Incentivizing Firms to Protect Consumer Data: Can Reputation Play a (Bigger) Role?

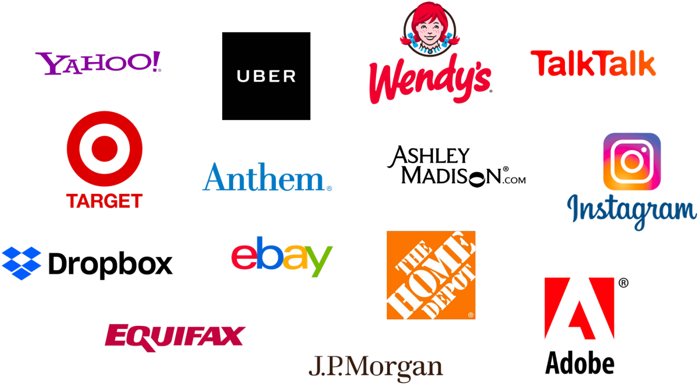
Ying Lei Toh

Toulouse School of Economics

Digital Workshop
Toulouse School of Economics
Dec 20, 2017

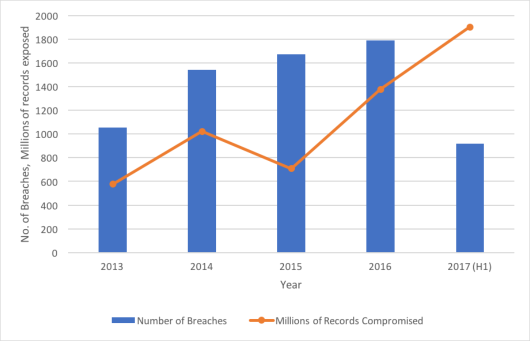
Motivation

What do all of these firms have in common?



Motivation

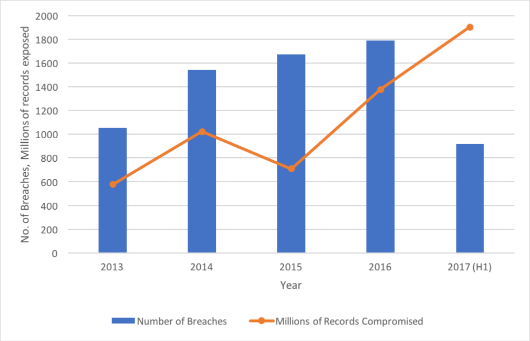
Data breaches are becoming increasingly prevalent.



Source: Breach Level Index

Motivation

Data breaches are becoming increasingly prevalent.



Source: Breach Level Index

Data breach victims may suffer costly consequences such as identity thefts and payment fraud.

Motivation

Protecting consumer data is a challenging task in this digital age.

Motivation

Protecting consumer data is a challenging task in this digital age.

> *Today's organizational crown jewels are built of bytes. Back in 2003, physical security was most important to secure a company's most valuable information...Today, everything is on a network.*
>
> —Ablon et al (2014, p.34)

Motivation

Protecting consumer data is a challenging task in this digital age.

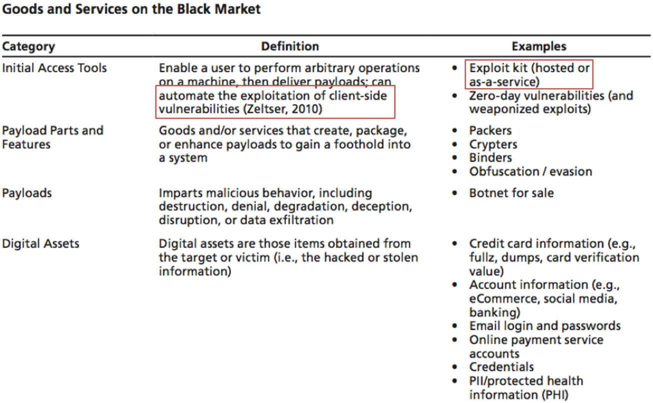
Today's organizational crown jewels are built of bytes. Back in 2003, physical security was most important to secure a company's most valuable information...Today, everything is on a network.

—Ablon et al (2014, p.34)

Increasingly hostile cyber-threat landscape, thanks to the emergence of dark-net marketplaces...

Motivation

...where criminals can buy hacking tools



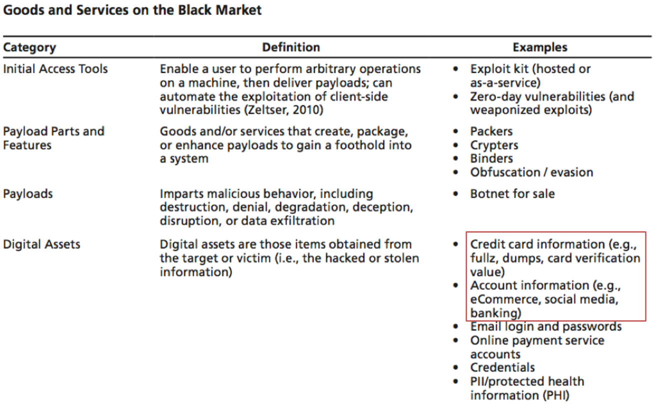
Goods and Services on the Black Market

Category	Definition	Examples
Initial Access Tools	Enable a user to perform arbitrary operations on a machine, then deliver payloads; can automate the exploitation of client-side vulnerabilities (Zeltser, 2010)	• Exploit kit (hosted or as-a-service) • Zero-day vulnerabilities (and weaponized exploits)
Payload Parts and Features	Goods and/or services that create, package, or enhance payloads to gain a foothold into a system	• Packers • Crypters • Binders • Obfuscation / evasion
Payloads	Imparts malicious behavior, including destruction, denial, degradation, deception, disruption, or data exfiltration	• Botnet for sale
Digital Assets	Digital assets are those items obtained from the target or victim (i.e., the hacked or stolen information)	• Credit card information (e.g., fullz, dumps, card verification value) • Account information (e.g., eCommerce, social media, banking) • Email login and passwords • Online payment service accounts • Credentials • PII/protected health information (PHI)

Source: Ablon et al., 2015

Motivation

...where criminals can buy hacking tools and sell stolen data.



Goods and Services on the Black Market

Category	Definition	Examples
Initial Access Tools	Enable a user to perform arbitrary operations on a machine, then deliver payloads; can automate the exploitation of client-side vulnerabilities (Zeltser, 2010)	• Exploit kit (hosted or as-a-service) • Zero-day vulnerabilities (and weaponized exploits)
Payload Parts and Features	Goods and/or services that create, package, or enhance payloads to gain a foothold into a system	• Packers • Crypters • Binders • Obfuscation / evasion
Payloads	Imparts malicious behavior, including destruction, denial, degradation, deception, disruption, or data exfiltration	• Botnet for sale
Digital Assets	Digital assets are those items obtained from the target or victim (i.e., the hacked or stolen information)	• Credit card information (e.g., fullz, dumps, card verification value) • Account information (e.g., eCommerce, social media, banking) • Email login and passwords • Online payment service accounts • Credentials • PII/protected health information (PHI)

Source: Ablon et al., 2015

Motivation

Despite that, firms are investing little (or not at all) in data security.

Motivation

Despite that, firms are investing little (or not at all) in data security.

Recent KPMG survey: 44% of CEOs do not plan to invest in cyber security in the next three years.

Motivation

Despite that, firms are investing little (or not at all) in data security.

Recent KPMG survey: 44% of CEOs do not plan to invest in cyber security in the next three years.

Weak investment incentives may be due to market failures.

Motivation

Despite that, firms are investing little (or not at all) in data security.

Recent KPMG survey: 44% of CEOs do not plan to invest in cyber security in the next three years.

