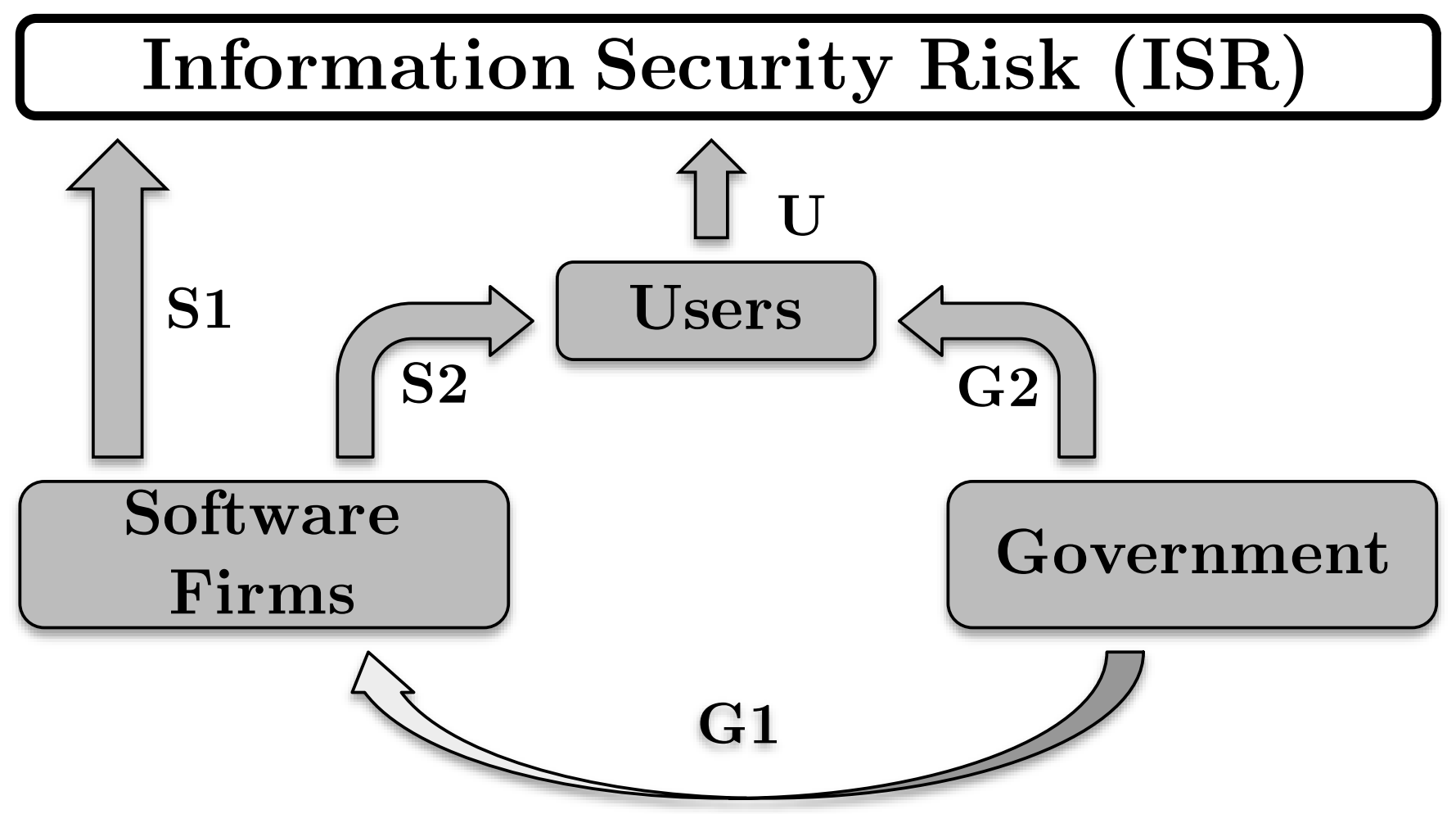
Vendor's Problem: Sets price and investment level

$$\begin{aligned} \max_{p,\beta \in [0,1]} \quad & \Pi(p, \beta, \lambda_\tau) \\ s.t. \quad & (v_b, v_p) \text{ satisfy } \sigma^*(\cdot \,|\, p, \beta, \lambda_\tau) \end{aligned} \qquad [\ddagger]$$

Regulator's Problem: Sets loss and patch liability shares

$$\begin{aligned} \max_{\lambda_\tau \in [0,1]} \quad & W(\lambda_\tau, \beta^*(\lambda_\tau)) \\ s.t. \quad & (v_b, v_p) \text{ satisfy } \sigma^*(\cdot \,|\, p^*(\lambda_\tau), \beta^*(\lambda_\tau), \lambda_\tau) \\ & (p^*(\lambda_\tau), \beta^*(\lambda_\tau)) \text{ solve } [\ddagger] \end{aligned}$$

