The Economic Costs of Cyber Risk

Aniket Baksy aniket.baksy@unimelb.edu.au

Daniele Caratelli danicaratelli@gmail.com

University of Queensland, November 2026

Cyber Risk Today



- Cybersecurity has gone from being a narrow IT concern to a widespread threat
- Attacks inflict massive direct losses, but also imply wider disruptions, eg via supply chains
- Unsurprisingly, a major concern for policymakers!
  - Data-intensive sectors particularly prone to attacks (finance, insurance, . . .)

  $\Longrightarrow$ concerns from policymakers, particularly CBs & financial regulators
  - concerns amplified with rise of the modern "AI" economy

Cyber Risk Today



- Cybersecurity has gone from being a narrow IT concern to a widespread threat
- Attacks inflict massive direct losses, but also imply wider disruptions, eg via supply chains
- Unsurprisingly, a major concern for policymakers!
  - Data-intensive sectors particularly prone to attacks (finance, insurance, ...)

  $\Longrightarrow$ concerns from policymakers, particularly CBs & financial regulators
  - concerns amplified with rise of the modern "AI" economy
- Surprisingly, full economic costs of cyber risk poorly understood $\rightarrow$ **This Paper**.

This Project ▸ literature

- Surprisingly, full economic costs of cyber risk poorly understood
  - empirical: focus on impacts of "exogenous" attacks on firm outcomes (stock prices, employment, revenue, ...)
  - theory: study incentives of firms/attackers taking other's behavior as given
- *What's missing*: **strategic considerations** in **general equilibrium**
  - unlike traditional risk, firms can **reduce** exposure to cyberattacks by investing in cybersecurity
  - and this in turn affects incentives of **attackers** to target specific kinds of firms
- **What we do**: **provide a framework formalising this idea**

This Project

literature

- *What's missing*: **strategic considerations** in **general equilibrium**
  - unlike traditional risk, firms can **reduce** exposure to cyberattacks by investing in cybersecurity
  - and this in turn affects incentives of **attackers** to target specific kinds of firms
- **What we do**: **provide a framework formalising this idea**
  - model with (i) firm dynamics and (ii) search/matching framework for cyber attacks

This Project literature

- *What's missing*: **strategic considerations** in **general equilibrium**
  - unlike traditional risk, firms can **reduce** exposure to cyberattacks by investing in cybersecurity
  - and this in turn affects incentives of **attackers** to target specific kinds of firms
- **What we do**: **provide a framework formalising this idea**
  - model with (i) firm dynamics and (ii) search/matching framework for cyber attacks
  - **attackers** target firms of different sizes in search of bounty, which rises with firm size
  - firms make costly **cybersecurity investments** to reduce likelihood of attack succeeding
  - search/matching framework: frictions in attack process, probabilistic nature of attacks

This Project literature

- *What's missing*: **strategic considerations** in **general equilibrium**
  - unlike traditional risk, firms can **reduce** exposure to cyberattacks by investing in cybersecurity
  - and this in turn affects incentives of **attackers** to target specific kinds of firms
- **What we do**: **provide a framework formalising this idea**
  - model with (i) firm dynamics and (ii) search/matching framework for cyber attacks
  - **attackers** target firms of different sizes in search of bounty, which rises with firm size
  - firms make costly **cybersecurity investments** to reduce likelihood of attack succeeding
  - search/matching framework: frictions in attack process, probabilistic nature of attacks
  - equilibrium $\equiv$ fixed point between **attack intensity** and **cybersecurity investment**

This Project ▸ literature

- *What's missing*: **strategic considerations** in **general equilibrium**
  - unlike traditional risk, firms can **reduce** exposure to cyberattacks by investing in cybersecurity
  - and this in turn affects incentives of **attackers** to target specific kinds of firms
- **What we do**: **provide a framework formalising this idea**
  - model with (i) firm dynamics and (ii) search/matching framework for cyber attacks
  - **attackers** target firms of different sizes in search of bounty, which rises with firm size
  - firms make costly **cybersecurity investments** to reduce likelihood of attack succeeding
  - search/matching framework: frictions in attack process, probabilistic nature of attacks
  - equilibrium $\equiv$ fixed point between **attack intensity** and **cybersecurity investment**
  - include a cyber externality: productivity falls with share of firms under attack

This Project

literature

- Two sets of exercises with model: (1) counterfactuals, (2) policy exercises

This Project

literature

- Two sets of exercises with model: (1) counterfactuals, (2) policy exercises

1. **Counterfactuals:** compare (a) *more intense* vs (b) *more frequent* attacks
   - (a) raises prob of attack success conditional on attack, (b) just raises meeting probabilities
   - We find that (b) is *much worse* for the economy than (a)! Key: *GE effects & spillovers*

This Project literature

- Two sets of exercises with model: (1) counterfactuals, (2) policy exercises

1. **Counterfactuals:** compare (a) *more intense* vs (b) *more frequent* attacks
   - (a) raises prob of attack success conditional on attack, (b) just raises meeting probabilities
   - We find that (b) is *much worse* for the economy than (a)! Key: *GE effects & spillovers*

2. **Policy Exercises:** evaluate effectiveness of different policy interventions
   - *ex-post* policies (bailouts) are **counterproductive**: moral hazard
   - *preventative* policies (eg cyber inv subsidies) are **effective**: correct spillover externalities

This Project literature

- Two sets of exercises with model: (1) counterfactuals, (2) policy exercises

1. **Counterfactuals:** compare (a) *more intense* vs (b) *more frequent* attacks
   - (a) raises prob of attack success conditional on attack, (b) just raises meeting probabilities
   - We find that (b) is *much worse* for the economy than (a)! Key: *GE effects & spillovers*

2. **Policy Exercises:** evaluate effectiveness of different policy interventions
   - *ex-post* policies (bailouts) are **counterproductive**: moral hazard
   - *preventative* policies (eg cyber inv subsidies) are **effective**: correct spillover externalities
   - policy effectiveness depends on *nature of cyber risk*: contact rates vs attack capacity

This Project ▸ literature

- Two sets of exercises with model: (1) counterfactuals, (2) policy exercises

1. **Counterfactuals:** compare (a) *more intense* vs (b) *more frequent* attacks
   - (a) raises prob of attack success conditional on attack, (b) just raises meeting probabilities
   - We find that (b) is *much worse* for the economy than (a)! Key: *GE effects & spillovers*

2. **Policy Exercises:** evaluate effectiveness of different policy interventions
   - *ex-post* policies (bailouts) are **counterproductive**: moral hazard
   - *preventative* policies (eg cyber inv subsidies) are **effective**: correct spillover externalities
   - policy effectiveness depends on *nature of cyber risk*: contact rates vs attack capacity
   - Good policies encourage under-investing firms to raise their security levels

This Project literature

- Two sets of exercises with model: (1) counterfactuals, (2) policy exercises

1. **Counterfactuals:** compare (a) *more intense* vs (b) *more frequent* attacks
   - (a) raises prob of attack success conditional on attack, (b) just raises meeting probabilities
   - We find that (b) is *much worse* for the economy than (a)! Key: *GE effects & spillovers*

2. **Policy Exercises:** evaluate effectiveness of different policy interventions
   - *ex-post* policies (bailouts) are **counterproductive**: moral hazard
   - *preventative* policies (eg cyber inv subsidies) are **effective**: correct spillover externalities
   - policy effectiveness depends on *nature of cyber risk*: contact rates vs attack capacity
   - Good policies encourage under-investing firms to raise their security levels *without inducing over-investment by best protected firms*

This Project literature

- Two sets of exercises with model: (1) counterfactuals, (2) policy exercises

1. **Counterfactuals:** compare (a) *more intense* vs (b) *more frequent* attacks
   - (a) raises prob of attack success conditional on attack, (b) just raises meeting probabilities
   - We find that (b) is *much worse* for the economy than (a)! Key: *GE effects & spillovers*

2. **Policy Exercises:** evaluate effectiveness of different policy interventions
   - *ex-post* policies (bailouts) are **counterproductive**: moral hazard
   - *preventative* policies (eg cyber inv subsidies) are **effective**: correct spillover externalities
   - policy effectiveness depends on *nature of cyber risk*: contact rates vs attack capacity
   - Good policies encourage under-investing firms to raise their security levels: in model, small/med *without inducing over-investment by best protected firms*: in model, large firms

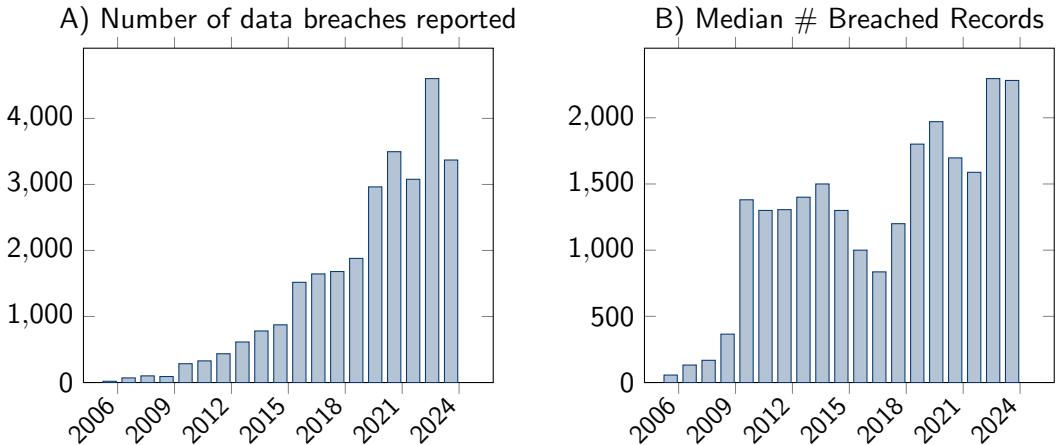
Cyber Risk: What You Need to Know

1. Cyber risk has increased dramatically
2. Incidence has risen sharply for medium-sized firms
3. Cybersecurity investments scale rapidly with firm size
4. Cyberattacks are largely motivated by financial gain

Cyber Risk: What You Need to Know

1. Cyber risk has increased dramatically
2. Incidence has risen sharply for medium-sized firms
3. Cybersecurity investments scale rapidly with firm size
4. Cyberattacks are largely motivated by financial gain

1. Cyber risk has increased dramatically



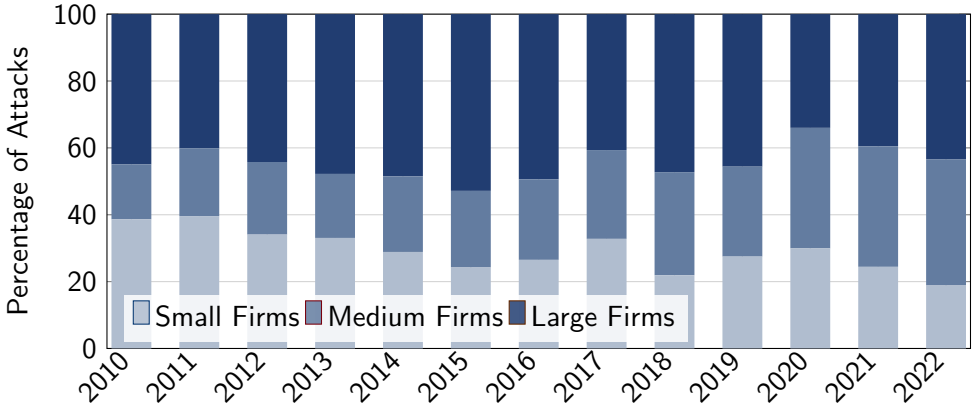
Source: Privacy Rights Clearinghouse, US-based organisations excl govt, Non-profits.