Weak investment incentives may be due to market failures.

- **Imperfect information**: security level not observed by consumers.

Motivation

Despite that, firms are investing little (or not at all) in data security.

Recent KPMG survey: 44% of CEOs do not plan to invest in cyber security in the next three years.

Weak investment incentives may be due to market failures.

- **Imperfect information**: security level not observed by consumers.
- **Externalities**: losses to third-parties not internalized by firms.

Motivation

Imperfectly observed product quality: reputation concerns arising from lost future sales can incentivize firms to provide high quality goods.

Motivation

Imperfectly observed product quality: reputation concerns arising from lost future sales can incentivize firms to provide high quality goods.

Research questions:

Motivation

Imperfectly observed product quality: reputation concerns arising from lost future sales can incentivize firms to provide high quality goods.

Research questions:

- Can reputation concerns play a role in incentivizing security investment? If so, how big a role does it play?

Motivation

Imperfectly observed product quality: reputation concerns arising from lost future sales can incentivize firms to provide high quality goods.

Research questions:

- Can reputation concerns play a role in incentivizing security investment? If so, how big a role does it play?
- How can we further improve investment incentives?

Overview

Theoretical framework:

Overview

Theoretical framework:

- Focuses on the protection of consumer payment data.

Overview

Theoretical framework:

- Focuses on the protection of consumer payment data.
- Two periods.

Overview

Theoretical framework:

- Focuses on the protection of consumer payment data.
- Two periods.
- Three agents: website, consumer and consumer's bank.

Overview

Theoretical framework:

- Focuses on the protection of consumer payment data.
- Two periods.
- Three agents: website, consumer and consumer's bank.
- Key elements:

Overview

Theoretical framework:

- Focuses on the protection of consumer payment data.
- Two periods.
- Three agents: website, consumer and consumer's bank.
- Key elements:
  - **Externalities**: losses to consumer and bank not internalized by website

Overview

Theoretical framework:

- Focuses on the protection of consumer payment data.
- Two periods.
- Three agents: website, consumer and consumer's bank.
- Key elements:
  - **Externalities**: losses to consumer and bank not internalized by website
  - **Imperfect Information**: website's security level not observed by consumer

Overview

Theoretical framework:

- Focuses on the protection of consumer payment data.
- Two periods.
- Three agents: website, consumer and consumer's bank.
- Key elements:
  - **Externalities**: losses to consumer and bank not internalized by website
  - **Imperfect Information**: website's security level not observed by consumer
  - **Customer turnover**: data breaches signal poor security; consumer may leave upon learning that website was breached → Reputation mechanism

Overview

Main findings:

Overview

Main findings:

- Reputation can play a role in incentivizing security investment.

Overview

Main findings:

- Reputation can play a role in incentivizing security investment.
- Its effectiveness depends on the consumer's willingness and ability to punish a breached firm, which may be limited in practice.

Overview

Main findings:

- Reputation can play a role in incentivizing security investment.
- Its effectiveness depends on the consumer's willingness and ability to punish a breached firm, which may be limited in practice.
  - Difficulty in detecting breaches.

Overview

Main findings:

- Reputation can play a role in incentivizing security investment.
- Its effectiveness depends on the consumer's willingness and ability to punish a breached firm, which may be limited in practice.
  - Difficulty in detecting breaches.
  - Limited consumer losses due to bank's fraud prevention and liability protection policy.

Overview

Main findings:

- Reputation can play a role in incentivizing security investment.
- Its effectiveness depends on the consumer's willingness and ability to punish a breached firm, which may be limited in practice.
  - Difficulty in detecting breaches.
  - Limited consumer losses due to bank's fraud prevention and liability protection policy.
- Policies aimed at raising investment via the reputation mechanism can make the consumer worse off.

Presentation Outline

1. Model set-up

Presentation Outline

1. Model set-up

2. Equilibrium analysis: The reputation mechanism

Presentation Outline

1. Model set-up

2. Equilibrium analysis: The reputation mechanism

3. Reputation concerns in practice

Presentation Outline

1. Model set-up
2. Equilibrium analysis: The reputation mechanism
3. Reputation concerns in practice
4. Policy analysis: Improving investment incentives

Presentation Outline

1. Model set-up
2. Equilibrium analysis: The reputation mechanism
3. Reputation concerns in practice
4. Policy analysis: Improving investment incentives
5. Related literature

Presentation Outline

1. Model set-up
2. Equilibrium analysis: The reputation mechanism
3. Reputation concerns in practice
4. Policy analysis: Improving investment incentives
5. Related literature
6. Conclusion

Theoretical Framework

Two periods: $t \in \{1, 2\}$.

Theoretical Framework

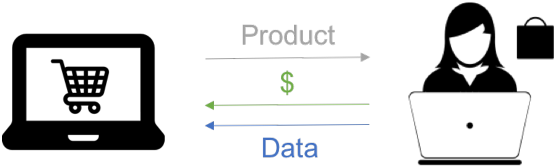
Two periods: $t \in \{1, 2\}$.

Two strategic players: a website and a consumer

Theoretical Framework

Two periods: $t \in \{1, 2\}$.

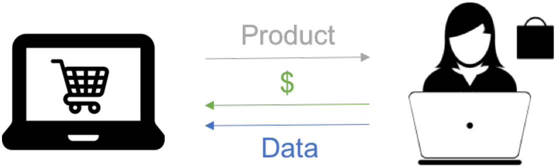
Two strategic players: a website and a consumer.



Theoretical Framework

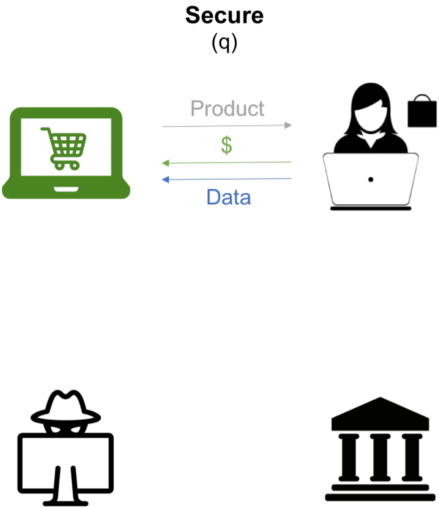
Two periods: $t \in \{1, 2\}$.

Two strategic players: a website and a consumer.



Website makes a one-time investment, $c(q)$, to protect consumer data at the start.

Theoretical Framework



Secure

(q)

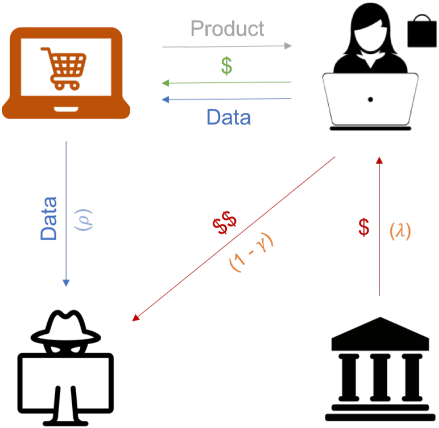
Product

$

Data

Theoretical Framework

Vulnerable
(1 - q)



Information

What do the players know?

Amount invested	Yes.	No, but has rational beliefs over *q* (website's reputation).
State of security	No.	No.
Data breaches	Yes.	With probability $\lambda\ (1 - \gamma)$.

Information

Website has initial reputation q_0.

Information

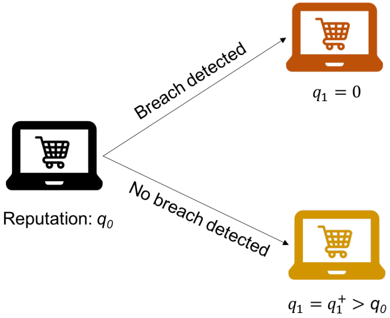
Website has initial reputation q_0.