Economic Agents / Incentives



Legend

G1: Software liability, open source development subsidies, regulations on software development security practices, and tax penalties on software with poor security

G2: Software liability, taxes on software usage, incentive rebates for patching, and subsidies for usage of open source software and/or SaaS offerings

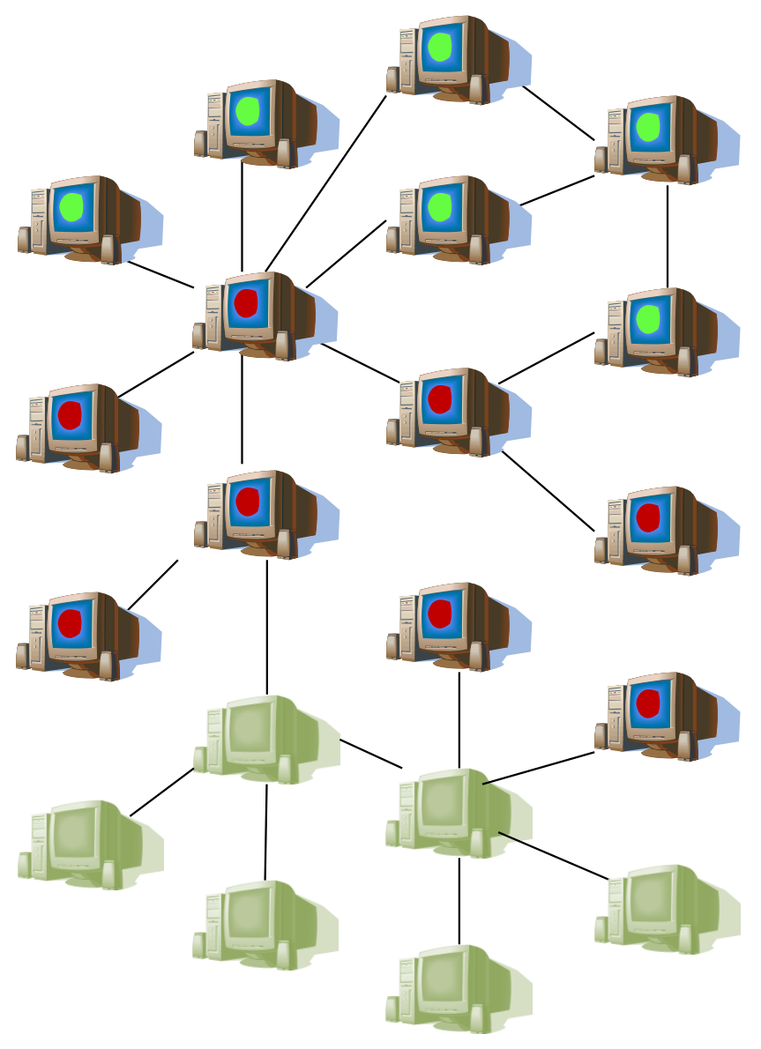
S1: Design of software offering (on-premises vs. SaaS), and investment in software product security

S2: Design of software offering, source code strategy (open source or proprietary), incentive rebates for patching, investment in software product security, and product pricing

U: Consumer usage and patching behavior

ISR: Measured by the likelihood of successful security attacks and expected aggregate security losses