▸ data details ▸ CISSM data ▸ all countries ▸ by org type ▸ by attack type

Cyber Risk: What You Need to Know

1. Cyber risk has increased dramatically
2. Incidence has risen sharply for medium-sized firms
3. Cybersecurity investments scale rapidly with firm size
4. Cyberattacks are largely motivated by financial gain

2. Incidence has risen sharply for medium-sized firms



Source: VERIS database maintained by Verizon's RISK Team

Takeaway: medium-sized firms go from $\approx 16\% \rightarrow 36\%$ of all attacks

▸ data details ▸ dbc attack sizes

Cyber Risk: What You Need to Know

1. Cyber risk has increased dramatically
2. Incidence has risen sharply for medium-sized firms
3. Cybersecurity investments scale rapidly with firm size
4. Cyberattacks are largely motivated by financial gain

3. Cybersecurity investments scale rapidly with firm size

- We're not aware of public data on cyber investments/expenditures by firms
  - Penetration testers, cyber consultants, etc. sometimes provide aggregated client survey data
  - frontier: cyber insurance companies (eg CyberCube), which provide detailed risk assessments
  - key challenge: most sources rely on self-reported survey info, biased towards larger firms
- We rely instead on more broadly available data on a key input to cybersecurity:

  IT workers involved in information security tasks

  - data from Revelio Labs, based on LinkedIn Profiles for workers based in the US
  - ca 90 million profiles/year, 8 mn unique firms, 290k cybersecurity-related job spells
  - we identify cyber workers using keywords in job titles

▸ details

3. Cybersecurity investments scale rapidly with firm size

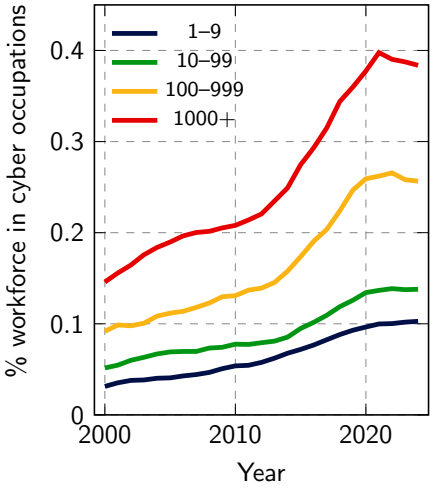


Figure: Revelio Labs data (Oct '24 vintage), positions located in the US only.

Variable	Share of cybersecurity-related employment		
log(EmpSize)	0.0128***	0.0092***	0.0167***
	(0.0002)	(0.0002)	(0.0004)
Year FE	No	Yes	Yes
Industry FE	No	Yes	No
Firm FE	No	No	Yes

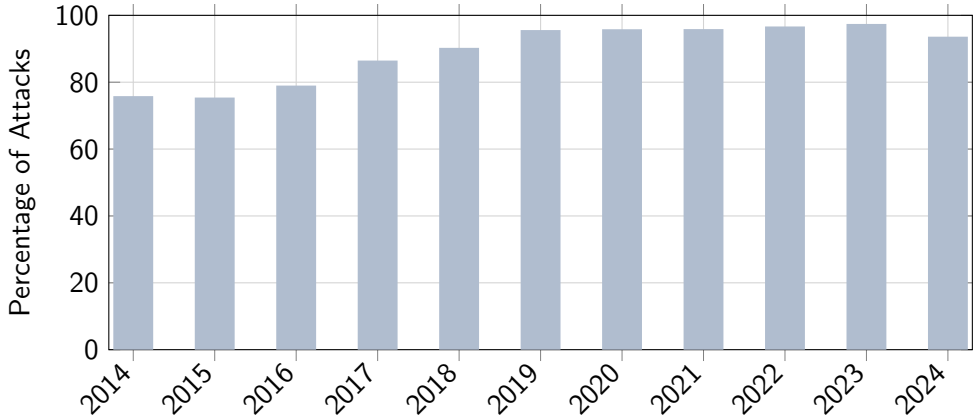
Table: Estimates of the semi-elasticity of the share of cybersecurity-related employees to firm size. All regressions are based on the set of firms in Revelio Labs data (Oct '24 vintage) reporting ≥ 1 US employee with valid industry code & firm ID. Firm size $=\#$ employees of firm recorded in Revelio Labs data.

▸ data details ▸ detailed size category ▸ outsourcing ▸ finance & insurance

Cyber Risk: What You Need to Know

1. Cyber risk has increased dramatically
2. Incidence has risen sharply for medium-sized firms
3. Cybersecurity investments scale rapidly with firm size
4. Cyberattacks are largely motivated by financial gain

4. Cyberattacks are largely motivated by financial gain



Source: Center for International and Security Studies at UMD, US orgs excl public admin.

data details

Cyber Risk: What You Need to Know

1. Cyber risk has increased dramatically
2. Incidence has risen sharply for medium-sized firms
3. Cybersecurity investments scale rapidly with firm size
4. Cyberattacks are largely motivated by financial gain

An Equilibrium Model of Cyber Risk

Environment

timeline

- Discrete time, $t = 0, 1, 2, \ldots$. One final good (numeraire), one factor (labour), 2 agents:
  - Households: supply a unit of labour inelastically to firms, consume output net of all costs.
  - Firms: heterogeneous in productivity φ, produce output using labour st fixed costs, entry/exit.

Environment

timeline

- Discrete time, $t = 0, 1, 2, \ldots$. One final good (numeraire), one factor (labour), 3 agents:
  - Households: supply a unit of labour inelastically to firms, consume output net of all costs.
  - Firms: heterogeneous in productivity φ, produce output using labour st fixed costs, entry/exit.
  - Attackers: pay a fixed cost per attack they undertake; attacks are *directed*
    - choose which firm types φ to direct attacks against, match to a firm of that type frictionally

Environment

timeline

- Discrete time, $t = 0, 1, 2, \ldots$. One final good (numeraire), one factor (labour), 3 agents:
  - Households: supply a unit of labour inelastically to firms, consume output net of all costs.
  - Firms: heterogeneous in productivity φ, produce output using labour st fixed costs, entry/exit.
  - Attackers: pay a fixed cost per attack they undertake; attacks are *directed*
    - choose which firm types φ to direct attacks against, match to a firm of that type frictionally
    - if matched to a firm, choose investment in attacking that firm (attack intensity a)

Environment

timeline

- Discrete time, $t = 0, 1, 2, \ldots$. One final good (numeraire), one factor (labour), 3 agents:
  - Households: supply a unit of labour inelastically to firms, consume output net of all costs.
  - Firms: heterogeneous in productivity φ, produce output using labour st fixed costs, entry/exit.
    - anticipating the chance of an attack, make cyber investments $x \geq 0$ (labour units)
    - we assume that cyber investment is predetermined and fully depreciates each period
  - Attackers: pay a fixed cost per attack they undertake; attacks are *directed*
    - choose which firm types φ to direct attacks against, match to a firm of that type frictionally
    - if matched to a firm, choose investment in attacking that firm (attack intensity a)

Environment ▸ timeline

- Discrete time, $t = 0, 1, 2, \ldots$. One final good (numeraire), one factor (labour), 3 agents:
  - Households: supply a unit of labour inelastically to firms, consume output net of all costs.
  - Firms: heterogeneous in productivity φ, produce output using labour st fixed costs, entry/exit.
    - anticipating the chance of an attack, make cyber investments $x \geq 0$ (labour units)
    - we assume that cyber investment is predetermined and fully depreciates each period
  - Attackers: pay a fixed cost per attack they undertake; attacks are *directed*
    - choose which firm types φ to direct attacks against, match to a firm of that type frictionally
    - if matched to a firm, choose investment in attacking that firm (attack intensity a) *given cyber invt!*
- Attacks **succeed** probabilistically:
  - probability of attack succeeding increases in attack intensity, decreases in cyber investment
  - successful attacks transfer resources from firms to attackers, can cause exits
  - aggregate spillovers: reduced form, agg TFP depends on the share of firms under attack

Firm Problems timeline

- Firms enter each period with productivity φ and an *attack status*
  - Attacked Firms are currently under attack: value $V^a(\varphi)$
  - Safe Firms are not currently under attack: value $V^s(\varphi)$

Firm Problems timeline

- Firms enter each period with productivity φ and an *attack status*
  - Attacked Firms are currently under attack: value $V^a(\varphi)$
  - Safe Firms are not currently under attack: value $V^s(\varphi)$
- Attacked firms can choose to exit (value 0) or continue
  - If they continue, hire labour & produce subject to lower productivity $(1-\ell)\varphi$ for one period
  - Enter next period as safe firms

Firm Problems timeline

- Firms enter each period with productivity φ and an *attack status*
  - Attacked Firms are currently under attack: value $V^a(\varphi)$
  - Safe Firms are not currently under attack: value $V^s(\varphi)$
- Attacked firms can choose to exit (value 0) or continue
  - If they continue, hire labour & produce subject to lower productivity $(1-\ell)\varphi$ for one period
  - Enter next period as safe firms
- Safe firms can choose to exit (value 0) or continue
  - If they continue, hire labour & produce, and choose cyber investments $x \geq 0$
  - After production, meet an attacker with probability $q(\varphi)$. No meetings $\implies$ safe next period

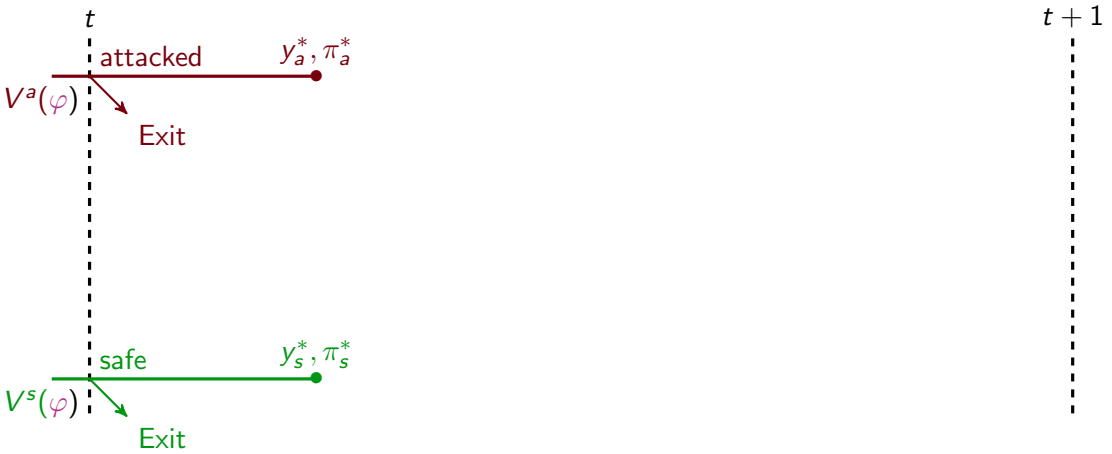
Firm Problems timeline

- Firms enter each period with productivity φ and an *attack status*
  - Attacked Firms are currently under attack: value $V^a(\varphi)$
  - Safe Firms are not currently under attack: value $V^s(\varphi)$
- Attacked firms can choose to exit (value 0) or continue
  - If they continue, hire labour & produce subject to lower productivity $(1-\ell)\varphi$ for one period
  - Enter next period as safe firms
- Safe firms can choose to exit (value 0) or continue
  - If they continue, hire labour & produce, and choose cyber investments $x \geq 0$
  - After production, meet an attacker with probability $q(\varphi)$. No meetings $\implies$ safe next period
  - If matched to an attacker, the attacker observes x and chooses attack intensity $a \in [0, A]$

Firm Problems timeline

- Firms enter each period with productivity φ and an *attack status*
  - Attacked Firms are currently under attack: value $V^a(\varphi)$
  - Safe Firms are not currently under attack: value $V^s(\varphi)$
- Attacked firms can choose to exit (value 0) or continue
  - If they continue, hire labour & produce subject to lower productivity $(1-\ell)\varphi$ for one period
  - Enter next period as safe firms
- Safe firms can choose to exit (value 0) or continue
  - If they continue, hire labour & produce, and choose cyber investments $x \geq 0$
  - After production, meet an attacker with probability $q(\varphi)$. No meetings $\implies$ safe next period
  - If matched to an attacker, the attacker observes x and chooses attack intensity $a \in [0, A]$
  - Attacks *succeed* with probability $\Lambda(a, x)$
    - If successful, firm enters next period as under attack. Else, safe next period.