Consumer learns about q via discovery of fraud losses and updates her beliefs using Bayes rule.

Information

Website has initial reputation q_0.

Consumer learns about q via discovery of fraud losses and updates her beliefs using Bayes rule.



Payoffs

At every period, when the consumer buys from a *secure* website

Sales revenue: *r*

Gross utility: *v*
Expected losses: 0

Financial gains: 0

Expected liability: 0

Payoffs

At every period, when the consumer buys from a *vulnerable* website

Sales revenue: r

Gross utility: v
Fraud losses:
$-\rho(1-\gamma)(1-\lambda\alpha)l$

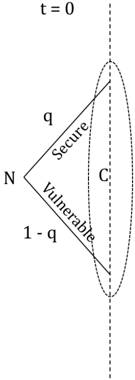
Financial gains:
$\rho(1-\gamma)l$

Fraud liability:
$-\rho(1-\gamma)\lambda\alpha l$

α: Fraud liability protection offered by the bank.

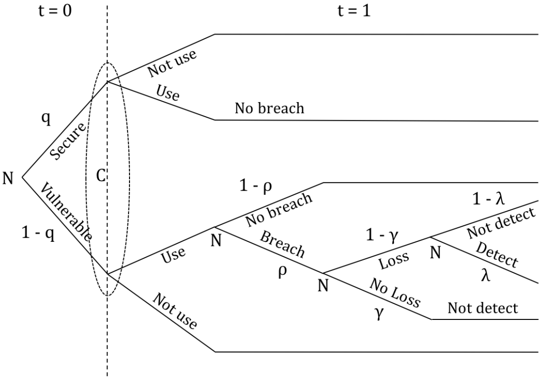
Timing

$t = 0$: Website invests $c(q)$ in security. With probability q, it is secure against cyber-attacks.



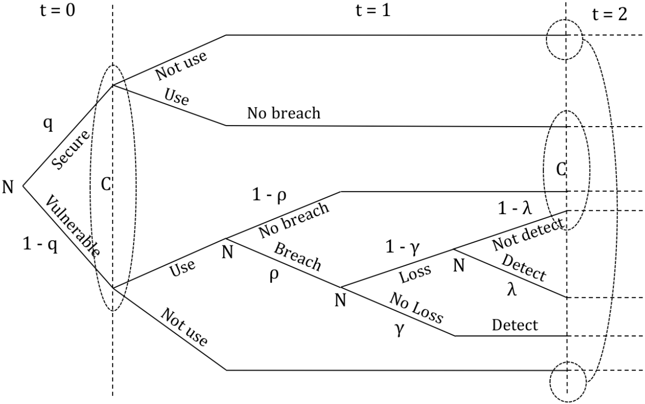
Timing

$t = 1$: Consumer makes purchase decision given website's initial reputation. If website is vulnerable, breach may occur and be detected. Beliefs are updated.



Timing

$t = 2$: Consumer makes purchase decision given website's updated reputation...



Consumer's Strategy

At every t, consumer has to decide whether to buy from the website.

Consumer's Strategy

At every t, consumer has to decide whether to buy from the website.

Expected within-period utility from purchasing is

$$E(U(q_{t-1})) = v - \underbrace{(1 - q_{t-1})\rho(1-\gamma)(1-\lambda\alpha)I}_{\text{Expected fraud losses from breach}}.$$

Consumer's Strategy

At every t, consumer has to decide whether to buy from the website.

Expected within-period utility from purchasing is

$$E(U(q_{t-1})) = v - (1 - q_{t-1}) \underbrace{\rho(1-\gamma)}_{\substack{\text{Prob of} \\ \text{exp. fraud}}} \underbrace{(1-\lambda\alpha)l}_{\substack{\text{(Net) fraud} \\ \text{losses}}} .$$

Consumer's Strategy

At every t, consumer has to decide whether to buy from the website.

Expected within-period utility from purchasing is

$$E(U(q_{t-1})) = v - (1 - q_{t-1}) \underbrace{\rho(1-\gamma)}_{\substack{\text{Prob of} \\ \text{exp. fraud}}} \underbrace{(1-\lambda\alpha)l}_{\substack{\text{(Net) fraud} \\ \text{losses}}}.$$

Her decision depends on:

Consumer's Strategy

At every t, consumer has to decide whether to buy from the website.

Expected within-period utility from purchasing is

$$E(U(q_{t-1})) = v - (1 - q_{t-1}) \underbrace{\rho(1-\gamma)}_{\substack{\text{Prob of} \\ \text{exp. fraud}}} \underbrace{(1-\lambda\alpha)l}_{\substack{\text{(Net) fraud} \\ \text{losses}}}.$$

Her decision depends on:

1. Her valuation for the product v

Consumer's Strategy

At every t, consumer has to decide whether to buy from the website.

Expected within-period utility from purchasing is

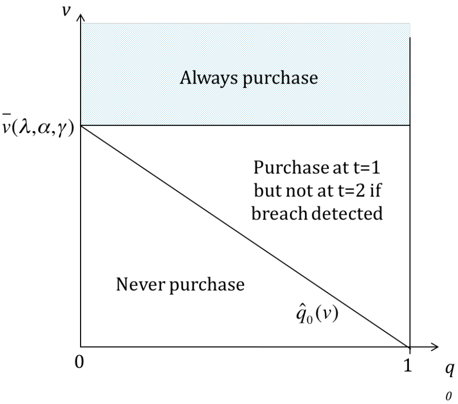
$$E(U(q_{t-1})) = v - (1 - q_{t-1}) \underbrace{\rho(1-\gamma)}_{\substack{\text{Prob of} \\ \text{exp. fraud}}} \underbrace{(1-\lambda\alpha) l}_{\substack{\text{(Net) fraud} \\ \text{losses}}}.$$

Her decision depends on:

1. Her valuation for the product v
2. Her expected fraud losses → depends on website's reputation $q_{t-1}(q_0)$

Consumer's Strategy

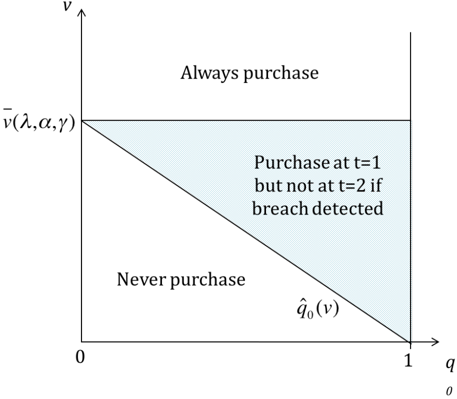
1) Consumer always buys from website regardless of its reputation.



$\overline{v}(\lambda, \alpha, \gamma)$: Max. expected losses
$\hat{q}_0(v)$: Min. initial reputation such that $E(U_1) \geq 0$.

Consumer's Strategy

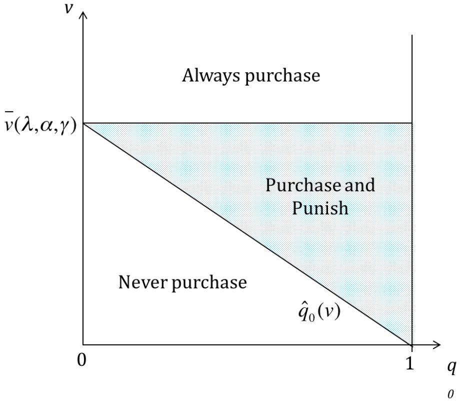
2) Consumer buys given website's initial reputation, but not after learning that it is vulnerable.



