Data Security in the Digital Age

Reputation and Strategic Interactions in Security Investment

Ying Lei Toh

Toulouse School of Economics

March 31, 2016

Motivation

Data security: A quick look... [1]

- **1,540** data breaches in 2014
- Over **1 billion** records compromised
- **55%** of breaches occurred due to malicious attacks
- Prominent breaches: Target, Home Depot, Ebay, Sony, Ashley Madison ...

[1] Source: http://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php

Motivation

- Data breaches can lead to adverse consequences for consumers
- Rampant data breaches may be indicative that firms underinvest in security
- More firms going digital + growing sophiscation of cybercriminals $\rightarrow$ more data breaches
- What can be done to incentivise firms to invest more?

Overview & Main Results

Model Overview

- Players
  - Baseline: Website and unit mass of consumers (het. valuation)
  - Extended: Website, representative consumer and bank
- Two periods
- Unobserved (one-time) security investment by website at the start
- Consumer learning via imperfect breach detection $\rightarrow$ customer turnover (reputation cost)

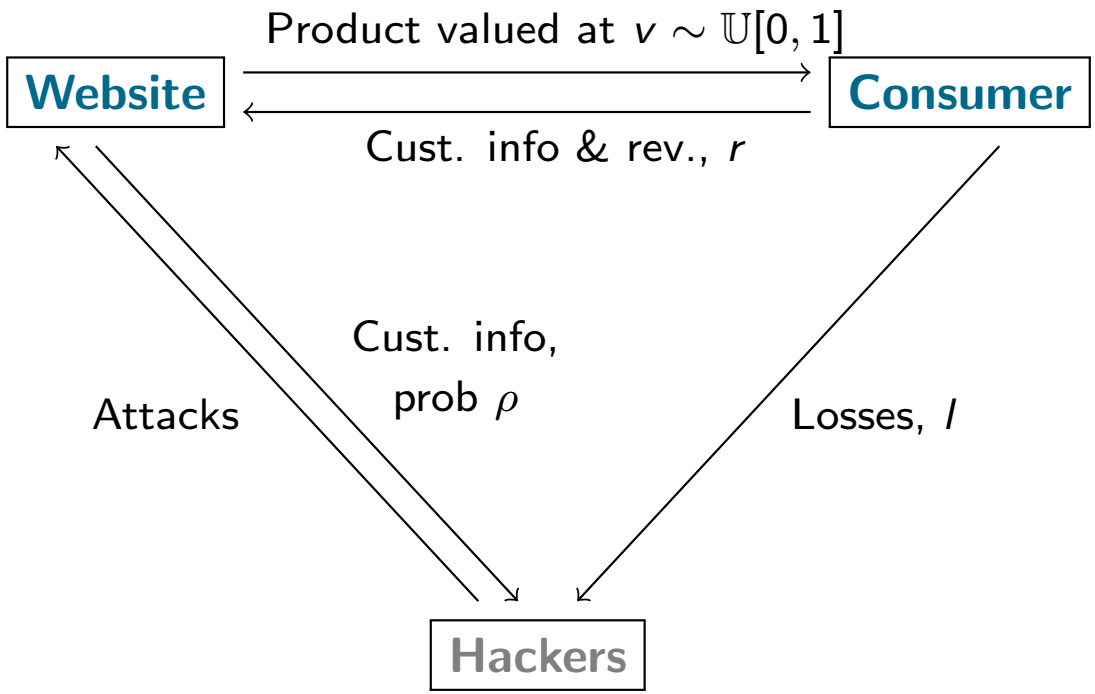
Overview & Main Results

Main Results

- Underinvestment in data security from perspective of consumer protection
- Mandatory breach notification
  - May not always lead to a higher level of investment/overall level of security
  - May result in full crowding out of website's investment
  - Effect on consumer surplus may be *ambiguous*

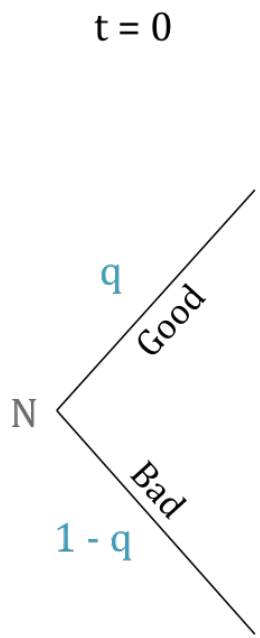
Baseline Model

- Website and unit mass of consumer with het. valuation, v
- Two states of security: good ($\rho = 0$) and bad ($\rho = \rho_B > 0$)