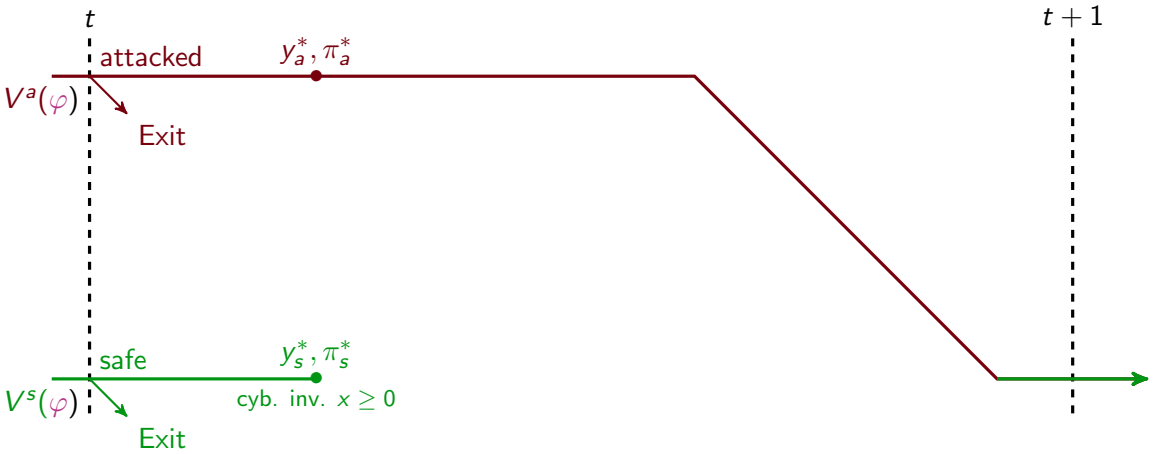
Timing of Events



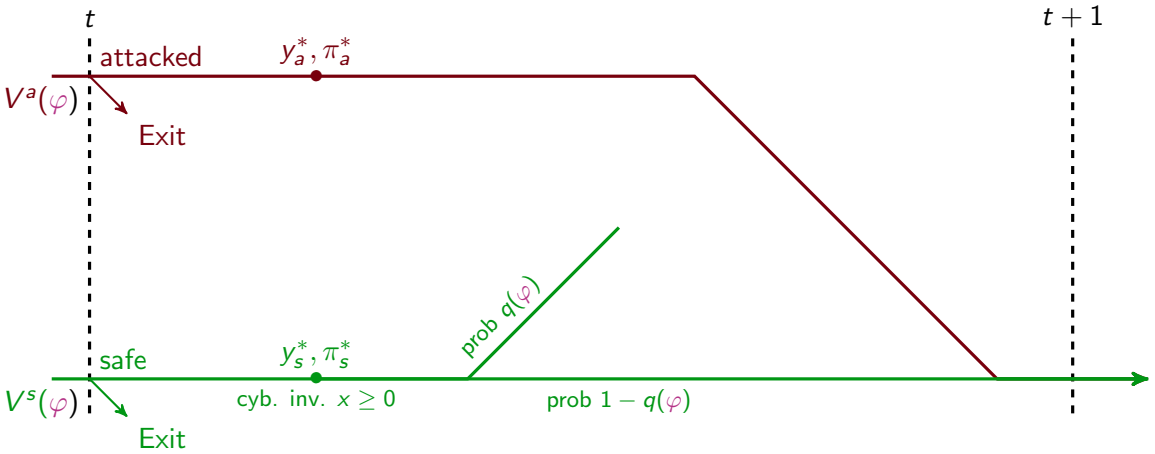
Timing of Events



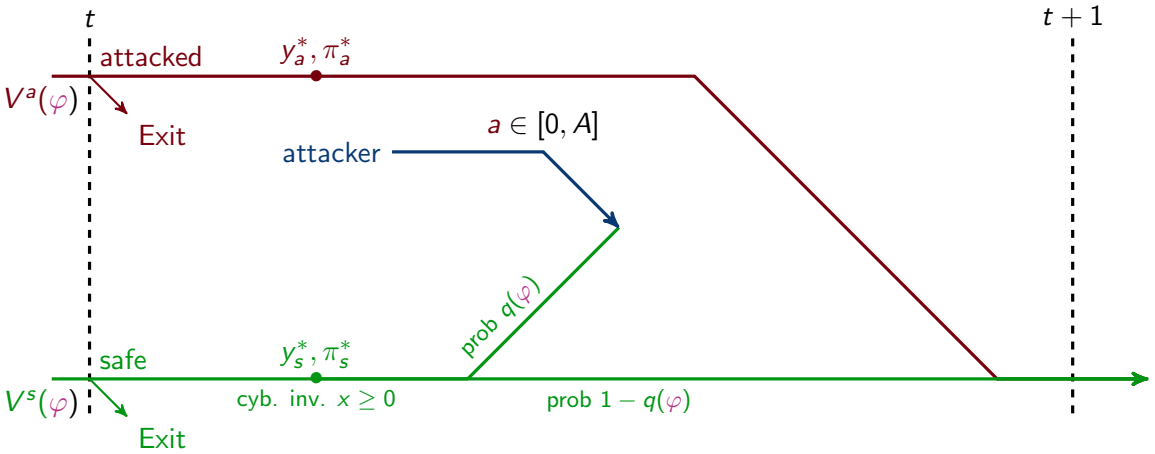
Timing of Events



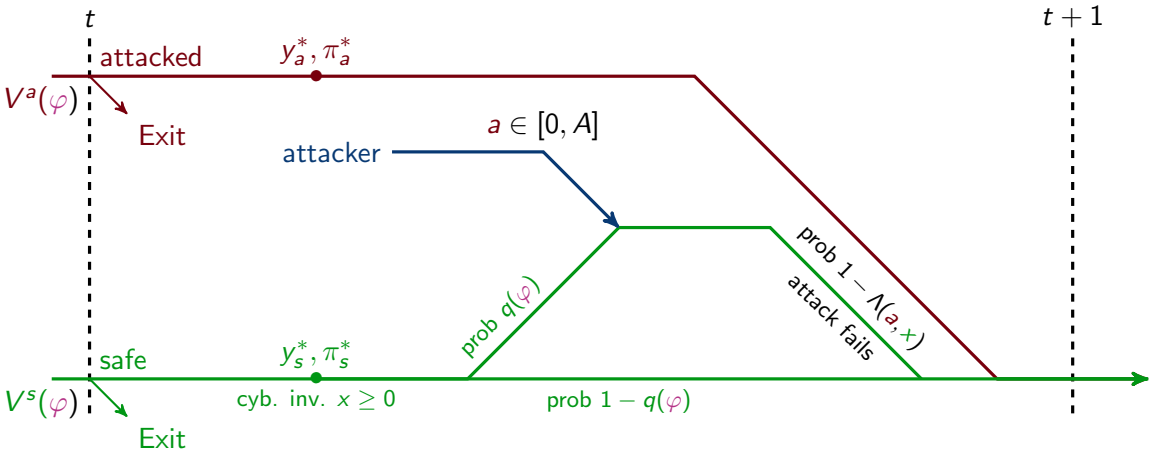
Timing of Events



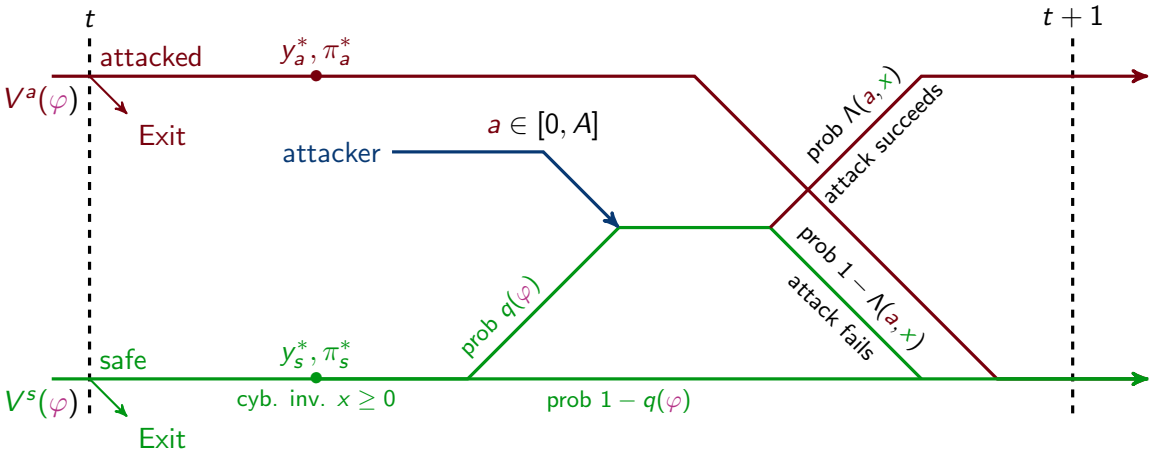
Timing of Events



Timing of Events



Timing of Events



Firm Problems timeline

Safe Firms

$$V^s(\varphi) = \max\left\{0,\ \max_{n,x\geq 0}\left[Z\varphi n^\alpha - wn - f - wx + \beta\mathbb{E}_{\varphi'|\varphi}V(\varphi', x)\right]\right\}$$

- Choose production, cybersecurity labour

Attacked Firms

$$V^a(\varphi) = \max\left\{0,\ \max_{n}\left[(1-\ell)Z\varphi n^\alpha - wn - f + \beta\mathbb{E}_{\varphi'|\varphi}V^s(\varphi')\right]\right\}$$

- Suffer prodtvty loss ℓ, safe next period

Firm Problems timeline

Safe Firms

$$V^s(\varphi) = \max\left\{0,\ \max_{n,x\geq 0}\left[Z\varphi n^\alpha - wn - f - wx + \beta\mathbb{E}_{\varphi'|\varphi}V(\varphi', x)\right]\right\}$$

- Choose production, cybersecurity labour

Attacked Firms

$$V^a(\varphi) = \max\left\{0,\ \max_{n}\left[(1-\ell)Z\varphi n^\alpha - wn - f + \beta\mathbb{E}_{\varphi'|\varphi}V^s(\varphi')\right]\right\}$$

- Suffer prodtvty loss ℓ, safe next period

Firm Problems timeline

Safe Firms

$$V^s(\varphi) = \max\left\{0,\ \max_{n,x\geq 0}\left[Z\varphi n^\alpha - wn - f - wx + \beta\mathbb{E}_{\varphi'|\varphi}V(\varphi', x)\right]\right\}$$