$\overline{v}(\lambda, \alpha, \gamma)$: Max. expected losses
$\hat{q}_0(v)$: Min. initial reputation such that $E(U_1) \geq 0$.

Consumer's Strategy

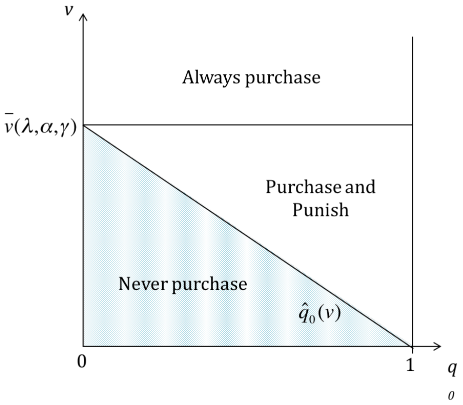
2) Consumer buys given website's initial reputation, but not after learning that it is vulnerable.



$\overline{v}(\lambda, \alpha, \gamma)$: Max. expected losses
$\hat{q}_0(v)$: Min. initial reputation such that $E(U_1) \geq 0$.

Consumer's Strategy

3) Consumer never buys from website.



$\overline{v}(\lambda, \alpha, \gamma)$: Max. expected losses
$\hat{q}_0(v)$: Min. initial reputation such that $E(U_1) \geq 0$.

Consumer's Strategy

Reputation and Purchase Decision

A firm's reputation for security matters *less* when the consumer values the product *more*.

Consumer's Strategy

Reputation and Purchase Decision

A firm's reputation for security matters *less* when the consumer values the product *more*.

Implications:

- Reputation is likely to be *less* important when

Consumer's Strategy

Reputation and Purchase Decision

A firm's reputation for security matters *less* when the consumer values the product *more*.

Implications:

- Reputation is likely to be *less* important when
  - there are no close/good substitutes for the product.

Consumer's Strategy

Reputation and Purchase Decision

A firm's reputation for security matters *less* when the consumer values the product *more*.

Implications:

- Reputation is likely to be *less* important when
  - there are no close/good substitutes for the product.

Website's Strategy

Website has to decide how much to invest at the start given q_0:

$$\max_{q} \pi(q; q_0, \lambda, \alpha) \equiv \underbrace{R_1(q_0, \lambda, \alpha)}_{\substack{\text{Revenue} \\ \text{at } t=1}} + \delta \underbrace{R_2(q; q_0, \lambda, \alpha)}_{\substack{\text{Expected revenue} \\ \text{at } t=2}} - c(q)$$

- δ: discount factor of the firm.

Website's Strategy

Website has to decide how much to invest at the start given q_0:

$$\max_q \pi(q; q_0, \lambda, \alpha) \equiv \underbrace{R_1(q_0, \lambda, \alpha)}_{\substack{\text{Revenue} \\ \text{at } t=1}} + \delta \underbrace{R_2(q; q_0, \lambda, \alpha)}_{\substack{\text{Expected revenue} \\ \text{at } t=2}} - c(q)$$

- δ: discount factor of the firm.

Invests a positive amount only when consumer is *willing* and *able* to punish it for breaches.

Website's Strategy

Website has to decide how much to invest at the start given q_0:

$$\max_q \pi(q; q_0, \lambda, \alpha) \equiv \underbrace{R_1(q_0, \lambda, \alpha)}_{\substack{\text{Revenue}\\ \text{at } t=1}} + \delta \underbrace{R_2(q; q_0, \lambda, \alpha)}_{\substack{\text{Expected revenue}\\ \text{at } t=2}} - c(q)$$

- δ: discount factor of the firm.

Invests a positive amount only when consumer is *willing* and *able* to punish it for breaches.

- Willing when expected fraud losses exceeds her valuation ($v < \overline{v}$).

Website's Strategy

Website has to decide how much to invest at the start given q_0:

$$\max_q \pi(q; q_0, \lambda, \alpha) \equiv \underbrace{R_1(q_0, \lambda, \alpha)}_{\substack{\text{Revenue} \\ \text{at } t=1}} + \delta \underbrace{R_2(q; q_0, \lambda, \alpha)}_{\substack{\text{Expected revenue} \\ \text{at } t=2}} - c(q)$$

- δ: discount factor of the firm.

Invests a positive amount only when consumer is *willing* and *able* to punish it for breaches.

- Willing when expected fraud losses exceeds her valuation ($v < \overline{v}$).
- Able when she learns about the breach.

Website's Strategy

Website has to decide how much to invest at the start given q_0:

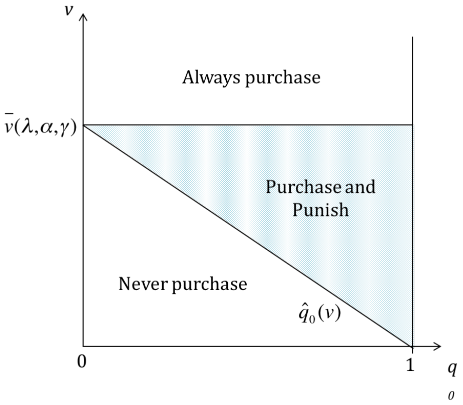
$$\max_q \pi(q; q_0, \lambda, \alpha) \equiv \underbrace{R_1(q_0, \lambda, \alpha)}_{\substack{\text{Revenue} \\ \text{at } t=1}} + \delta \underbrace{R_2(q; q_0, \lambda, \alpha)}_{\substack{\text{Expected revenue} \\ \text{at } t=2}} - c(q)$$

- δ: discount factor of the firm.

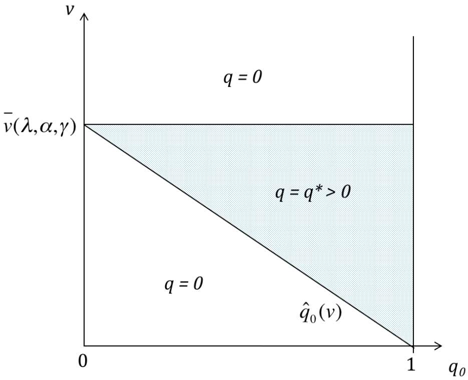
Invests a positive amount only when consumer is *willing* and *able* to punish it for breaches.

- Willing when expected fraud losses exceeds her valuation ($v < \overline{v}$).
- Able when she learns about the breach.

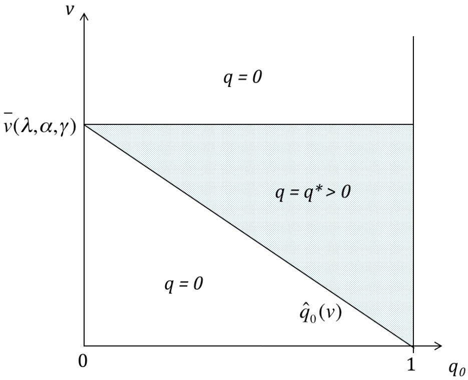
Website's Strategy



Website's Strategy



Website's Strategy



Optimal security level q^* is increasing in consumer's ability to punish.

Website's Strategy

Website's Investment Strategy

1. Website only invests when it expects to be punished by the consumer.

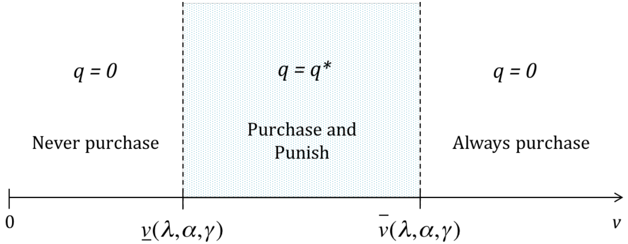
Website's Strategy

Website's Investment Strategy

1. Website only invests when it expects to be punished by the consumer.
2. It invests more when the consumer is more likely to learn of breaches.