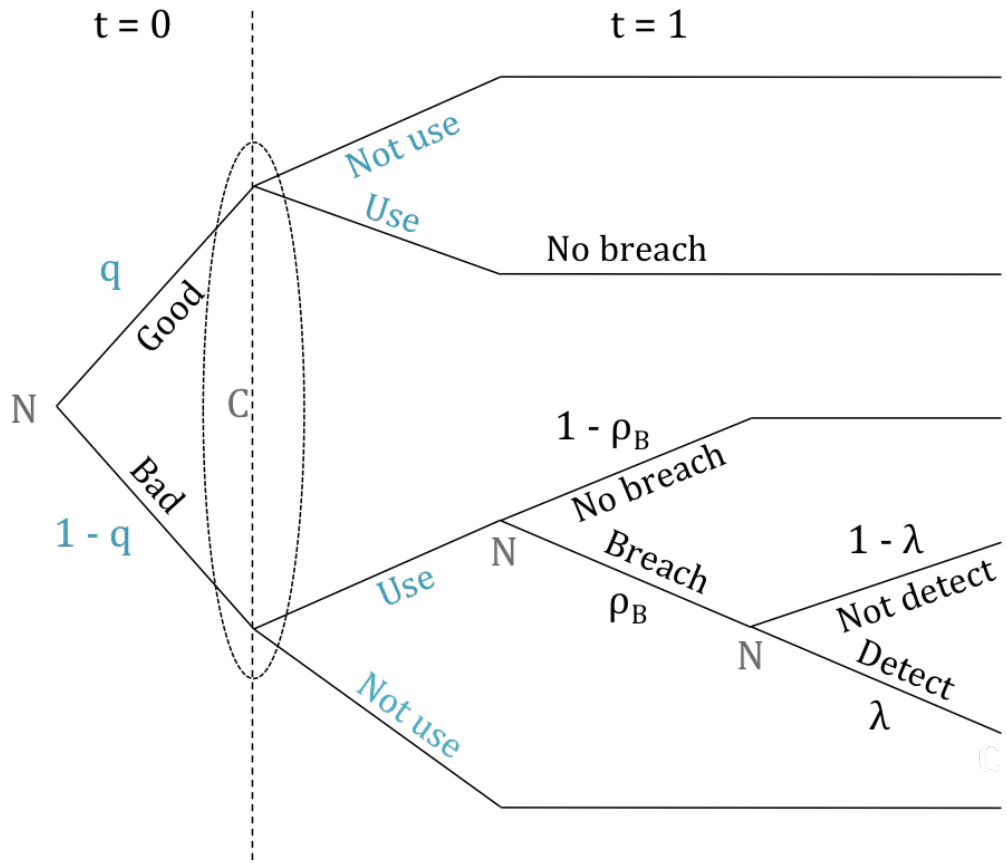
Timing

- t=0: Website invests $c(q)$ in security



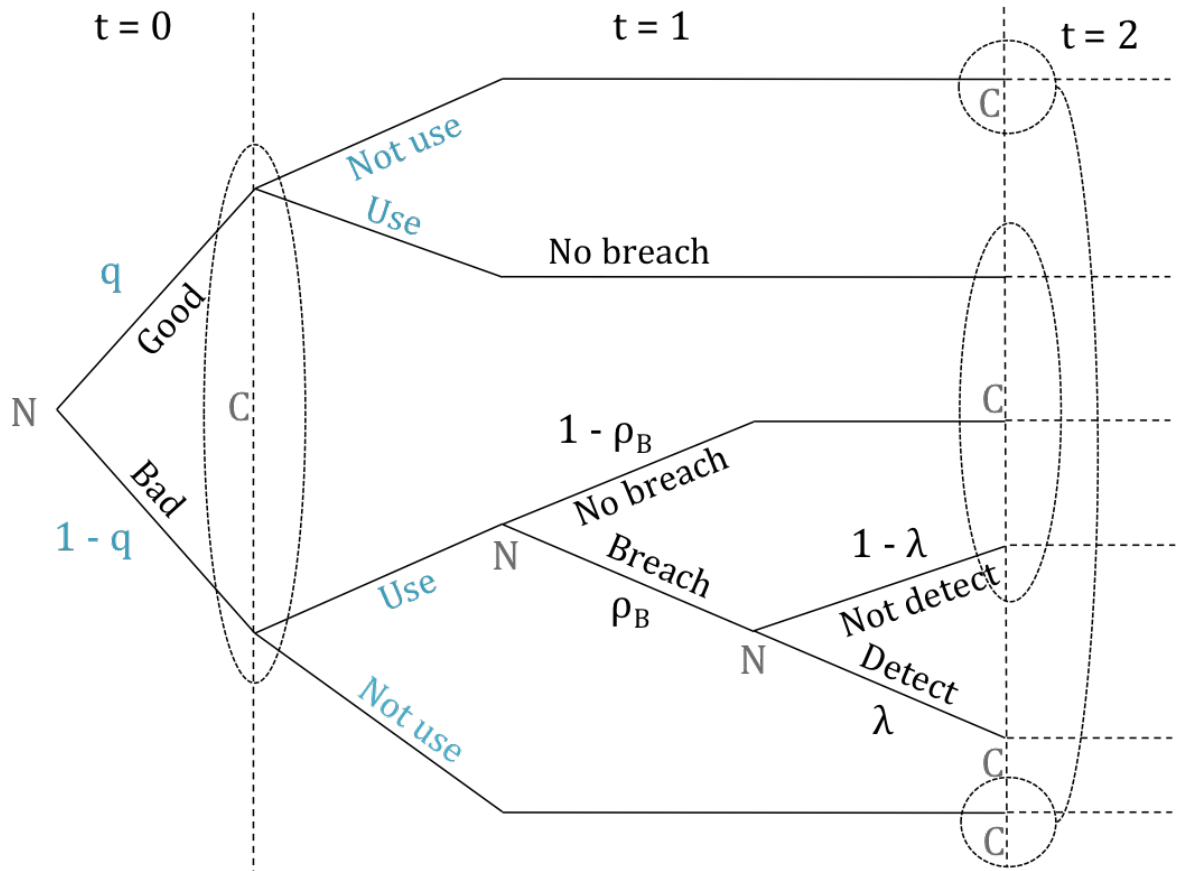
Timing

- t=0: Website invests $c(q)$ in security
- t=1: Consumers decide whether to use website, breach may occur and may be detected. Users update their beliefs.