- Choose production, cybersecurity labour

Attacked Firms

$$V^a(\varphi) = \max\left\{0,\ \max_{n}\left[(1-\ell)Z\varphi n^\alpha - wn - f + \beta\mathbb{E}_{\varphi'|\varphi}V^s(\varphi')\right]\right\}$$

- Suffer prodtvty loss ℓ, safe next period

- After production, safe firms either meet an attacker (V^m) or remain safe (V^s)

$$V(\varphi, x) = q(\varphi)V^m(\varphi, x) + (1 - q(\varphi))V^s(\varphi)$$

Firm Problems

timeline

Safe Firms

$$V^s(\varphi) = \max\Big\{0,\ \max_{n,x\geq 0}\big[Z\varphi n^\alpha - wn - f - wx + \beta\mathbb{E}_{\varphi'|\varphi}V(\varphi', x)\big]\Big\}$$

- Choose production, cybersecurity labour

Attacked Firms

$$V^a(\varphi) = \max\Big\{0,\ \max_{n}\big[(1-\ell)Z\varphi n^\alpha - wn - f + \beta\mathbb{E}_{\varphi'|\varphi}V^s(\varphi')\big]\Big\}$$

- Suffer prodtvty loss ℓ, safe next period

- After production, safe firms either meet an attacker (V^m) or remain safe (V^s)

$$V(\varphi, x) = q(\varphi)V^m(\varphi, x) + (1 - q(\varphi))V^s(\varphi)$$

- Conditional on matching, attacks succeed with probability $\Lambda(a, x)$

more

$$V^m(\varphi, x) = \Lambda(a, x)V^a(\varphi) + (1 - \Lambda(a, x))V^s(\varphi)$$

Attackers, Search and Congestion ▸ timeline ▸ model ingredients

1. **Before Matching:** An unbounded mass of potential attackers decides whether to attack
   - Paying cost κ to attack, acquire $A > 0$ units of *attack capacity*
   - Choose which firm type φ to target with their attack: attacks are *directed*

Attackers, Search and Congestion

timeline | model ingredients

1. **Before Matching:** An unbounded mass of potential attackers decides whether to attack
   - Paying cost κ to attack, acquire $A > 0$ units of *attack capacity*
   - Choose which firm type φ to target with their attack: attacks are *directed*

2. **Matching:** Let $S(\varphi) = \#$ safe firms with tfp φ, $X(\varphi) = \#$ attackers choosing type φ
   - Frictional matching: $\mathcal{M}(S(\varphi), X(\varphi)) = \#$ matches between safe firms and attackers
   - Contact rates for firms $q(\varphi)$, attackers $\lambda(\varphi)$:

$$q(\varphi) = \frac{\mathcal{M}\left(S(\varphi), X(\varphi)\right)}{S(\varphi)} \qquad , \qquad \lambda(\varphi) = \frac{\mathcal{M}\left(S(\varphi), X(\varphi)\right)}{X(\varphi)}$$

Attackers, Search and Congestion

timeline | model ingredients

3. **If Matched:** observe firm's cyber investment x, choose attack intensity $a \in [0, A]$

$$a^*(x, \varphi) = \arg \max_{a \in [0,A]} \left\{ -a + \Lambda(a, x) \times \underbrace{\ell}_{\text{loss rate}} \times \underbrace{y^a(\varphi)}_{\substack{\text{Prodn chosen by} \\ \text{firm under attack}}} \right\}$$

Attackers, Search and Congestion

timeline | model ingredients

3. **If Matched:** observe firm's cyber investment x, choose attack intensity $a \in [0, A]$

$$a^*(x, \varphi) = \arg \max_{a \in [0,A]} \left\{ -a + \Lambda(a, x) \times \underbrace{\ell}_{\text{loss rate}} \times \underbrace{y^a(\varphi)}_{\substack{\text{Prodn chosen by} \\ \text{firm under attack}}} \right\}$$

- Higher φ firms have higher y^a, so attackers prefer targeting larger firms ceteris paribus

Attackers, Search and Congestion

▸ timeline ▸ model ingredients

3. **If Matched:** observe firm's cyber investment x, choose attack intensity $a \in [0, A]$

$$a^*(x, \varphi) = \arg \max_{a \in [0,A]} \left\{ -a + \Lambda(a, x) \times \underbrace{\ell}_{\text{loss rate}} \times \underbrace{y^a(\varphi)}_{\substack{\text{Prodn chosen by} \\ \text{firm under attack}}} \right\}$$

- Higher φ firms have higher y^a, so attackers prefer targeting larger firms ceteris paribus
- Free entry $\implies$ Congestion: more desirable targets have lower attacker contact rates

$$\kappa = \lambda(\varphi) \cdot \Lambda(a^*(x, \varphi), x) \cdot \ell \cdot y^a(\varphi)$$

- We assume attackers are foreigners: costs/bounties not in economy's resource constraint

▸ data?

The Economics of Cybersecurity Investments

timeline | model ingredients

- Firms anticipate that attackers will react to their cyber investments

  $\Longrightarrow$ will behave as Stackelberg leaders in the game against attackers

- From firm's point of view, probability of being successfully attacked is

$$\Pr(\text{successful attack}|x,\varphi) = q(\varphi)\cdot\Lambda(a^*(x,\varphi),x)$$

- The first-order condition characterising $x^*(\varphi)$ is

$$\underbrace{w}_{\substack{\text{marginal cost}\\ \text{of unit of}\\ \text{cyber investment}}} = \mathbb{E}_{\varphi'|\varphi}\left\{\underbrace{q(\varphi')\cdot\left(-\frac{d\Lambda(a^*(x,\varphi'),x)}{dx}\right)\Bigg|_{x=x^*(\varphi)}}_{\text{fall in prob of successful attack}}\cdot\underbrace{\beta\left(V^s(\varphi')-V^a(\varphi')\right)}_{\text{discounted value of avoiding attack}}\right\}$$

Entry, Exit, and Spillovers

timeline model ingredients

Firm dynamics

1. Entrants pay f_e and draw φ
2. Entry value falls when cyber risk rises
3. Free entry by firms implies that

$$f_e = \int_{\varphi} V^s(\varphi) dG(\varphi)$$

Entry, Exit, and Spillovers

timeline model ingredients

Firm dynamics

1. Entrants pay f_e and draw φ
2. Entry value falls when cyber risk rises
3. Free entry by firms implies that

$$f_e = \int_{\varphi} V^s(\varphi) dG(\varphi)$$

Aggregate spillovers

1. Breaches disrupt connected firms
2. Productivity falls with attack prevalence

$$Z = \left(\int S(\varphi) d\varphi \right)^{\epsilon}$$

Equilibrium

▸ timeline ▸ model ingredients

A **stationary equilibrium** of the model is a collection of

- a wage w
- firm policies $\{n_s(\varphi), y_s(\varphi), \pi_s(\varphi), x^*(\varphi), n_a(\varphi), y_a(\varphi), \pi_a(\varphi)\}_\varphi$
- attack policies $a^*(\varphi)$
- market tightnesses, matching rates, attack success rates $\{\theta(\varphi), q(\varphi), \lambda(\varphi), \Lambda(\varphi)\}_\varphi$
- a mass of entrants $M(\varphi)$, total mass $L(\varphi)$ of firms of type φ and mass $S(\varphi)$ of safe firms
- firm value functions $\{V^s(\varphi), V^a(\varphi)\}_\varphi$

such that

Equilibrium

timeline | model ingredients

1. Attackers anticipate defenses:

   Given $x^*(\varphi)$, $\theta(\varphi)$, and firm policies, attack policies solve the attacker's problem

$$a^*(\varphi) \equiv a^*(x, \varphi)|_{x=x^*(\varphi)} = \arg \max_{a \in [0,A]} \left\{ -a + \underbrace{\Lambda(a, x^*(\varphi)) \cdot \zeta(\varphi) \cdot \ell \varphi n^{\alpha}}_{\text{Successful Attack}} \right\}$$

Equilibrium

▸ timeline ▸ model ingredients

1. Attackers anticipate defenses:

   Given $x^*(\varphi)$, $\theta(\varphi)$, and firm policies, attack policies solve the attacker's problem

$$a^*(\varphi) \equiv a^*(x, \varphi)|_{x=x^*(\varphi)} = \arg \max_{a \in [0,A]} \left\{ -a + \underbrace{\Lambda(a, x^*(\varphi)) \cdot \zeta(\varphi) \cdot \ell \varphi n^\alpha}_{\text{Successful Attack}} \right\}$$

2. Firms behave as Stackelberg leaders:

   Given $a^*(\varphi)$, $\theta(\varphi)$, and w, value functions and firm policies solve the firm's problem

$$w = \beta \mathbb{E}_{\varphi'|\varphi} \left[q(\varphi') \cdot \left(-\frac{\mathbf{d}\Lambda(a^*(\varphi'), x(\varphi'))}{\mathbf{d}x} \right) \cdot \left[V^s(\varphi') - V^a(\varphi') \right] \right]$$

   and $\{n_s(\varphi), y_s(\varphi), \pi_s(\varphi), n_a(\varphi), y_a(\varphi), \pi_a(\varphi)\}_\varphi$ satisfy static profit max problems.

Equilibrium

timeline | model ingredients

3. Given attack and security policies, the probability of a successful attack is determined

$$\Lambda(\varphi) \equiv \Lambda(a^*(\varphi), x^*(\varphi)) = \frac{\exp\left[\frac{a^*(\varphi) - C(x^*(\varphi))}{\varrho}\right]}{1 + \exp\left[\frac{a^*(\varphi) - C(x^*(\varphi))}{\varrho}\right]}$$

4. Given the value functions, the free entry conditions for firms and attackers hold
5. Given masses of safe firms and attackers, tightnesses and matching rates are consistent
6. Labour markets clear:

$$\int_{\varphi} \left[S(\varphi) \cdot (n_s^*(\varphi) + x^*(\varphi)) + (L(\varphi) - S(\varphi)) \cdot n_a^*(\varphi)\right] d\varphi = 1$$

7. The stationary masses of firms $L(\varphi), S(\varphi)$ are consistent with policy fns, transition laws.

Quantification

parameters | calibration step 1 | calibration step 2

- Two-step calibration: "Firm Dynamics block" & "Cyber block"
  - Firm block: productivity process, entry and fixed operating costs, entrant TFP distbn
  - Cyber block: matching & attack success prob, attack capacity, direct + spillover losses
- Main target moments:
  - "firm dynamics block": firm size distbn, entrant sizes, exit rates
  - average cyber employment share by firm size
  - aggregate losses from cyber risk as share of GDP
  - total share of firms under attack
  - amplification of direct losses via spillovers

The costs of cyber attacks

- We compare the "Cyber" equilibrium ($\ell > 0$) to the "No-Cyber" equilibrium ($\ell = 0$)

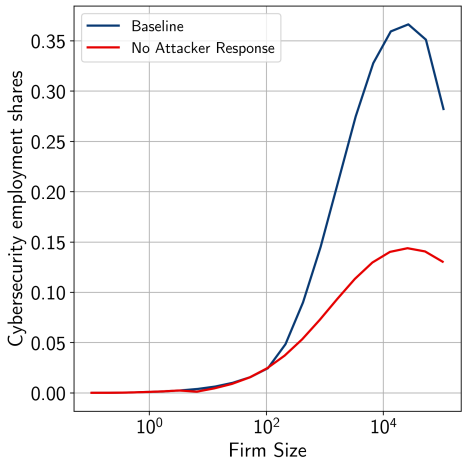
	Productivity (Z)	Entry Mass (M)	Output (Y)	Consumption (C)
No-Cyber	1.0000	0.00370	0.4862	0.4593
Cyber	0.9938	0.00357	0.4776	0.4517
Percent change (%)	−0.62	−3.61	−1.76	−1.66

- **Mechanism**
  - Attacks lower aggregate productivity through propagation spillovers
    1. Lower prodtvty $\Longrightarrow$ lower value of entry $\Longrightarrow$ fewer firms, lower wages
    2. Lower prodtvty $\Longrightarrow$ smaller $V^s - V^a$ gap $\Longrightarrow$ $\downarrow$ cyber investments $\Longrightarrow$ $\uparrow$ firms under attack

  $\Longrightarrow$ **amplification!**
  - Consumption falls as output declines and resources move to cyber defense

Does "endogenous" cyber risk matter?