Reputation Mechanism

Bayes-Nash Equilibrium (with Rational Expectations).



Reputation Mechanism

The Role of Reputation

1. Reputation plays a role when the consumer is *willing* to purchase and to punish the firm (v is neither too high nor too low).

Reputation Mechanism

The Role of Reputation

1. Reputation plays a role when the consumer is *willing* to purchase and to punish the firm (v is neither too high nor too low).

2. Its role is bigger when the consumer is more *able* to punish the firm.

Reputation Concerns in Practice

How much does reputation matters in reality?

Reputation Concerns in Practice

How much does reputation matters in reality?

Not too much: consumers seem to lack the willingness and/or ability to punish breached firms.

Reputation Concerns in Practice

How much does reputation matters in reality?

Not too much: consumers seem to lack the willingness and/or ability to punish breached firms.

- Only 11% of surveyed consumers terminated business relationship with the affected firm (Ablon et al, 2015).

Weak Reputation Effect

1. **Low probability of breach detection** (small λ)
   - Only 10% of breaches are discovered by consumers noticing suspicious activities (Ablon et al, 2015)

Weak Reputation Effect

1. **Low probability of breach detection** (small λ)
   - Only 10% of breaches are discovered by consumers noticing suspicious activities (Ablon et al, 2015)
   - Why breach detection may be difficult:

Weak Reputation Effect

1. **Low probability of breach detection** (small λ)
   - Only 10% of breaches are discovered by consumers noticing suspicious activities (Ablon et al, 2015)
   - Why breach detection may be difficult:
     - Confusing merchant descriptors (e.g., Burger King = "JEFFREY GIANGRANDE CORP"?)

Weak Reputation Effect

1. **Low probability of breach detection** (small λ)
   - Only 10% of breaches are discovered by consumers noticing suspicious activities (Ablon et al, 2015)
   - Why breach detection may be difficult:
     - Confusing merchant descriptors (e.g., Burger King = "JEFFREY GIANGRANDE CORP"?)
     - Micro charges (e.g., the $9.84 scam)

Weak Reputation Effect

1. **Low probability of breach detection** (small λ)
   - Only 10% of breaches are discovered by consumers noticing suspicious activities (Ablon et al, 2015)
   - Why breach detection may be difficult:
     - Confusing merchant descriptors (e.g., Burger King = "JEFFREY GIANGRANDE CORP"?)
     - Micro charges (e.g., the $9.84 scam)
   - Low *ability* to punish the firm → Firm invests little in security

Weak Reputation Effect

2. **Strong protection against fraud liability** (large α)

Weak Reputation Effect

2. **Strong protection against fraud liability** (large α)
   - Banks typically absorb a large share of fraud losses.

Weak Reputation Effect

2. **Strong protection against fraud liability** (large α)
   - Banks typically absorb a large share of fraud losses.

	Consumer's Maximum Loss
Credit	\$50.
Debit	\$50 if reported within 2 days. \$500 if reported between 2 - 60 days. Unlimited thereafter.

Table: Consumer's liability under the FCBA and EFTA in the U.S.

Weak Reputation Effect

2. **Strong protection against fraud liability** (large α)

   - Banks typically absorb a large share of fraud losses.

	Consumer's Maximum Loss
Credit	\$50.
Debit	\$50 if reported within 2 days. \$500 if reported between 2 - 60 days. Unlimited thereafter.

Table: Consumer's liability under the FCBA and EFTA in the U.S.

   - Many major card networks (e.g., Visa, Mastercard, Amex) even offer a zero-liability policy.

Weak Reputation Effect

Consumer has low *willingness* to punish the firm ...

Weak Reputation Effect

Consumer has low *willingness* to punish the firm ...

"Credit card fraud losses totaled $8 billion last year, but **many consumers may see it as a victimless crime**. *Certainly there is a high hassle factor... but* **consumers are generally not held responsible for the fraudulent charges** *that occur... there is* **no evidence that they shifted their spending patterns** *to use cash rather than plastic."*

- The New York Times, Sept. 28, 2015

Weak Reputation Effect

Consumer has low *willingness* to punish the firm ...

"Credit card fraud losses totaled $8 billion last year, but **many consumers may see it as a victimless crime***. Certainly there is a high hassle factor... but* **consumers are generally not held responsible for the fraudulent charges** *that occur... there is* **no evidence that they shifted their spending patterns** *to use cash rather than plastic."*

- The New York Times, Sept. 28, 2015

→ Firm has little incentives to invest.

Weak Reputation Effect

3. **Better fraud prevention ability**

Weak Reputation Effect

3. **Better fraud prevention ability**
    - Better fraud prevention technology lowers success rate of fraud.

Weak Reputation Effect

3. **Better fraud prevention ability**
   - Better fraud prevention technology lowers success rate of fraud.
   - Example: Bank of America
     - Chip-and-PIN technology
     - Multi-factor authentication: Verified by Visa and MasterCard SecureCode
     - Photosecurity

Weak Reputation Effect

3. **Better fraud prevention ability**
   - Better fraud prevention technology lowers success rate of fraud.
   - Example: Bank of America
     - Chip-and-PIN technology
     - Multi-factor authentication: Verified by Visa and MasterCard SecureCode
     - Photosecurity
   - Lower expected losses → consumer less willing to punish

Weak Reputation Effect

3. Better fraud prevention ability

- Better fraud prevention technology lowers success rate of fraud.
- Example: Bank of America
  - Chip-and-PIN technology
  - Multi-factor authentication: Verified by Visa and MasterCard SecureCode
  - Photosecurity
- Lower expected losses → consumer less willing to punish
- Lower rate of breach detection → consumer less able to punish

→ Firm has little incentives to invest.

Weak Reputation Effect

Limited Role of Reputation in Reality

The consumer's *willingness* and *ability* to punish a breached firm in reality limited by:

- a low rate of breach detection
- a high level of liability protection
- a high ability of fraud prevention.

Weak Reputation Effect

Limited Role of Reputation in Reality

The consumer's *willingness* and *ability* to punish a breached firm in reality limited by:

- a low rate of breach detection
- a high level of liability protection
- a high ability of fraud prevention.

Implication:

- Reputation concerns may not provide firms with sufficient investment incentives.

Improving Investment Incentives

Improving Investment Incentives

1. **"Indirect" Interventions**

Improving Investment Incentives

1. **"Indirect" Interventions**

   - Strengthening the reputation mechanism by raising the consumer's

Improving Investment Incentives

1. **"Indirect" Interventions**

- Strengthening the reputation mechanism by raising the consumer's
  - *Willingness* to punish: Expulsion of breached merchants from card network

Improving Investment Incentives

1. **"Indirect" Interventions**

- Strengthening the reputation mechanism by raising the consumer's
    - *Willingness* to punish: Expulsion of breached merchants from card network
    - *Ability* to punish: Active fraud monitoring by bank, mandatory breach notification

Improving Investment Incentives

1. **"Indirect" Interventions**

   - Strengthening the reputation mechanism by raising the consumer's
     - *Willingness* to punish: Expulsion of breached merchants from card network
     - *Ability* to punish: Active fraud monitoring by bank, mandatory breach notification

2. **"Direct" Interventions**

Improving Investment Incentives

1. **“Indirect” Interventions**
    - Strengthening the reputation mechanism by raising the consumer’s
        - *Willingness* to punish: Expulsion of breached merchants from card network
        - *Ability* to punish: Active fraud monitoring by bank, mandatory breach notification
2. **“Direct” Interventions**
    - Improving consumer information: Certification of investment level or state of security

Improving Investment Incentives

1. **"Indirect" Interventions**
   - Strengthening the reputation mechanism by raising the consumer's
     - *Willingness* to punish: Expulsion of breached merchants from card network
     - *Ability* to punish: Active fraud monitoring by bank, mandatory breach notification

2. **"Direct" Interventions**
   - Improving consumer information: Certification of investment level or state of security
   - Increasing the direct cost of data breaches: Liability rule

Expulsion from Card Network

In the US, a breached merchant that is not compliant with the PCI's DSS may be suspended or expelled from the network.