Timing

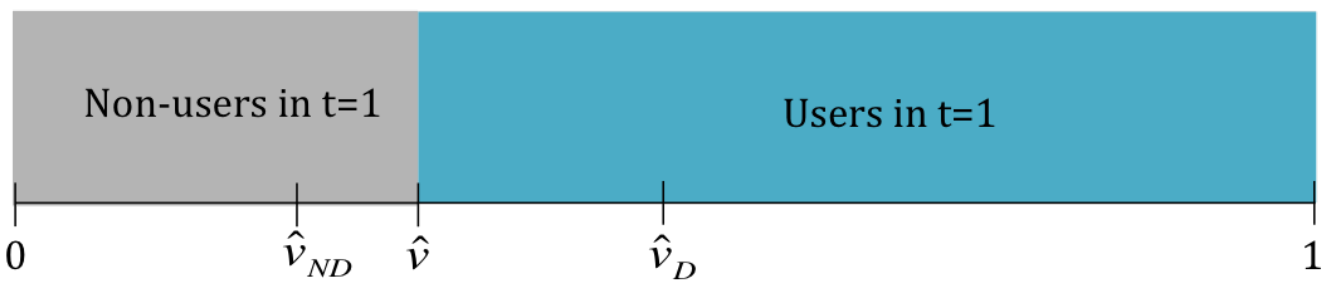
- t=0: Website invests $c(q)$ in security.
- t=1: Consumers decide whether to use website, breach may occur and may be detected. Users update their beliefs.
- t=2: Consumers decide whether to use website...



Strategies

Consumers:

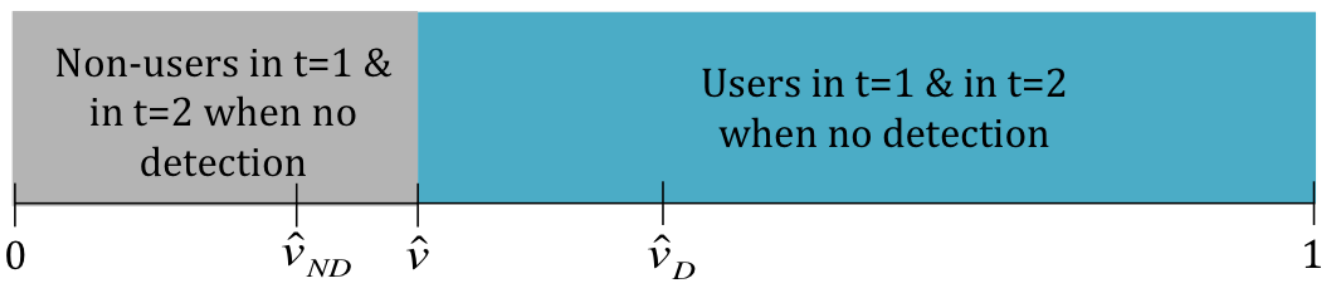
- Decide whether to use the website given beliefs: $E(U) = v - E(\rho)l$ vs. 0
  - t=1: Use if $v \geq \hat{v}$



Strategies

Consumers:

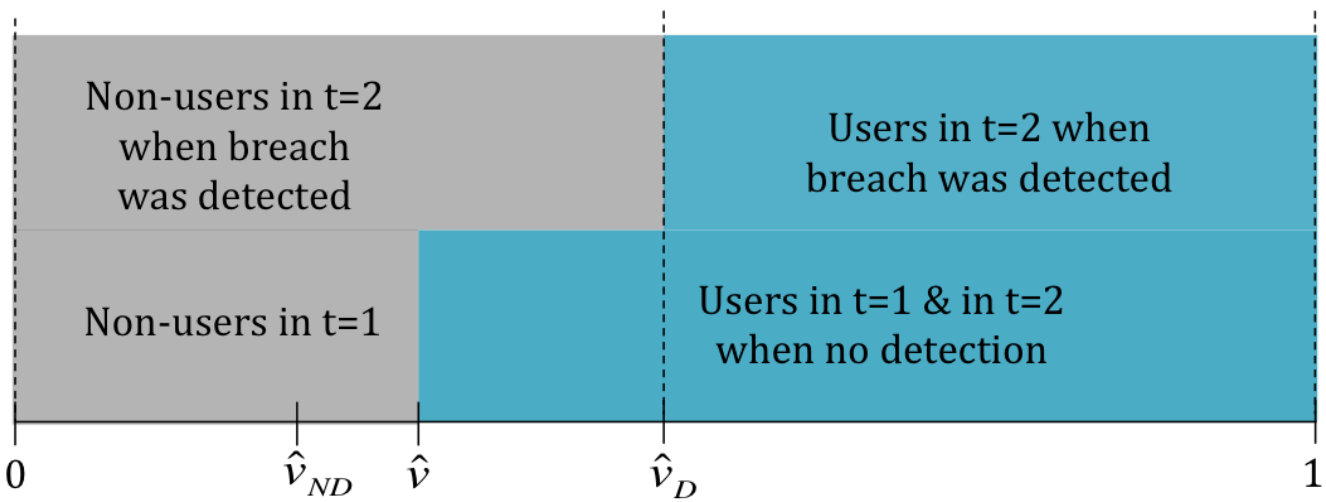
- Decide whether to use the website given beliefs: $E(U) = v - E(\rho)l$ vs. 0
  - t=1: Use if $v \geq \hat{v}$
  - t=2: Use if $v \geq \hat{v}_{ND}$ when no breach detected



Strategies

Consumers:

- Decide whether to use the website given beliefs: $E(U) = v - E(\rho)l$ vs. 0
  - t=1: Use if $v \geq \hat{v}$
  - t=2: Use if $v \geq \hat{v}_{ND}$ when no breach detected and $v \geq \hat{v}_D$ when breach detected ($\hat{v}_{ND} > \hat{v} > \hat{v}_D$)



Strategies

Website:

- Set level of security, q^f, to max profit: Website's Problem

$$\max_{q^f} \pi(q^f, \lambda, \rho_B, \hat{v}, \hat{v}_D, r)$$

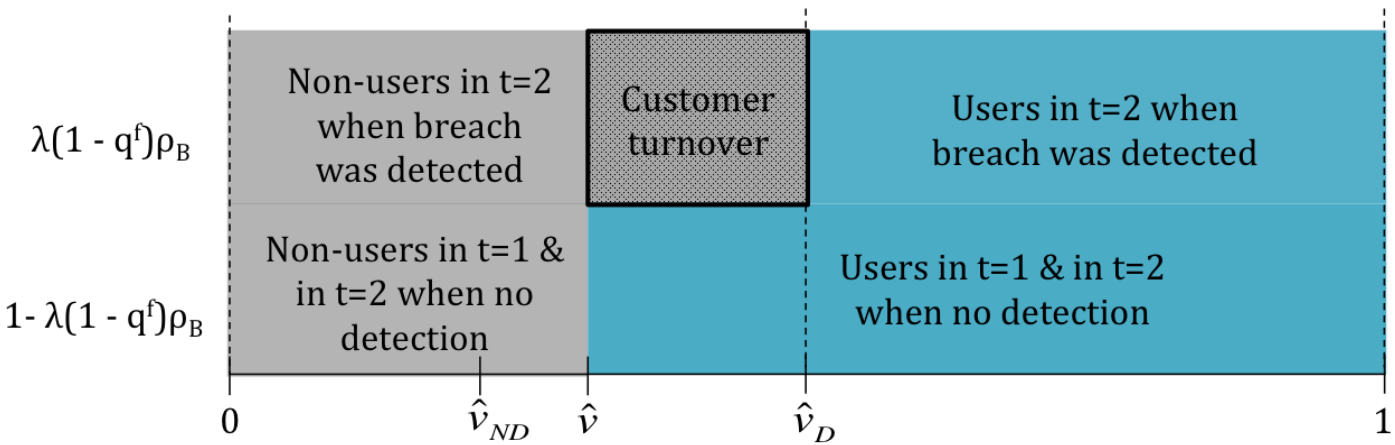
Strategies

Website:

- Set level of security, q^f, to max profit: Website's Problem

$$\max_{q^f} \pi(q^f, \lambda, \rho_B, \hat{v}, \hat{v}_D, r)$$

- $c'(q^*)$ = Marg. reduction in loss from cust. turnover ($MB(q^*)$)



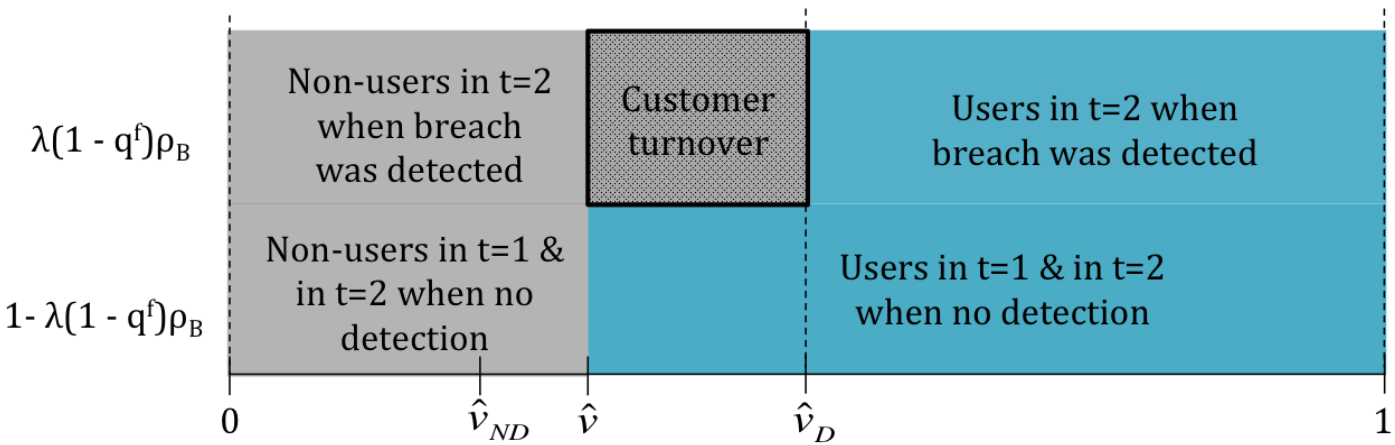
Strategies

Website:

- Set level of security, q^f, to max profit: Website's Problem

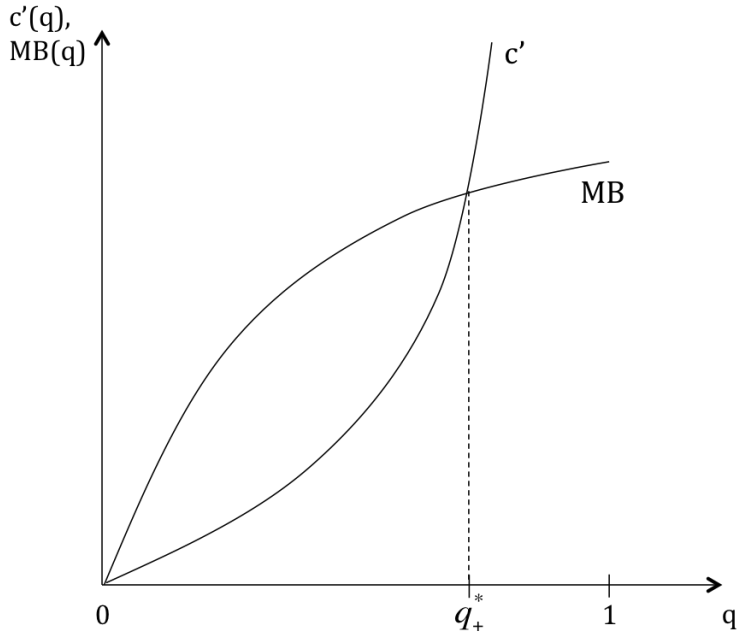
$$\max_{q^f} \pi(\underbrace{q^f, \lambda, \rho_B}_{\text{prob. of turnover}}, \underbrace{\hat{v}, \hat{v}_D, r}_{\text{size of turnover}})$$