- We study our baseline vs an economy where attackers cannot choose a
  - require $a(\varphi) = \bar{a}$, (baseline avg)
  - x now equally effective across sizes
- Shr attacked firms similar (0.6% vs 0.5%)
- But firm investments decline significantly
  - largest declines for large firms!
- counterfactual output 0.7% higher, wages 0.6%



Takeaway: Modeling endogenous cyber risk can dramatically affect GE consequences

Counterfactuals

- Study rise in cyber risk due to (i) higher attack capacity, (ii) higher match rate
- Former raises typical intensity of attacks, latter raises share of firms under attack
- Latter is substantially more costly for economy: *spillovers reduce productivity!*

How does higher cyber risk affect the economy?

- **Our goal**: show that GE effects emphasized affect the economics of rising cyber risk
  - We consider two shocks that raise the level of cyber risk in the economy
  - capture plausible forms of technological change that favour attackers (AI??)
- **Our approach**: solve for the model's steady state under alternative parameter values
  1. Higher attack capacity A, allowing attackers to deploy more severe attacks against firms
  2. Higher matching rates $\lambda(\varphi), q(\varphi)$, raising contact rates between attackers and firms
- Let Y denote aggregate output. We decompose this into

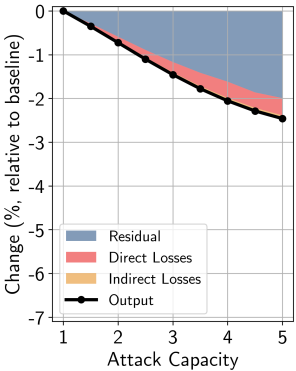
$$\Delta Y = \underbrace{\Delta Y^{direct}}_{\text{Direct Losses}} + \underbrace{\Delta Y^{indirect}}_{\text{Indirect Losses}} + \underbrace{\Delta Y^{Residual}}_{\text{Residual Change}}$$

How does higher cyber risk affect the economy?

- **Our goal**: show that GE effects emphasized affect the economics of rising cyber risk
  - We consider two shocks that raise the level of cyber risk in the economy
  - capture plausible forms of technological change that favour attackers (AI??)
- **Our approach**: solve for the model's steady state under alternative parameter values
  1. Higher attack capacity A, allowing attackers to deploy more severe attacks against firms
  2. Higher matching rates $\lambda(\varphi), q(\varphi)$, raising contact rates between attackers and firms
- Let Y denote aggregate output. We decompose this into

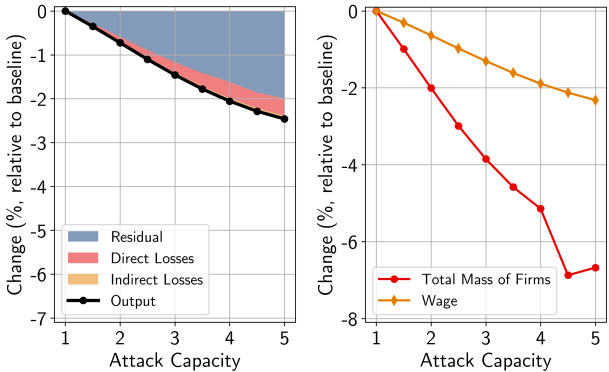
$$\Delta Y = \underbrace{\Delta\left[\ell Z \int y_a(\varphi)\left(L(\varphi) - S(\varphi)\right) d\varphi\right]}_{\text{Direct Losses}} + \underbrace{\Delta\left[w \int x^*(\varphi) S(\varphi) d\varphi + \frac{1-Z}{Z} Y\right]}_{\text{Indirect Losses}} + \underbrace{\Delta Y^{Residual}}_{\text{Residual Change}}$$

Higher Attack Capacity has modest effects



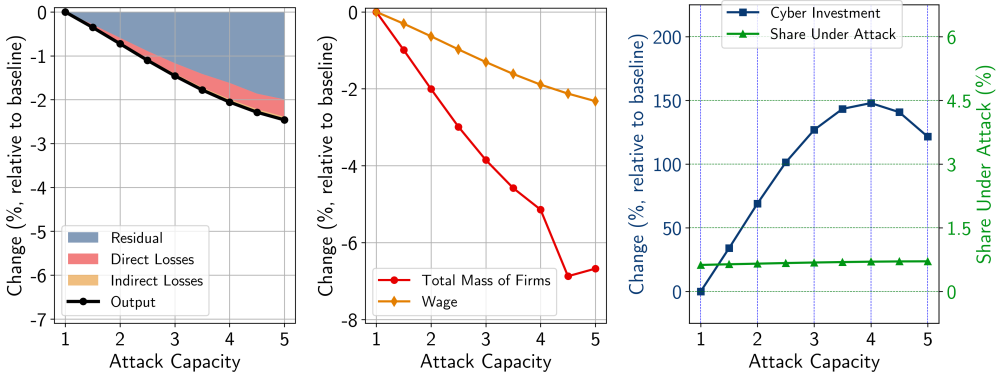
- 5x rise in attack capacity $\implies$ modest fall in output, direct $>$ indirect losses

Higher Attack Capacity has modest effects



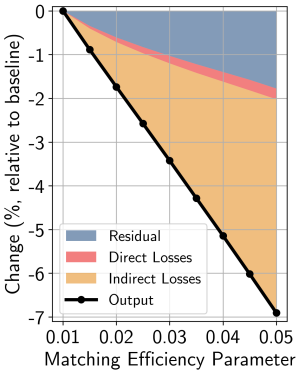
- Modest fall in wages and in total mass of firms: exits by mid-sized firms

Higher Attack Capacity has modest effects



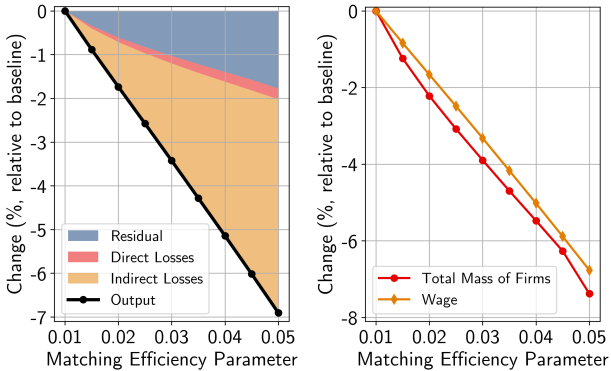
- Modest rise in cyber investment by larger firms $\Longrightarrow$ small rise in share under attack

Higher Matching Rates have drastic consequences



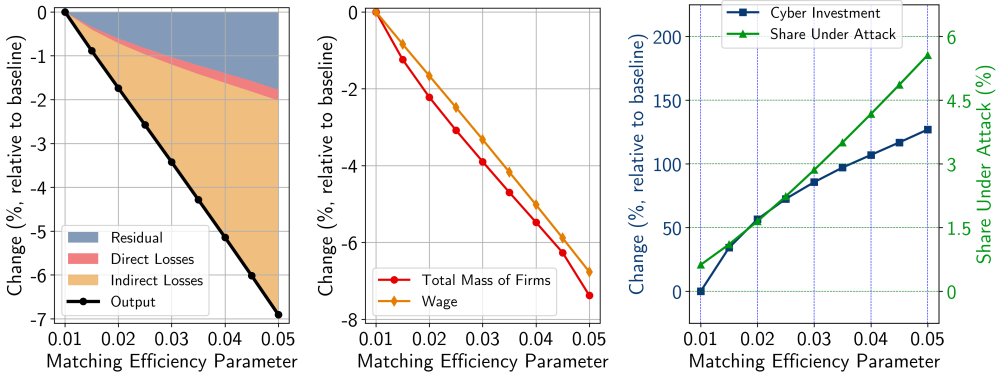
- 5x rise in match rate $\implies$ large fall in output, indirect $>>$ direct losses

Higher Matching Rates have drastic consequences



- Large falls in wages & mass of firms: exits by *all firms*, fall in prodn + cyber labour dd

Higher Matching Rates have drastic consequences



- Much weaker rise in cyber investment, large rise in share under attack

The Source of Rising Cyber Risk Matters!

attack probs output conc

- Higher Attack Capacity has relatively small effects on aggregate output

- Higher Matching Rates have large effects on aggregate output

The Source of Rising Cyber Risk Matters!

attack probs | output conc

- Higher Attack Capacity has relatively small effects on aggregate output
  - Higher attack capacity leads to a higher probability of success, *conditional on matching*
  - Incumbents respond by investing more, especially mid/large sized firms!

- Higher Matching Rates have large effects on aggregate output

The Source of Rising Cyber Risk Matters!

attack probs | output conc

- Higher Attack Capacity has relatively small effects on aggregate output
  - Higher attack capacity leads to a higher probability of success, *conditional on matching*
  - Incumbents respond by investing more, especially mid/large sized firms!
  - Overall attacked share barely changes: no increase in spillover-driven losses

- Higher Matching Rates have large effects on aggregate output

The Source of Rising Cyber Risk Matters!

attack probs | output conc

- Higher Attack Capacity has relatively small effects on aggregate output
  - Higher attack capacity leads to a higher probability of success, *conditional on matching*
  - Incumbents respond by investing more, especially mid/large sized firms!
  - Overall attacked share barely changes: no increase in spillover-driven losses

- Higher Matching Rates have large effects on aggregate output

The Source of Rising Cyber Risk Matters! attack probs output conc

- Higher Attack Capacity has relatively small effects on aggregate output
  - Higher attack capacity leads to a higher probability of success, *conditional on matching*
  - Incumbents respond by investing more, especially mid/large sized firms!
  - Overall attacked share barely changes: no increase in spillover-driven losses

- Higher Matching Rates have large effects on aggregate output
  - Lead to a rising attack probability across all firms, including smaller ones
  - Smaller firms are less willing to invest in security, and more likely to just exit

The Source of Rising Cyber Risk Matters!

attack probs output conc

- Higher Attack Capacity has relatively small effects on aggregate output
  - Higher attack capacity leads to a higher probability of success, *conditional on matching*
  - Incumbents respond by investing more, especially mid/large sized firms!
  - Overall attacked share barely changes: no increase in spillover-driven losses

- Higher Matching Rates have large effects on aggregate output
  - Lead to a rising attack probability across all firms, including smaller ones
  - Smaller firms are less willing to invest in security, and more likely to just exit
  - Leads to fall in measure of firms, much sharper rise in share of attacked firms
  - Large indirect losses driven by the spillover effect reducing aggregate TFP

The Source of Rising Cyber Risk Matters!