Expulsion from Card Network

In the US, a breached merchant that is not compliant with the PCI's DSS may be suspended or expelled from the network.

Suppose that the bank can expel the website following a breach.

Expulsion from Card Network

In the US, a breached merchant that is not compliant with the PCI's DSS may be suspended or expelled from the network.

Suppose that the bank can expel the website following a breach.

Let τ denote the resulting inconvenience cost to the consumer.

Expulsion from Card Network

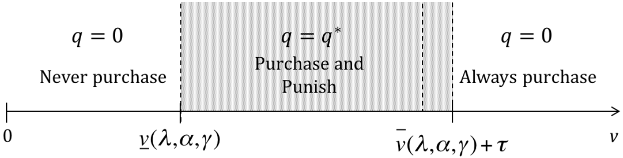
In the US, a breached merchant that is not compliant with the PCI's DSS may be suspended or expelled from the network.

Suppose that the bank can expel the website following a breach.

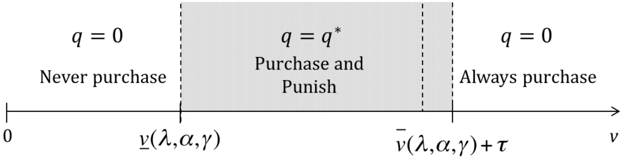
Let τ denote the resulting inconvenience cost to the consumer.

The policy raises the consumer's willingness to punish, but does not affect her ability.

Expulsion from Card Network

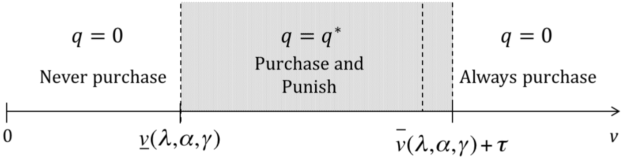

$q = 0$
Never purchase
$q = q^*$
Purchase and Punish
$q = 0$
Always purchase
0
$\underline{v}(\lambda, \alpha, \gamma)$
$\bar{v}(\lambda, \alpha, \gamma) + \tau$
v

Expulsion from Card Network


$q = 0$
Never purchase
$q = q^*$
Purchase and Punish
$q = 0$
Always purchase
0
$\underline{v}(\lambda,\alpha,\gamma)$
$\bar{v}(\lambda,\alpha,\gamma)+\tau$
v

Website's investment level is (weakly) higher.

Expulsion from Card Network



$q = 0$
Never purchase
$q = q^*$
Purchase and Punish
$q = 0$
Always purchase
0
$\underline{v}(\lambda,\alpha,\gamma)$
$\bar{v}(\lambda,\alpha,\gamma)+\tau$
v

Website's investment level is (weakly) higher.

Consumer surplus is *higher* when her valuation is *sufficiently small* ($v < \hat{v} \in (\overline{v}, \overline{v} + \tau]$) and is lower otherwise.

Active Monitoring by Bank

Bank can prevent fraud by

Active Monitoring by Bank

Bank can prevent fraud by

- Passive deterrence: making it harder to commit fraud with stolen data (e.g., chip-and-PIN card)

Active Monitoring by Bank

Bank can prevent fraud by

- Passive deterrence: making it harder to commit fraud with stolen data (e.g., chip-and-PIN card)
    - Neither consumer nor bank learns of breach.

Active Monitoring by Bank

Bank can prevent fraud by

- Passive deterrence: making it harder to commit fraud with stolen data (e.g., chip-and-PIN card)
  - Neither consumer nor bank learns of breach.
- Active detection: monitoring transactions for suspicious activities (e.g., data analytics)

Active Monitoring by Bank

Bank can prevent fraud by

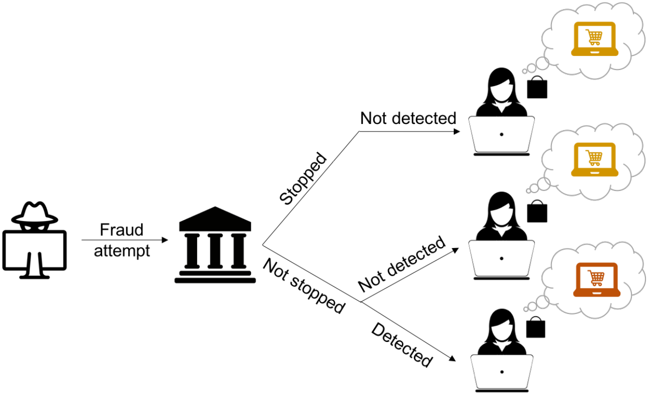
- Passive deterrence: making it harder to commit fraud with stolen data (e.g., chip-and-PIN card)
  - Neither consumer nor bank learns of breach.
- Active detection: monitoring transactions for suspicious activities (e.g., data analytics)
  - Bank learns of breach and can inform consumer.

Active Monitoring by Bank

Consumer is better able to punish website under active detection.

Active Monitoring by Bank

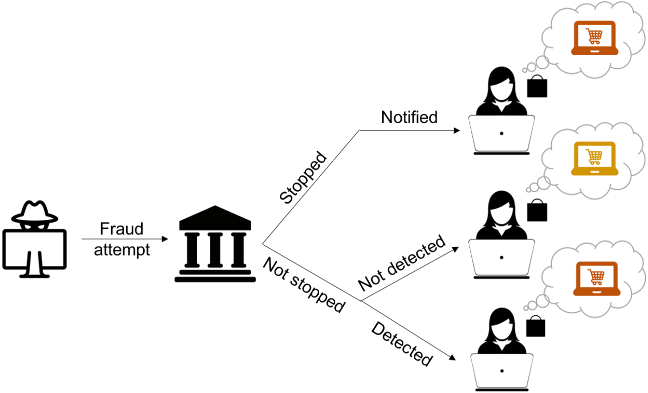
Consumer is better able to punish website under active detection.



Passive Deterrence

Active Monitoring by Bank

Consumer is better able to punish website under active detection.



Active Detection

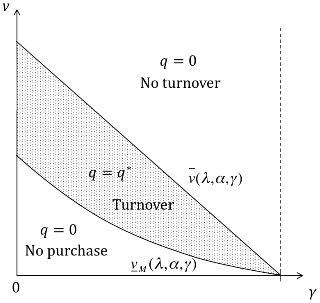
Active Monitoring by Bank

Suppose active detection and passive deterrence are equally effective.

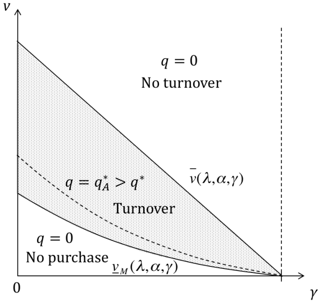
Active Monitoring by Bank

Suppose active detection and passive deterrence are equally effective.

- Website invests (weakly) more under active detection.


v
$q = 0$
No turnover
$q = q^*$
Turnover
$\bar{v}(\lambda,\alpha,\gamma)$
$q = 0$
No purchase
$\underline{v}_M(\lambda,\alpha,\gamma)$
0
γ

Passive deterrence

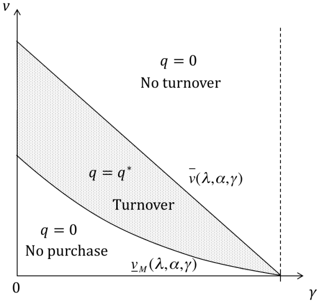


Active detection

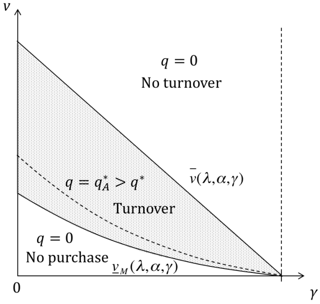
Active Monitoring by Bank

Suppose active detection and passive deterrence are equally effective.