- $c'(q^*)$ = Marg. reduction in loss from cust. turnover ($MB(q^*)$)



Equilibrium

- Stable Bayes-Nash equilibrium where website invests q_+^* in security



- Too little investment from consumer protection perspective

Mandatory Breach Notification

- Website to inform customers of breaches in a timely fashion
- Increases prob. of breach detection (λ) to 1
- More investment in equilibrium if consumers are passive

Mandatory Breach Notification

- Website to inform customers of breaches in a timely fashion
- Increases prob. of breach detection (λ) to 1
- More investment in equilibrium if consumers are passive

  Intuition:

  Stronger learning/reputation effect
  - Direct: Breach detected with higher prob $\rightarrow$ more likely to lose customers
  - Indirect: Higher participation when no breach detected ($\hat{v}$ is smaller) $\rightarrow$ more to lose

Mandatory Breach Notification

Consumer self-protection

- Upon detecting breach, consumers may take action to mitigate fraction α of potential losses $\rightarrow U = v - \rho(1 - \lambda\alpha)l$
- $\lambda\alpha$: measure of consumers' ability to self-protect

Mandatory Breach Notification

Consumer self-protection

- Upon detecting breach, consumers may take action to mitigate fraction α of potential losses $\rightarrow U = v - \rho(1 - \lambda\alpha)l$
- $\lambda\alpha$: measure of consumers' ability to self-protect

Proposition

Equilibrium level of investment, q_+^*

- *increases* for *small* α;
- *increases* for *intermediate* α, provided that r is *large*;
- decreases otherwise.

Consumers are better off whenever q_+^* is higher (ambiguous otherwise).

Full Proposition

Mandatory Breach Notification

Intuition:

- Learning/reputation effect (+):
  - Same as with passive consumers
  - Higher reputation cost when r is larger

Mandatory Breach Notification

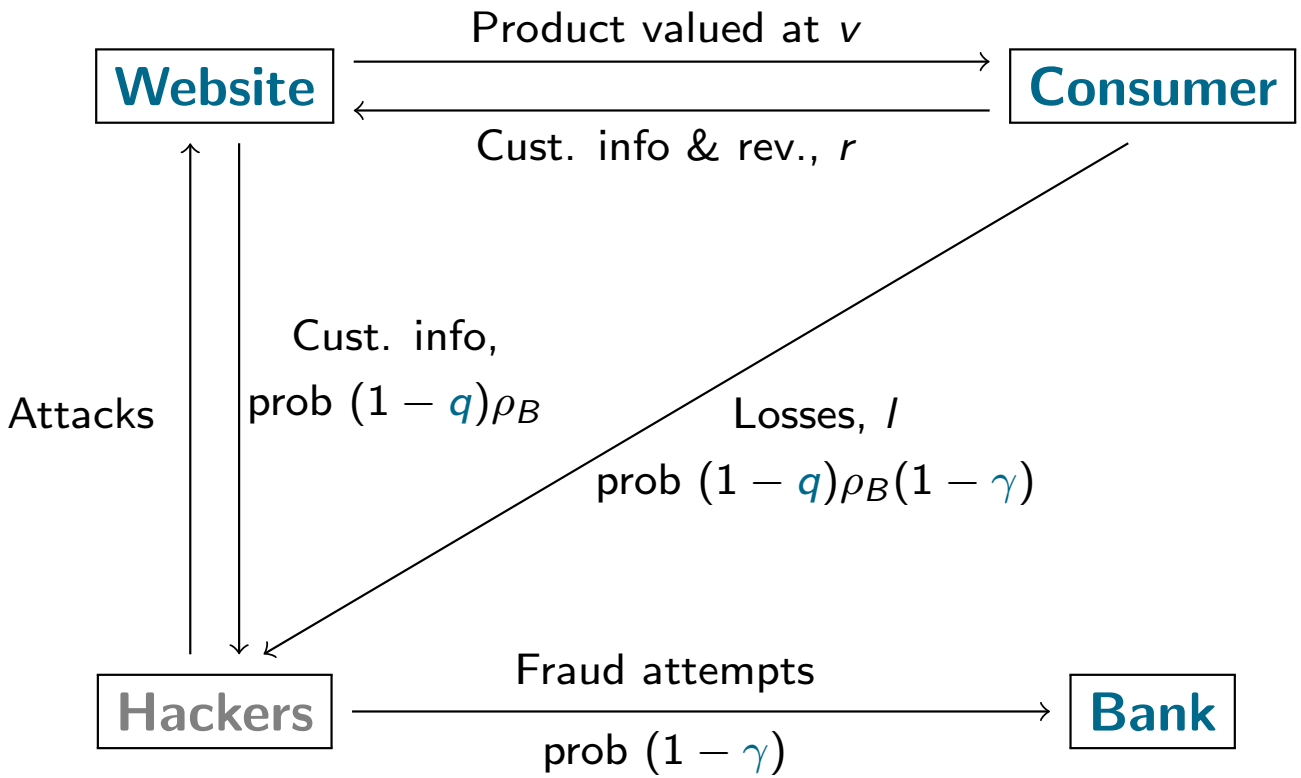
Intuition:

- Learning/reputation effect (+):
  - Same as with passive consumers
  - Higher reputation cost when r is larger
- Crowding out effect (–):
  - Larger $\lambda \rightarrow$ larger $\lambda\alpha \rightarrow$ stronger ability to self-protect
- Crowding out effect dominates when α is large

Extended Model

New player: Bank

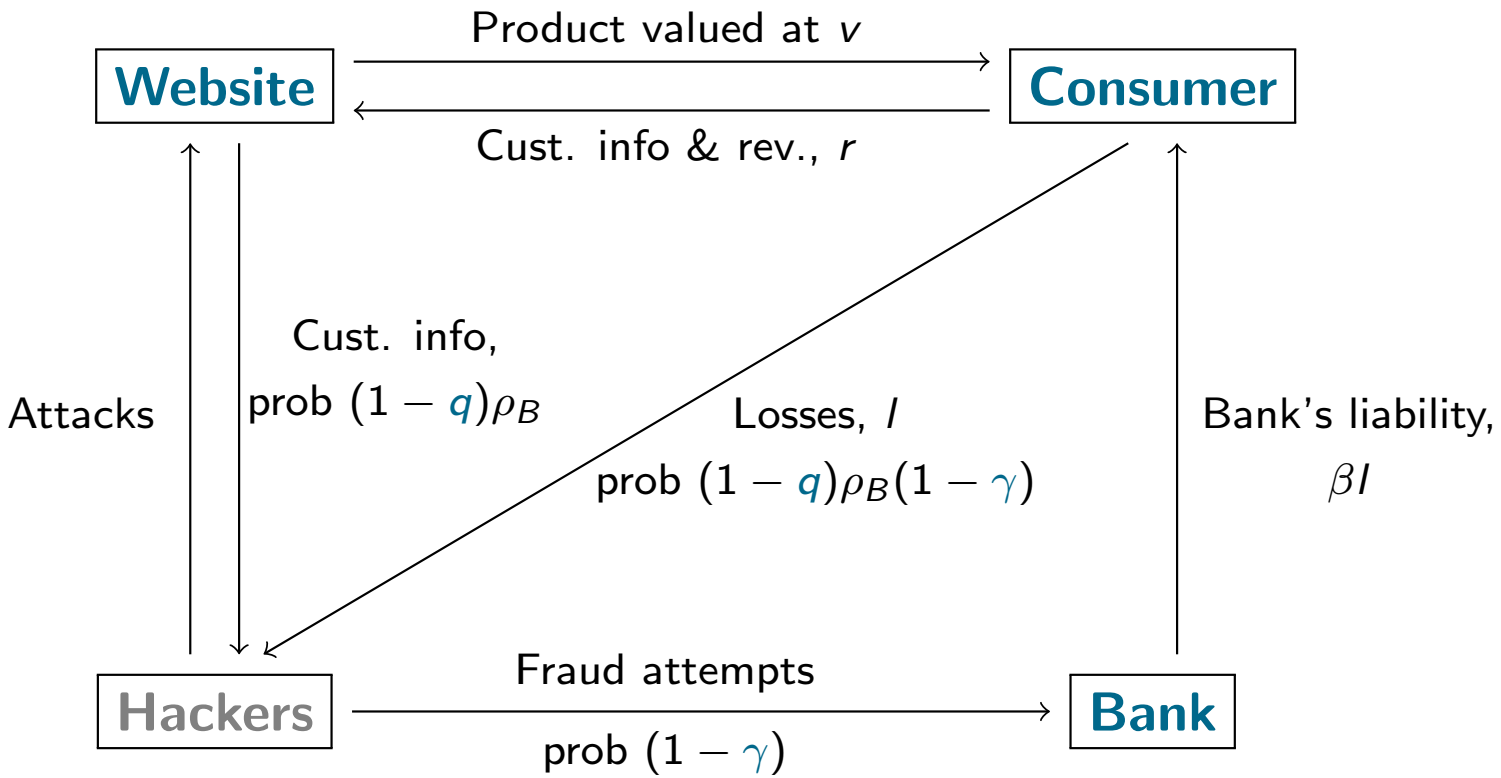
- Affects overall security level via its investment, γ (0bserved)