attack probs output conc

- Higher Attack Capacity has relatively small effects on aggregate output
  - Higher attack capacity leads to a higher probability of success, *conditional on matching*
  - Incumbents respond by investing more, especially mid/large sized firms!
  - Overall attacked share barely changes: no increase in spillover-driven losses
  - Redistributes output away from largest firms: likelihood of successful attack rises the most
- Higher Matching Rates have large effects on aggregate output
  - Lead to a rising attack probability across all firms, including smaller ones
  - Smaller firms are less willing to invest in security, and more likely to just exit
  - Leads to fall in measure of firms, much sharper rise in share of attacked firms
  - Large indirect losses driven by the spillover effect reducing aggregate TFP
  - Redistributes output toward large firms, who can better withstand attacks

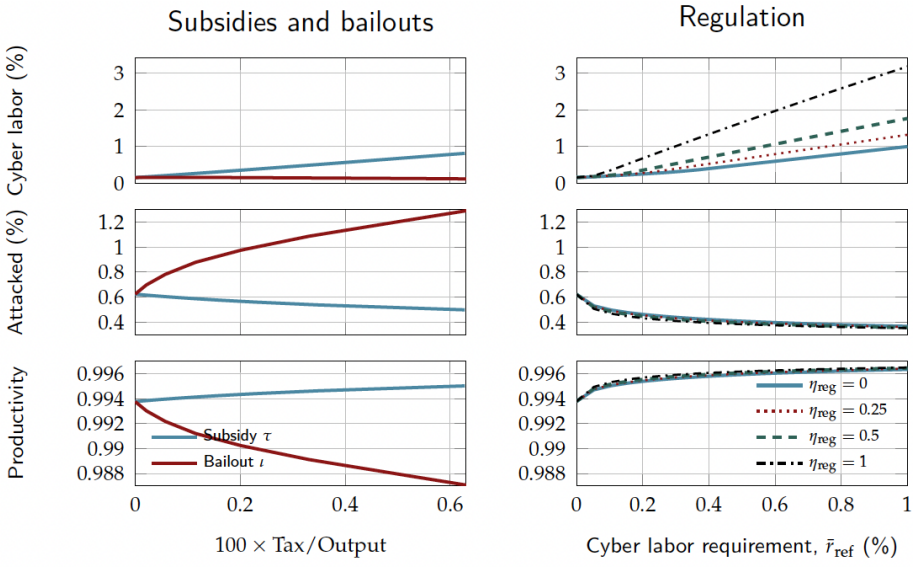
Policies to Alleviate Cyber Risk

- Distortionary tax-financed subsidies for cyber investment vs Bailouts for affected firms
- Most of the time, subsidies are better: fixing an externality vs moral hazard
- Why "most of the time": distortions $\implies$ sometimes subsidies aren't "good enough"

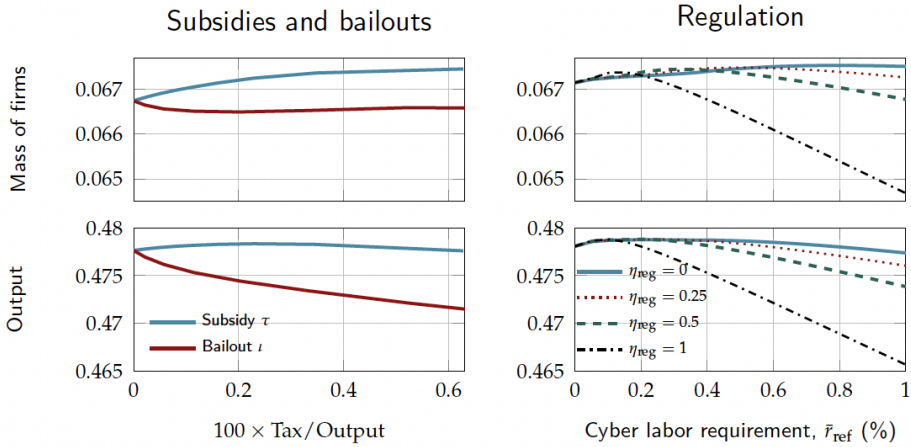
How should we respond to rising cyber risk?

- We evaluate three policy responses to rising cyber risk:
  - **Bailouts** details
    - government finances fraction ι of direct losses for attacked firms via proportional tax
    - effectively reduces proportional loss from attack from $1-\ell$ to $1-\ell(1-\iota)$
  - **Subsidies** details
    - government pays for share τ of firms' cyber investments via proportional tax
    - effectively reduces cost of cyber investment from wx to $(1-\tau)wx$
  - **Regulation** details
    - government forces firms to have minimum cyber security, $x \geq \rho(\varphi)n$
    - cyber requirement *can* be progressive $\rho(\varphi) = \frac{\bar{r}_{\text{reg}}}{1-\bar{r}_{\text{reg}}} \left(\frac{\varphi}{\varphi_{\text{reg}}}\right)^{\eta_{\text{reg}}}$

Preventative vs. Reactive Policies: Firm Dynamics



Preventative vs. Reactive Policies: Aggregate Outcomes



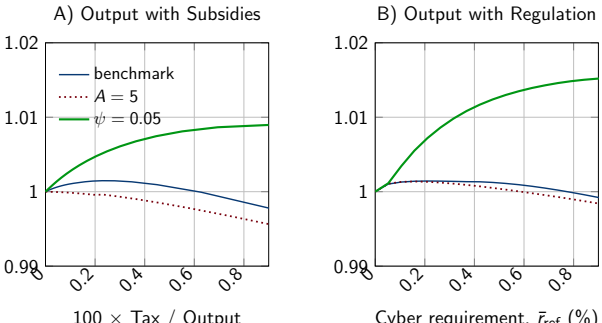
- Optimal subsidy: $\sim 75\% \rightarrow \Delta Y \approx 0.13\%$
- Optimal regulation: no progressivity $\eta_{\text{reg}} = 0$, $\bar{r}_{\text{reg}} = 0.2\% \rightarrow \Delta Y \approx 0.14\%$

Policy Effectiveness Depends on the Cyber Environment

- Preventative policies can mitigate cyber risk and increase output.
- But their effectiveness depends on the nature of cyber risk.

Policy Effectiveness Depends on the Cyber Environment

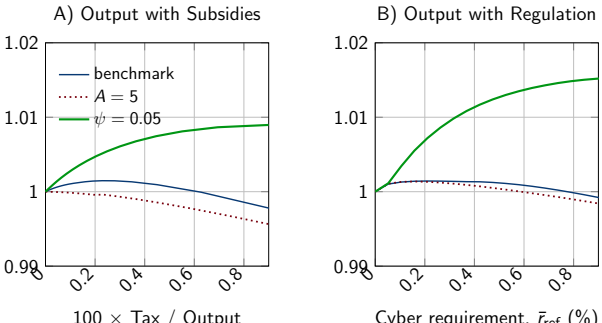
- Preventative policies can mitigate cyber risk and increase output.
- But their effectiveness depends on the nature of cyber risk.



- Higher contact rates: stronger case for prevention.
- Higher attack capacity: subsidies can reduce output.

Policy Effectiveness Depends on the Cyber Environment

- Preventative policies can mitigate cyber risk and increase output.
- But their effectiveness depends on the nature of cyber risk.



- Higher contact rates: stronger case for prevention.
- Higher attack capacity: subsidies can reduce output.

- Moderate regulation delivers more robust output gains.

Policy Tradeoffs

- As in most contexts, ex-post bailouts are a bad idea: moral hazard
- Subsidies are more effective, but fiscally costly and redistribute resources
  - As attacks become more intense, subsidies become transfers from small to large firms
  - Lead to exit among small firms, reducing mass of firms in equilibrium
- In our model, regulations mandating minimum cybersecurity levels are most effective
  - Key idea: an effective policy raises investment by firms which aren't investing ...
  - ... without inducing over-investment by firms which are already safe

Conclusion

- Model of cyber risk featuring **strategic considerations** in **general equilibrium**.
- The *source* of rising cyber risk is critical for understanding its effects
  - rising *frequency* of attacks *much* worse than *more intense* attacks
  - key role for entry/exit and GE effects via factor markets
- We evaluate policy responses to rising cyber risk in our model

  Lesson 1. "Preventative" policies can raise output: internalize spillover

  Lesson 2. "Ex-post" policies (bailouts): reduce output by weakening cybersecurity investment

  Lesson 3. Policy should target underinvestment without distorting already protected firms.

Appendix

Our Contribution

back back (model) back (results)

1. **Economic consequences of cyber risk:** Kopp et al ('17), Kamiya et al ('18, '21), Duffie Younger ('19), Jamilov-Rey ('21), Eisenbach et al ('22), Koo et al ('22), Crosignani et al ('23), Florakis et al ('23), Cobos-Cakir ('24), Murciano-Goroff et al. ('25)
   - Evidence on costs to affected firms, little on spillovers and aggregate consequences
2. **Theoretical frameworks exploring cyber risk:** Anderson ('01), Gordon Loeb ('02), Moore Clayton Anderson ('09), Anand et al ('22), Ebel Mitra ('22), Ahnert et al ('24'), Ramirez ('25)
   - Focus on individual firms' security choices; nascent lit on strategic interactions

- **This Paper:** Tractable GE model of firm dynamics with endogenous cyber risk
  - Jointly determined attack incentives and cyber responses
  - Policy: subsidise cyber investment, don't bailout firms once attacked

1. Cyber risk has increased dramatically over past 20 years

back

- Measurement is severely complicated by two features of environment:
  - substantial bias in regulatory requirements surrounding cyber risk reporting
  - particularly salient reputational concerns around disclosure
  - no common reporting standards until relatively recently, making historical trends hard to track
- Main source for aggregate trends: the *Data Breach Chronology (DBC)*
  - compiled by the Privacy Rights Clearinghouse, a nonprofit research group, since 2005
  - underlying source: public disclosures at national/state level in the US
  - emphasis on data breaches, comprehensive coverage across countries

The Rising Number of Attacks: CISSM Data

back

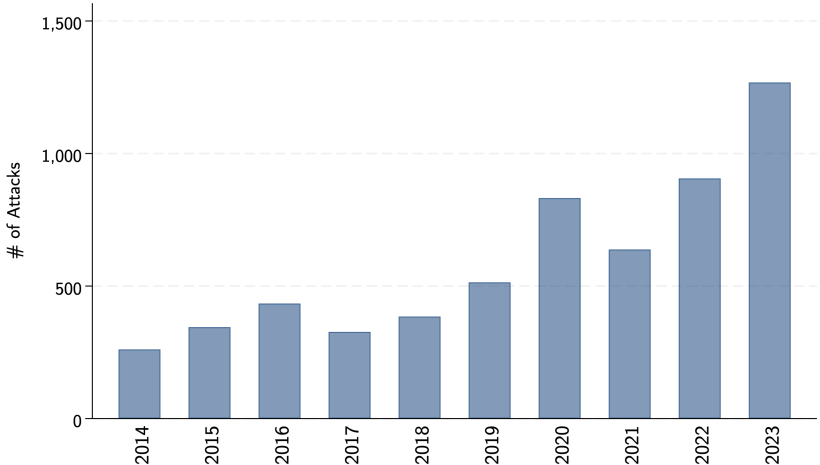


Figure: Number of cyberattacks reported to the Center for International and Security Studies in Maryland, 2014-2023. Data for attacks on US-based private business organisations only.