- Website invests (weakly) more under active detection.


v
$q = 0$
No turnover
$q = q^*$
Turnover
$\bar{v}(\lambda,\alpha,\gamma)$
$q = 0$
No purchase
$\underline{v}_M(\lambda,\alpha,\gamma)$
0
γ

Passive deterrence



Active detection

- Consumer surplus is always *higher*.

Mandatory Breach Notification

Breach Notification Laws

Mandatory Breach Notification

Breach Notification Laws

- General Data Protection Regulation (GDPR) in the EU
  - Notification must be provided *no later than 72 hours* after data controller becomes aware of the breach, whenever it is likely to "result in a risk for the rights and freedoms of individuals".

Mandatory Breach Notification

Breach Notification Laws

- General Data Protection Regulation (GDPR) in the EU
  - Notification must be provided *no later than 72 hours* after data controller becomes aware of the breach, whenever it is likely to "result in a risk for the rights and freedoms of individuals".
- Data Security and Breach Notification Act in the US
  - Notification must be provided in a timely fashion, unless there is no reasonable risk that the breach has or will result in harm for its victims.

Mandatory Breach Notification

Breach Notification Laws

- General Data Protection Regulation (GDPR) in the EU
  - Notification must be provided *no later than 72 hours* after data controller becomes aware of the breach, whenever it is likely to "result in a risk for the rights and freedoms of individuals".
- Data Security and Breach Notification Act in the US
  - Notification must be provided in a timely fashion, unless there is no reasonable risk that the breach has or will result in harm for its victims.
- Failure to comply with regulations will result in high fines or penalties.

Mandatory Breach Notification

Website to notify to consumer whenever breaches occur → raises detection rate from λ to 1.

Mandatory Breach Notification

Website to notify to consumer whenever breaches occur → raises detection rate from λ to 1.

Two cited benefits

Mandatory Breach Notification

Website to notify to consumer whenever breaches occur → raises detection rate from λ to 1.

Two cited benefits

1. **Higher investment**: Improves consumer's ability to punish the firm → Higher expected cost of turnover.

Mandatory Breach Notification

Website to notify to consumer whenever breaches occur → raises detection rate from λ to 1.

Two cited benefits

1. **Higher investment**: Improves consumer's ability to punish the firm → Higher expected cost of turnover.
2. **Loss mitigation**: Allows consumer to take actions to reduce her losses.

Mandatory Breach Notification

Website to notify to consumer whenever breaches occur → raises detection rate from λ to 1.

Two cited benefits

1. **Higher investment**: Improves consumer's ability to punish the firm → Higher expected cost of turnover.
2. **Loss mitigation**: Allows consumer to take actions to reduce her losses.

But loss mitigation may adversely affect investment incentives

Mandatory Breach Notification

Website to notify to consumer whenever breaches occur → raises detection rate from λ to 1.

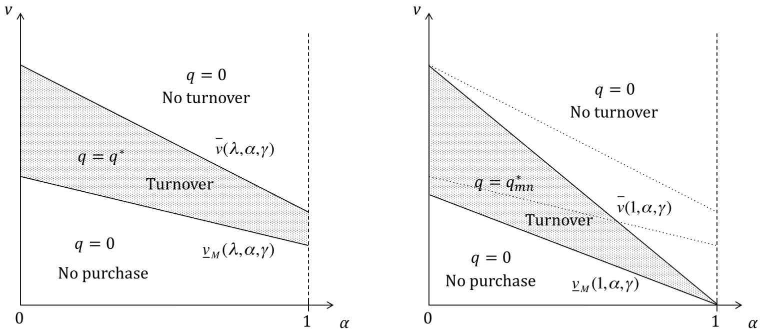
Two cited benefits

1. **Higher investment**: Improves consumer's ability to punish the firm → Higher expected cost of turnover.
2. **Loss mitigation**: Allows consumer to take actions to reduce her losses.

But loss mitigation may adversely affect investment incentives

- Lower expected losses from breaches → Less willing to punish the firm.

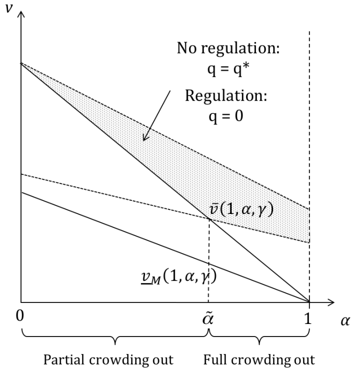
Mandatory Breach Notification



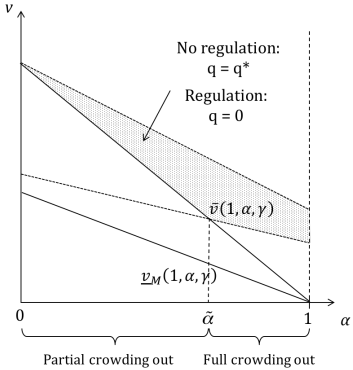
No regulation

Mandatory notification

Mandatory Breach Notification

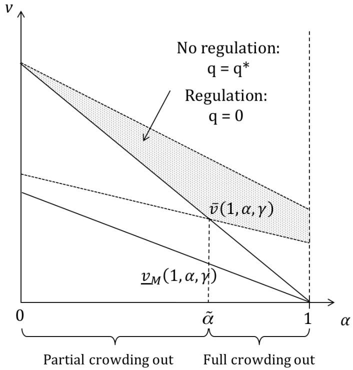


Mandatory Breach Notification



When consumer is initially willing to punish, notification may result in crowding out.

Mandatory Breach Notification



When consumer is initially willing to punish, notification may result in crowding out.

- Larger crowding out effect when α is higher.

Mandatory Breach Notification

The website invests less in the region of crowding out and (weakly) more otherwise.

Mandatory Breach Notification

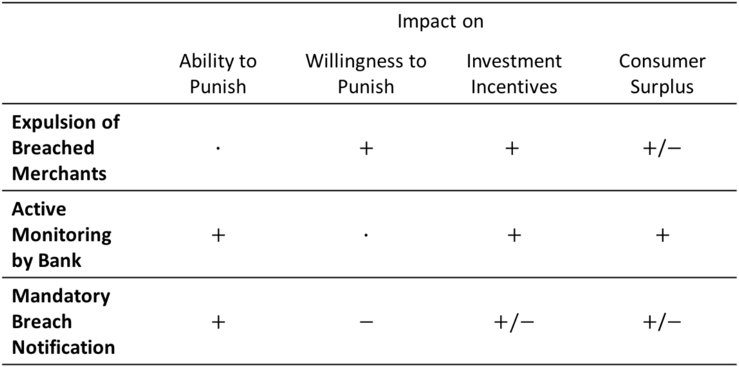
The website invests less in the region of crowding out and (weakly) more otherwise.

Consumer surplus is *higher* under breach notification if

- the website invests more;
- the website invests less but the loss mitigation benefit is sufficiently big (α is high enough).

Consumer surplus is lower otherwise.

Summary



	Impact on			
	Ability to Punish	Willingness to Punish	Investment Incentives	Consumer Surplus
Expulsion of Breached Merchants	·	+	+	+/−
Active Monitoring by Bank	+	·	+	+
Mandatory Breach Notification	+	−	+/−	+/−

Summary

Policy Implications - Indirect Interventions

- Raising the consumer's *ability* to punish always lead to *higher investment* and *higher consumer surplus*.