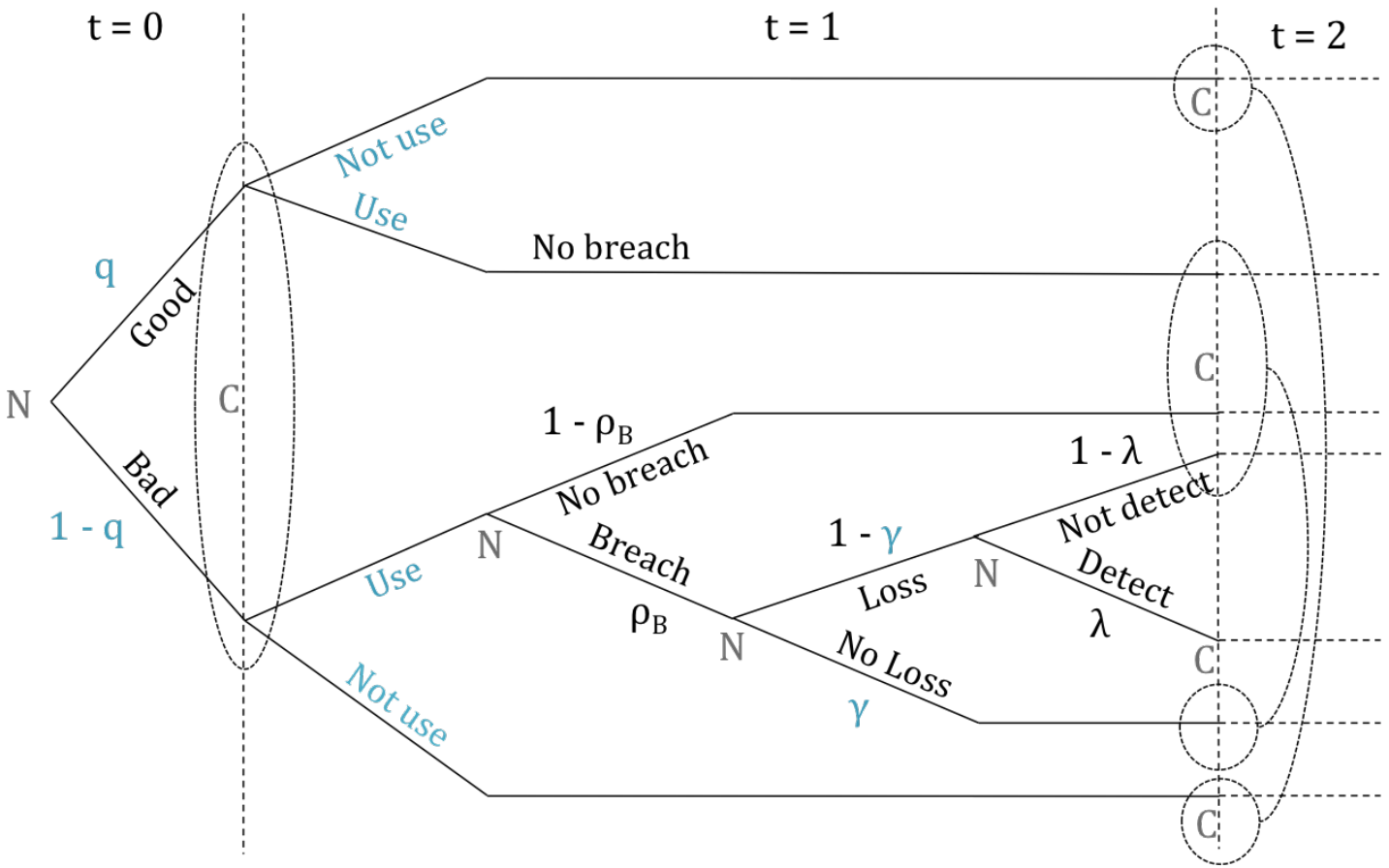
Extended Model

New player: Bank

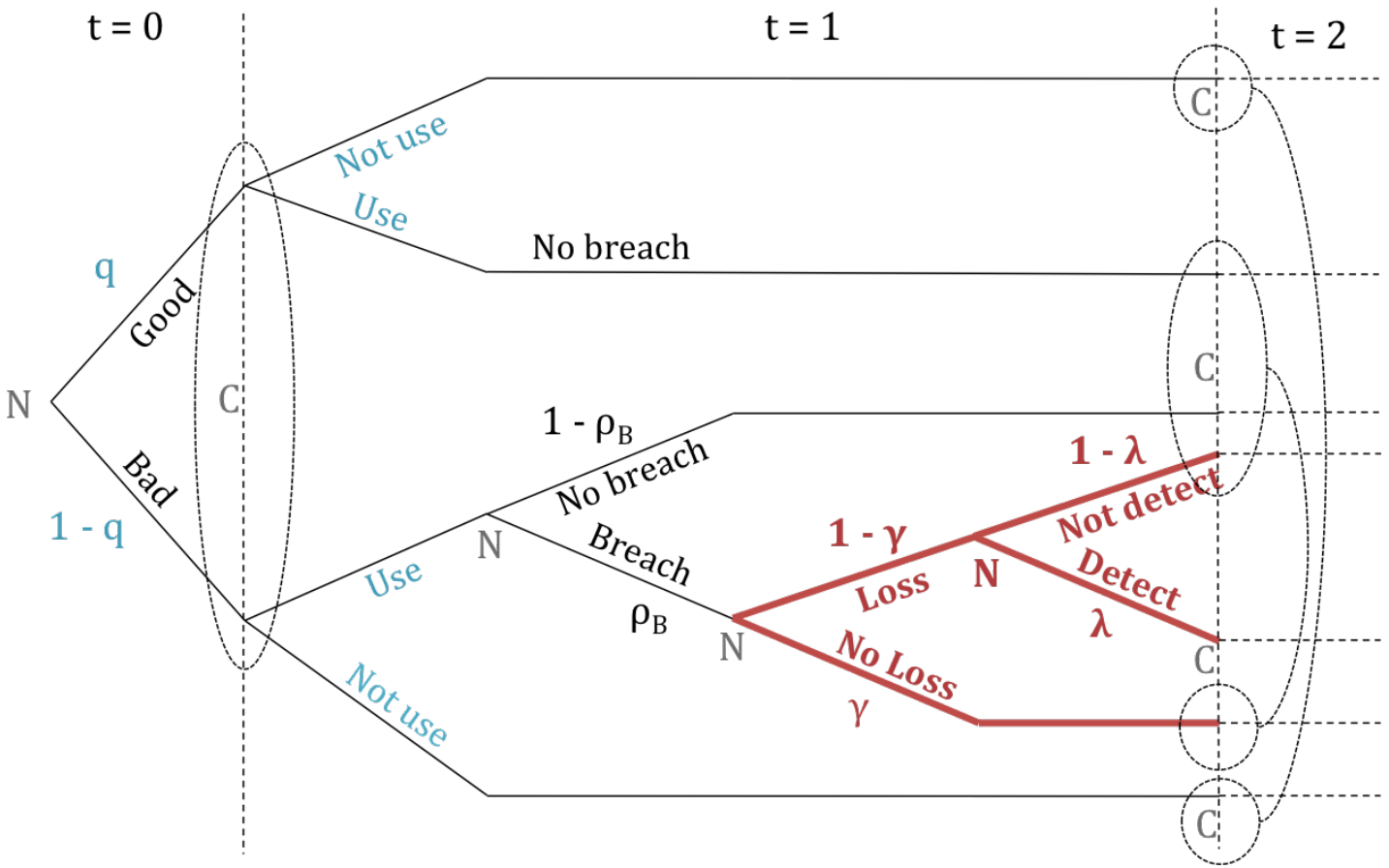
- Affects overall security level via its investment, γ (0bserved)
- Provides partial insurance to consumer, βl