The Rising Number of Attacks: DBC Data, All Countries

back

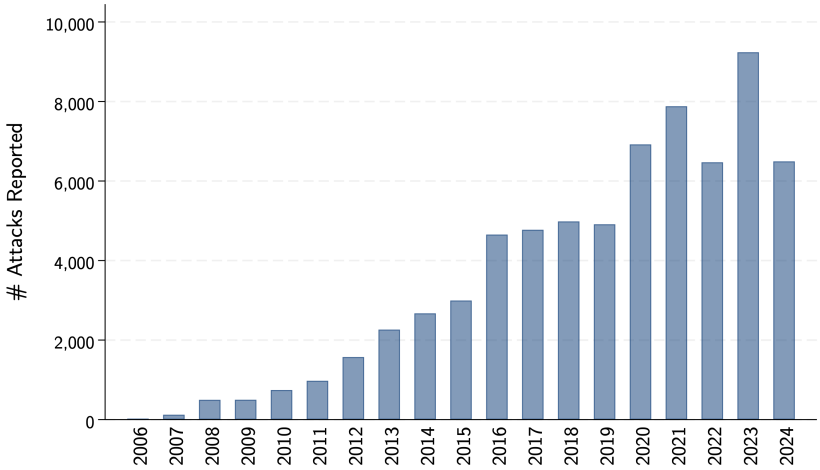


Figure: Number of data breaches reported in DBC dataset. Data for attacks on private business organisations only.

The Rising Number of Attacks: DBC Data, by Organization Type

back

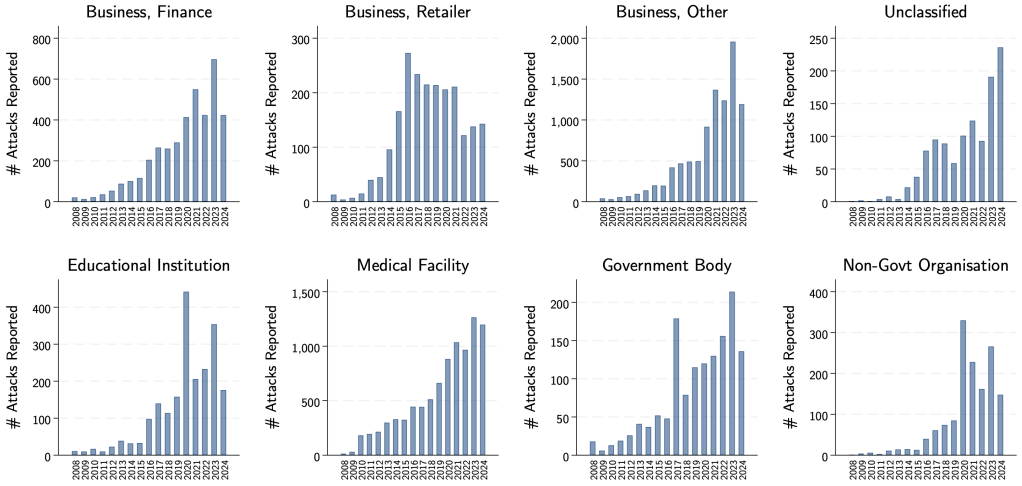


Figure: Number of data breaches reported in DBC dataset, by organization type. Data for attacks on US-based businesses only.

The Rising Number of Attacks: DBC Data, by Attack Type

back

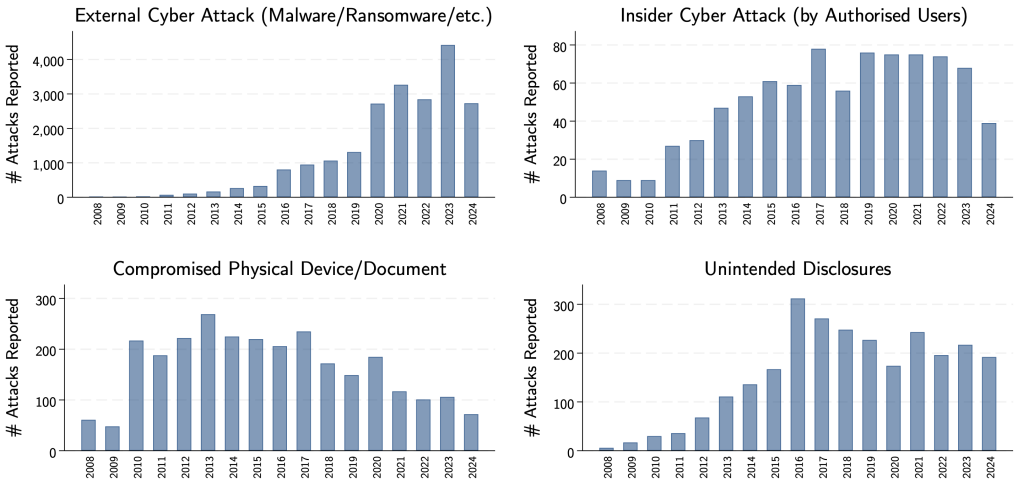


Figure: Number of data breaches reported in DBC dataset, by broad breach type. Data for attacks on US-based businesses only.

2. Incidence has risen sharply for medium-sized firms

back

- DBC does not contain firm size information, only the identity of the attacked firm
  - Very limited readily available data on US private firms, including on measures of size
- We rely on the *Verizon Data Breach Investigations Report (DBIR)*
  - crowdsourced dataset compiled by Verizon in a harmonised incident reporting format (VERIS)
  - incident reporting is anonymised and voluntary: tradeoff between coverage and detail

Distribution of Attacks in the DBC by Records Compromised

back

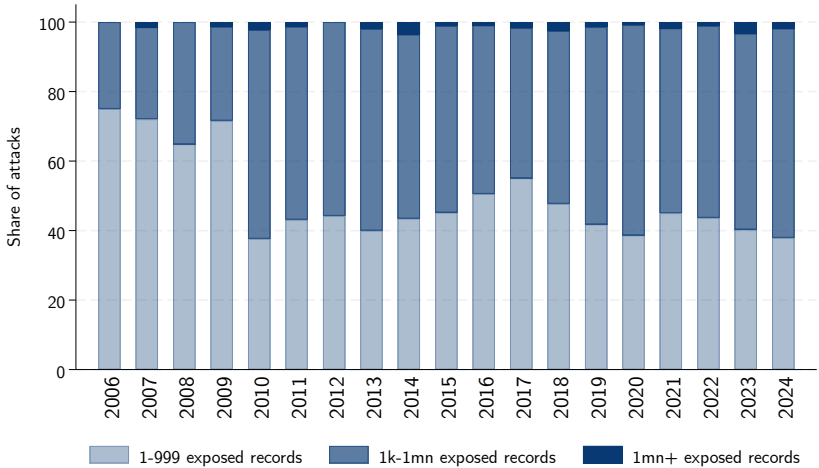


Figure: Number of data breaches reported in DBC dataset, by size category (in terms of records compromised). Data for attacks on US-based private business organisations only.

Identifying Cybersecurity Workers

back

- Our data: snapshot of LinkedIn profiles as of October 2024 for US-located jobs
- An observation: a job-spell, including information on title, employer, start and end dates
- Job spells which were active in $\geq$2000 $\implies$ annual firm-level cyber worker counts
- We rely on Revelio's detailed harmonised occupation classification (1500 distinct occs)
- We identify cyber workers whose titles contain either of the regular expressions

"{it, information, cyber, network} security"
OR
"security {analyst, architect, engineer}"

- Our choices are conservative; trends robust to alternatives (eg only use ONET 15.1212)

Share of Cybersecurity Workers by Firm Size

back

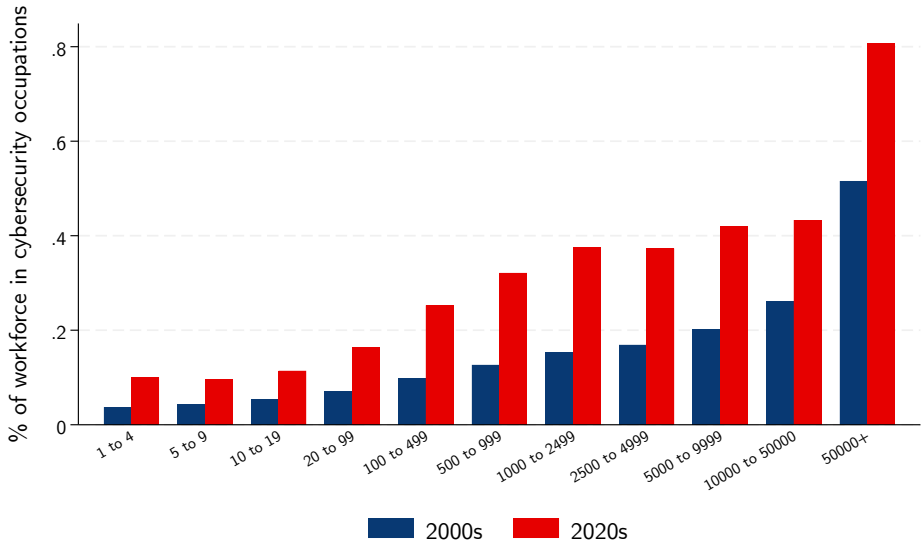
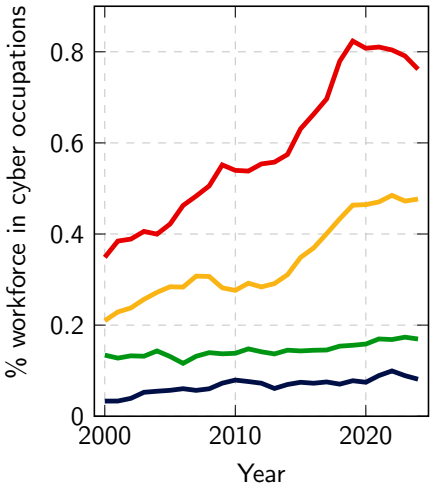
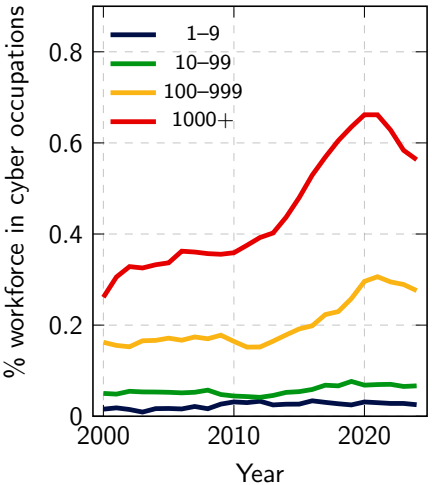


Figure: Share of workers in cybersecurity roles, by firm size category. Revelio Labs data (Oct '24 vintage). Includes only positions in the US.