Summary

Policy Implications - Indirect Interventions

- Raising the consumer's *ability* to punish always lead to *higher investment* and *higher consumer surplus*.
- Raising the consumer's *willingness* to punish lead to *higher investment* but can *reduce consumer surplus* when consumer's valuation is very high.

Summary

Policy Implications - Indirect Interventions

- Raising the consumer's *ability* to punish always lead to *higher investment* and *higher consumer surplus*.
- Raising the consumer's *willingness* to punish lead to *higher investment* but can *reduce consumer surplus* when consumer's valuation is very high.
- Ex-post protection of consumers against losses reduces ex-ante investment incentives of firms.

Improving Consumer Information

Consumer information can be improved by obliging website to reveal

Improving Consumer Information

Consumer information can be improved by obliging website to reveal

- its state of security: *secure* or *vulnerable*;

Improving Consumer Information

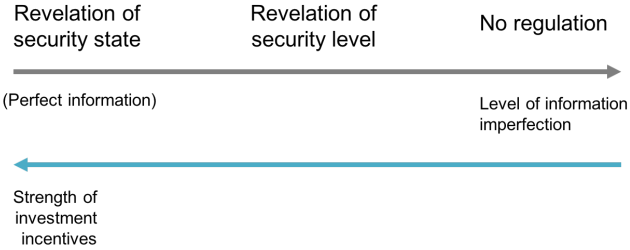
Consumer information can be improved by obliging website to reveal

- its state of security: *secure* or *vulnerable*;
- its level of security: q

Improving Consumer Information

Consumer information can be improved by obliging website to reveal

- its state of security: *secure* or *vulnerable*;
- its level of security: q


Revelation of security state
Revelation of security level
No regulation
(Perfect information)
Level of information imperfection
Strength of investment incentives

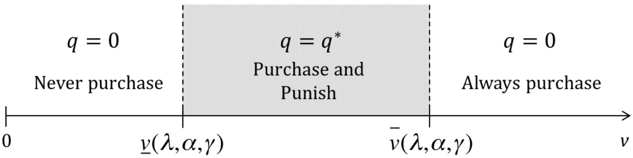
Improving Consumer Information

Comparison Across Regimes

Improving Consumer Information

Comparison Across Regimes

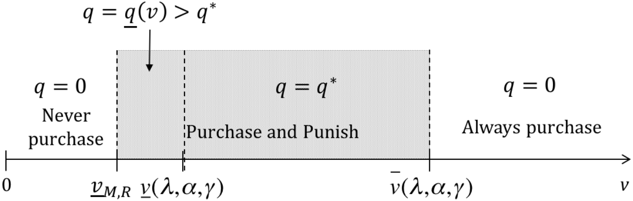
1. No regulation:



Improving Consumer Information

Comparison Across Regimes

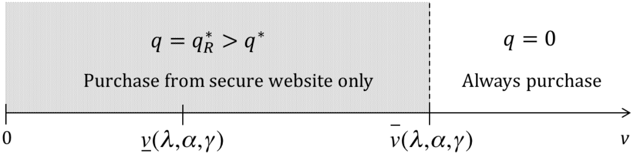
2. Revelation of security level:


$q = \underline{q}(v) > q^*$
$q = 0$
Never purchase
$q = q^*$
Purchase and Punish
$q = 0$
Always purchase
0
$\underline{v}_{M,R}$
$\underline{v}(\lambda,\alpha,\gamma)$
$\bar{v}(\lambda,\alpha,\gamma)$
v

Improving Consumer Information

Comparison Across Regimes

3. Revelation of security state:


$q = q_R^* > q^*$
Purchase from secure website only
$q = 0$
Always purchase
0
$\underline{v}(\lambda,\alpha,\gamma)$
$\bar{v}(\lambda,\alpha,\gamma)$
v

Increasing the Direct Costs of Breaches

Consider a liability rule that makes the website liable for a share of the fraud losses incurred by bank.

Increasing the Direct Costs of Breaches

Consider a liability rule that makes the website liable for a share of the fraud losses incurred by bank.

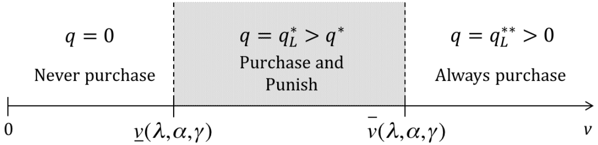
- Website incurs a cost whenever fraud losses arising from breaches are detected (even when there is no turnover).

Increasing the Direct Costs of Breaches

Consider a liability rule that makes the website liable for a share of the fraud losses incurred by bank.

- Website incurs a cost whenever fraud losses arising from breaches are detected (even when there is no turnover).

The website invests (weakly) more under the liability regime.

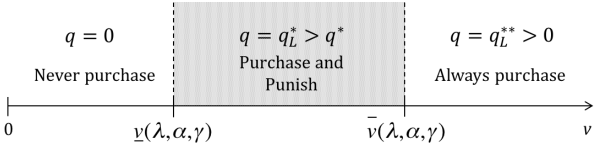


Increasing the Direct Costs of Breaches

Consider a liability rule that makes the website liable for a share of the fraud losses incurred by bank.

- Website incurs a cost whenever fraud losses arising from breaches are detected (even when there is no turnover).

The website invests (weakly) more under the liability regime.



$q = 0$

Never purchase

$q = q_L^* > q^*$

Purchase and Punish

$q = q_L^{**} > 0$

Always purchase

0
$\underline{v}(\lambda,\alpha,\gamma)$
$\bar{v}(\lambda,\alpha,\gamma)$
v

Consumer surplus is (weakly) higher.

Related Literature

Economics of Info Security:
- Probabilistic model of security investment: Gordon and Loeb (2002)
- Public good games: Varian (2004), Grossklags et al. (2008)
- Contagion: Acemoglu et al. (2016), Kunreuther and Heal (2003)
- Composite security model: Riordan (2014)

Reputation and Product Quality:
Board and Meyer-ter Vehn (2013), Allen (1984), Dybvig and Spatt (1983), Rogerson (1983), Shapiro (1982), Shapiro (1983), Klein and Leffler (1981), Smallwood and Conlisk (1979)

Related Literature

Product Safety:
See Daughety and Reinganum (2011) for an overview.

Data Breaches:
- Consumer reactions: Kwon and Johnson (2015), Mikhed and Vogan (2015, 2017), Ablon et al. (2016), Greene and Stavins (2017)
- Stock prices: Campbell et al. (2003), Cavusoglu et al. (2004), Acquisti and Grossklags (2005)
- Breach notification: Romanosky et al. (2010)

Conclusion

Reputation concerns may provide incentives for a firm to invest in security...

Conclusion

Reputation concerns may provide incentives for a firm to invest in security...

but their impact may be limited by *low breach detection rate*, *high liability protection* and *strong fraud prevention ability*.

Conclusion

Reputation concerns may provide incentives for a firm to invest in security...

but their impact may be limited by *low breach detection rate*, *high liability protection* and *strong fraud prevention ability*.

Incentives can be improved indirectly by *raising the reputation cost* or directly by *reducing the information imperfection and externalities*.

Conclusion

Reputation concerns may provide incentives for a firm to invest in security...

but their impact may be limited by *low breach detection rate*, *high liability protection* and *strong fraud prevention ability*.

Incentives can be improved indirectly by *raising the reputation cost* or directly by *reducing the information imperfection and externalities*.

Attention should be paid to how indirect measures affect the consumer's willingness to punish → may lower her surplus.

Thank you.

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