Extended Model



Extended Model



Extended Model

Extended vs. Baseline:

- Pr(Loss | Breach) $= 1 - \gamma < 1$
- Consumer learns of "bad" state with prob. $\lambda\rho_B(1-\gamma) < \lambda\rho_B$

Extended Model

Extended vs. Baseline:

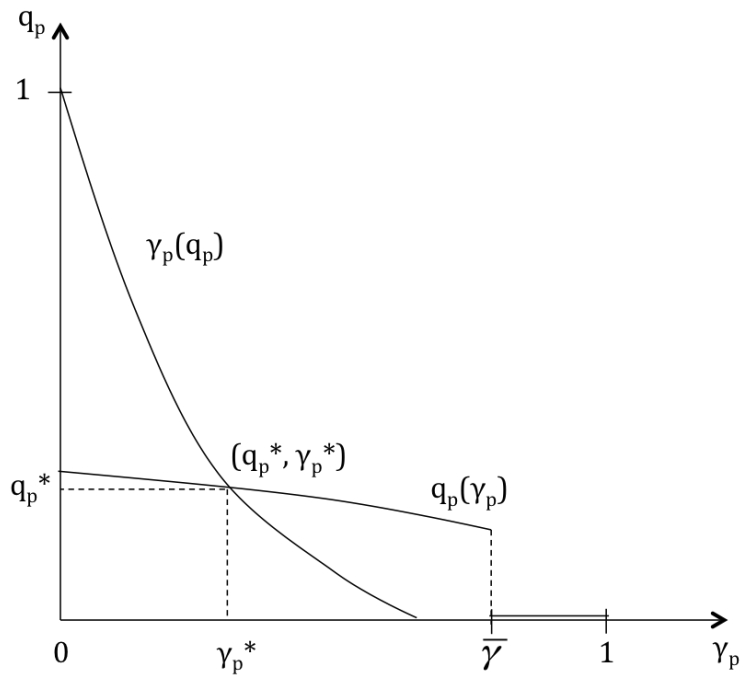
- Pr(Loss | Breach) $= 1 - \gamma < 1$
- Consumer learns of "bad" state with prob. $\lambda\rho_B(1-\gamma) < \lambda\rho_B$

Strategies:

- Bank: $\min_{\gamma} \psi(\gamma, q) = \underbrace{\phi(\gamma, q)}_{\text{Expected liability}} + \underbrace{t(\gamma)}_{\text{Inv't cost}}$
- Website: $\max_{q} \pi(q, \gamma)$
- Consumer: participate or not

Equilibrium

- Investments are strategic substitutes (for $\gamma < \overline{\gamma}$)
- Unique equilibrium with positive levels of investment by both website and bank when t' is sufficiently high



Mandatory Breach Notification

Proposition

Both *website and bank invest more* when the initial loss detection probability, $\tilde{\lambda}$, *is sufficiently small*. Consumer is made better off.

Mandatory Breach Notification

Proposition

Both *website and bank invest more* when the initial loss detection probability, $\tilde{\lambda}$, *is sufficiently small*. Consumer is made better off.

Intuition:

- Website
  - Learning/reputation effect (+)

Mandatory Breach Notification

Proposition

Both *website and bank invest more* when the initial loss detection probability, $\tilde{\lambda}$, *is sufficiently small*. Consumer is made better off.

Intuition:

- Website
  - Learning/reputation effect $(+)$
- Bank:
  - Loss detection $(+)$: higher prob. of detection $\rightarrow$ higher expected liability
  - Learning $(-)$: lower prob. of using insecure website in $t = 2 \rightarrow$ lower expected liability
  - Loss detection effect dominates when $\tilde{\lambda}$ is small

Mandatory Breach Notification

Proposition

Increase in bank's investment *fully crowds out of website's investment* when t' *is sufficiently small*.

Mandatory Breach Notification

Proposition

Increase in bank's investment *fully crowds out of website's investment* when t' *is sufficiently small*.

Intuition:

- Bank's optimality condition: $-\underbrace{\phi'(\gamma, q)}_{\substack{\text{Marg.} \\ \text{expected} \\ \text{liability}}} = \underbrace{t'(\gamma)}_{\substack{\text{MC of} \\ \text{inv't}}}$
- Optimal $\gamma > \overline{\gamma}$ for t' small $\rightarrow$ consumer moral hazard
- Consumer always participates $\rightarrow$ no incentive for website to invest

Related Literature

- Data/cyber-security investment: Gordon and Loeb (2002), Varian (2004), Bauer and Van Eeten (2009)
- Mandatory breach notification: Romanosky et al (2010)

Conclusion

- Proposed a model of security investment with reputation cost endogenously generated through consumer learning
- Consumers may be made better off by policies such as mandatory breach notification...
- But important to consider *strategic interactions* between the agents

Thank you.

Feedback and comments are welcomed at
yinglei.toh@gmail.com