Main Results
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.

Optimal Liability Shares for Patch Liability:

Microeconomic Model
- Consumer valuation space: $v \in \mathcal{V} = [0, 1]$
- Security losses: $AL$
- Cost of patching: $c_p > 0$
- Probability of security attack on patchable vulnerability: $\pi_v$
- Probability of security attack on zero-day vulnerability: $\pi_z$
- Consumer strategy set: $S = \{B, N, B\} \times \{P, NP\} - \{NB, P\}$

\[ C(v, \sigma) = \max_{s \in S} \left( v - p \right) \cdot 1_{\{s \neq (NB, NP)\}} - C(v, \sigma_v) \]

Vendor’s Problem
\[
\max_{p, L_T, \lambda_v \in [0, 1]} \quad \Pi(p, \beta, \lambda_v) = p(1 - v_b) - \lambda_v L_T - C(\beta)
\]
\[ s.t. \quad (v_b, v_p) \text{ satisfy } \sigma_v^*: (p, L_T, \lambda_v) \]
- Vendor’s share of security losses: $\lambda_v$
- Security losses:
  \[ L_T = \begin{cases} 
  \int_0^{v_b} \pi_v (1 - v) \, dv & \text{if } \tau = p; \\
  \int_0^{v_b} \pi_z (1 - v) \, dv & \text{if } \tau = z, 
\end{cases} \]

Regulator’s Problem
\[
\max_{\lambda_v \in [0, 1]} \quad W(\lambda_v, \beta(\lambda_v))
\]
\[ s.t. \quad (v_b, v_p) \text{ satisfy } \sigma_v^*: (\lambda_v, \beta(\lambda_v), \lambda_v, (p^*(\lambda_v), \beta^*(\lambda_v))) \text{ solve } [\dagger] \]

Equilibrium Consumer Market Structure
\[
\begin{array}{c}
0 \\
\text{Unpatched Users} \\
1 \\
\text{Patched Users}
\end{array}
\]

Discussion
- 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.