Consumer Market Structure

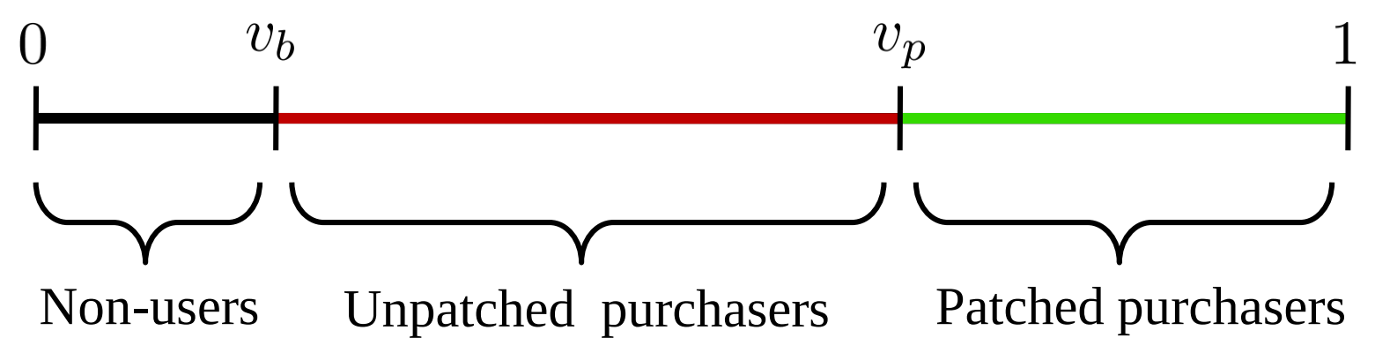


Non-users

Patched users

Unpatched users

Low Price Region



Equilibrium Equations

$$\text{I.} \quad v_b = p + \pi_a (v_p - v_b)\alpha v_b + \pi_z (1 - v_b)\alpha v_b$$

$$\text{II.} \quad c_p = \pi_a (v_p - v_b)\alpha v_p$$

Results

We find that:

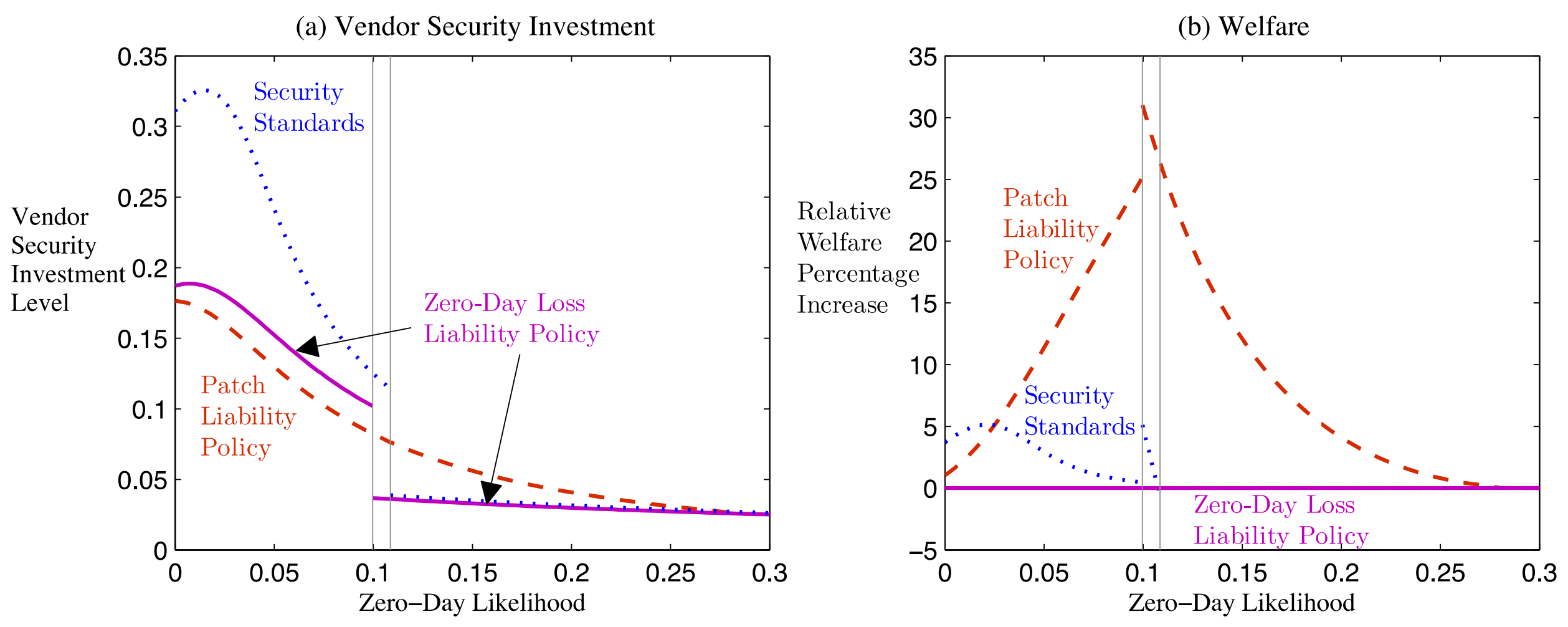
1. Liability on zero-day losses tends to be outperformed by security standards and liability on patching costs
2. Security standards work best in environments with low zero-day security risk
3. Liability on patching costs is generally effective and outperforms security standards as zero-day attack likelihood becomes higher

Table Summary:

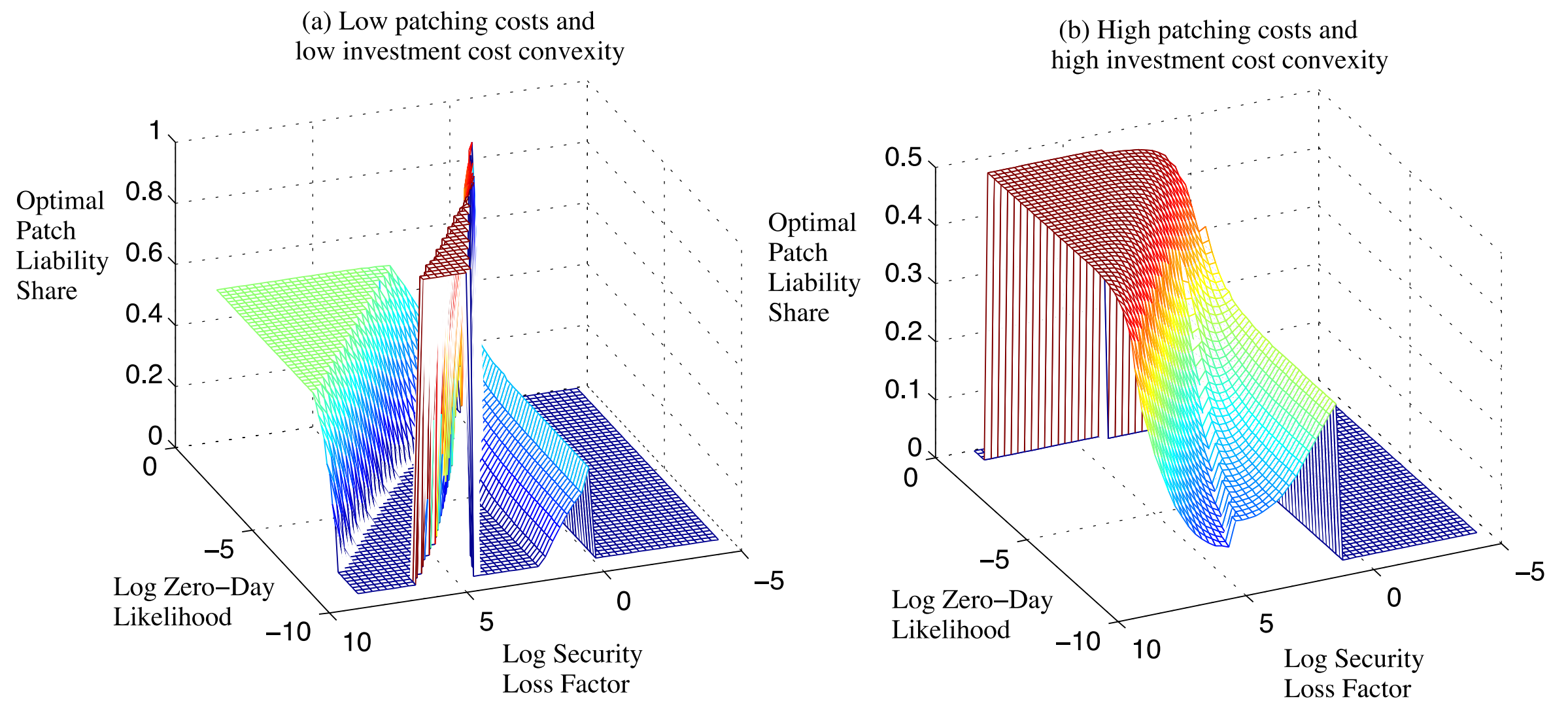
Short Run: Vendors only set prices
Long Run: Vendors also invest to adapt their security investments

	(a) Short Run		(b) Long Run	
Optimal Policy	Low patching cost	High patching cost	Low patching cost	High patching cost
Low zero-day risk	No Liability	Patch Liability	Standards	Standards
High zero-day risk	Patch Liability	No Liability	Patch Liability	Standards

Graphical Illustration of Policy Recommendations:



Optimal Liability Shares for Patch Liability:



Discussion

- Software vendors naturally have substantial incentives to invest in security
  - ❖ Investments are being made, but they are also quite costly
  - ❖ The role of liability is to encourage more "efficient" outcomes (not necessarily larger investments)
- Loss liability policies tend to be ineffective
  - ❖ Do not create incentives to boost vendor security investments
  - ❖ In fact, they can reduce these investments in many cases
- Utilizing security standards leads to the greatest level of security but is primarily useful in less risky environments where the vendor lacks strong investment incentives
- Patch liability (or sharing of patching costs) works best in risky environments
  - ❖ Provides greater incentives for users to protect the entire network
  - ❖ Patch liability is actually a ***substitute*** to security investment (i.e., it is more efficient to address user behavior than the inherent attack likelihood)
  - ❖ Easy to implement as a price discount because patching status is readily communicated

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 - 29th 2012
National Harbor, MD