Share of Cybersecurity Workers, Finance & Insurance

back





Outsourcing of cybersecurity investments, by firm size

back

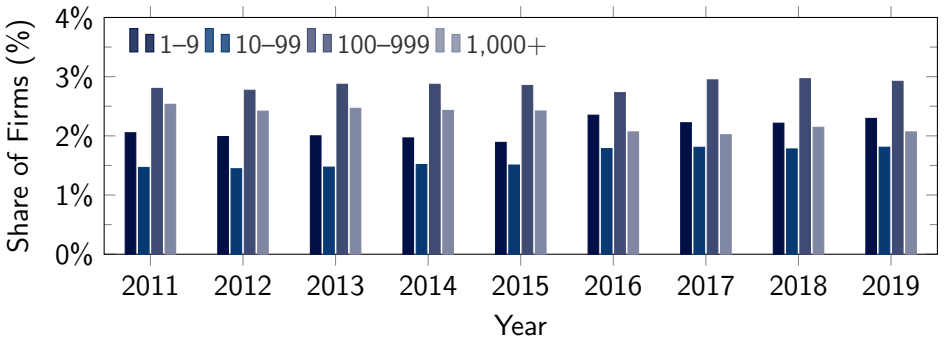


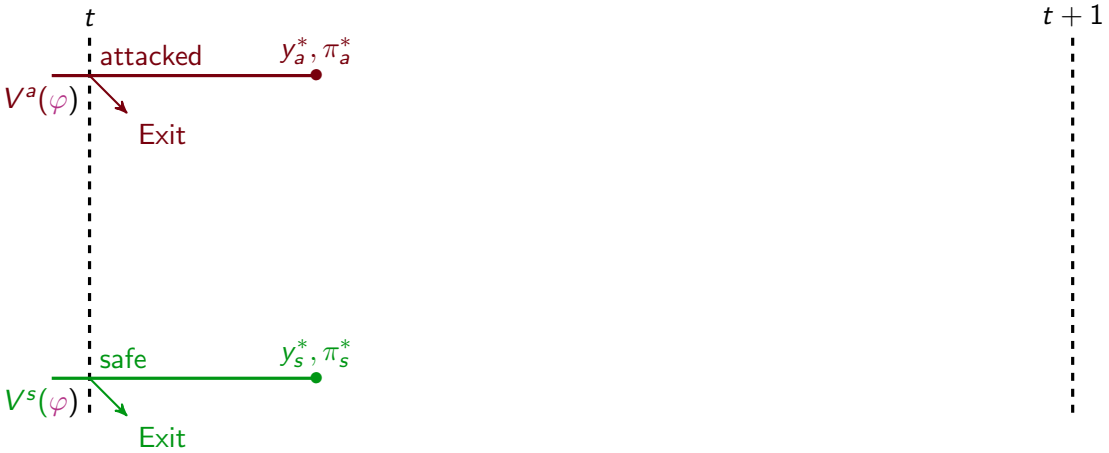
Figure: Share of establishments at firms with $\geq$ 10 employees outsourcing the maintenance of their firewalls, intrusion detection or intrusion protection systems, by firm size category. Zipf-Spiceworks-Davis-Aberdeen Computer Intelligence Technology Database, 2011-2019. Data originally collected for use in Bloom, van Reenen and Draca ('16); we sincerely thank Nick Bloom for permission to use the data.

4. Cyberattacks Are Largely Motivated by Financial Gain

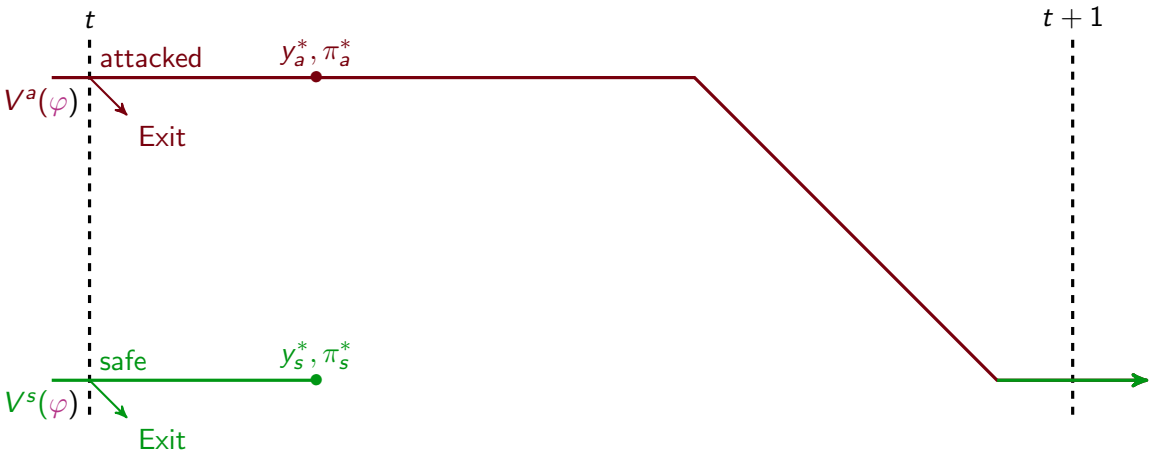
back

- DBC data don't include any information on motives
  - most attacks are anonymous, and attribution is difficult, so motives are hard to identify
- Our data: Center for International and Security Studies at Maryland
  - Data constructed by compiling information from public sources (including news reports)
  - Data contain a bias towards larger attacks, geopolitical motives, state-sponsored attackers

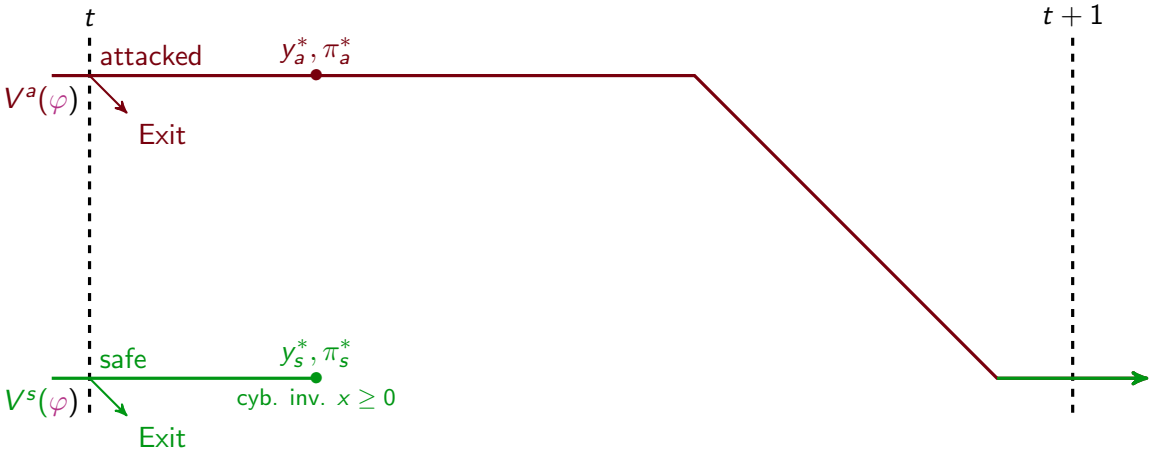
Timing of Events



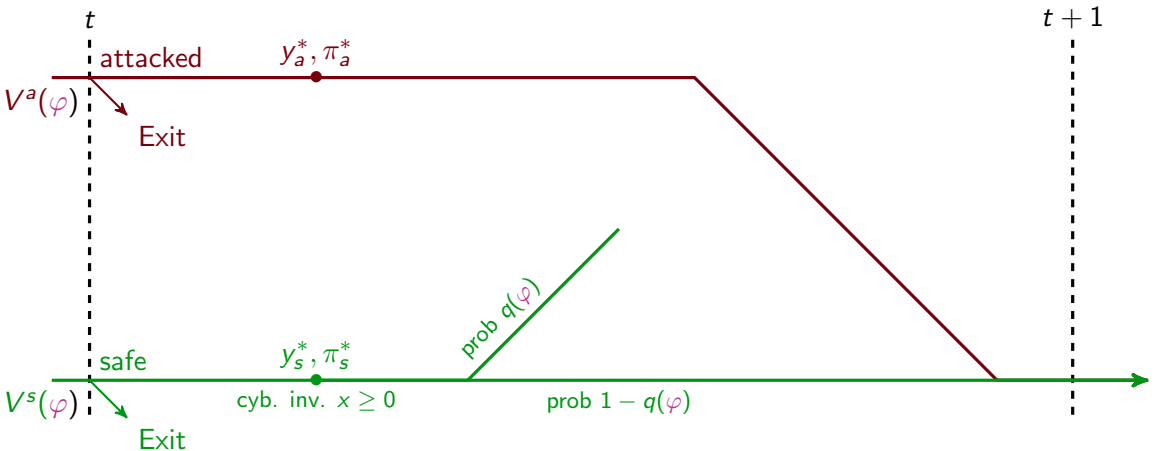
Timing of Events



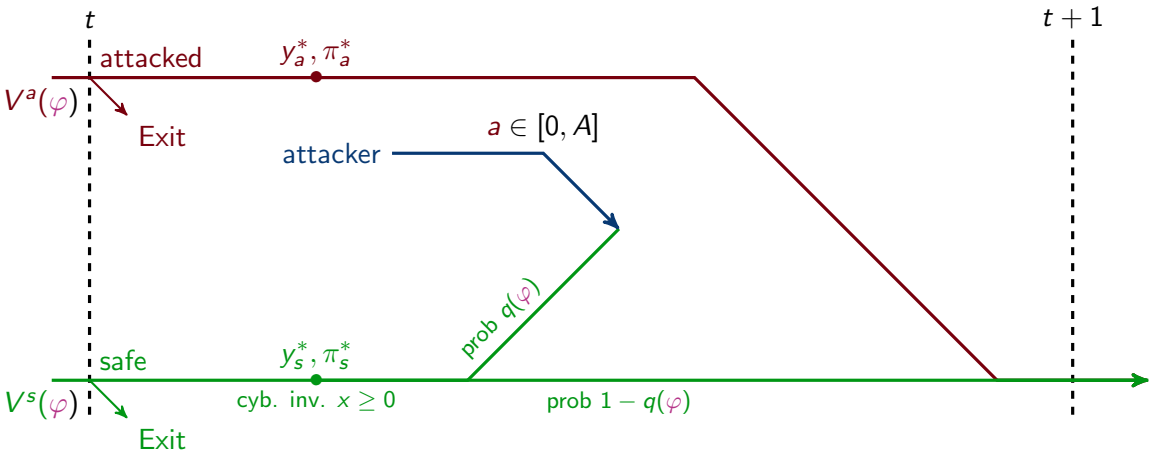
Timing of Events



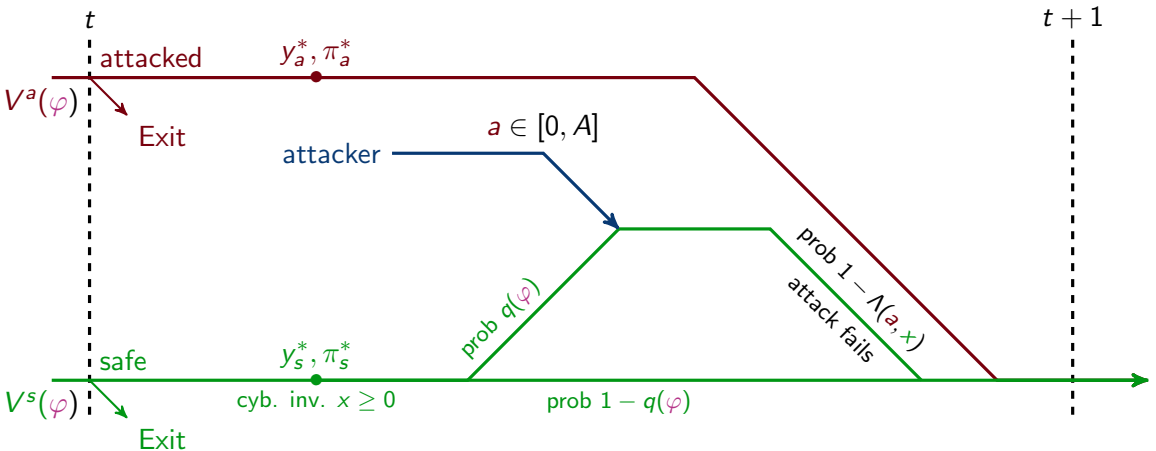
Timing of Events



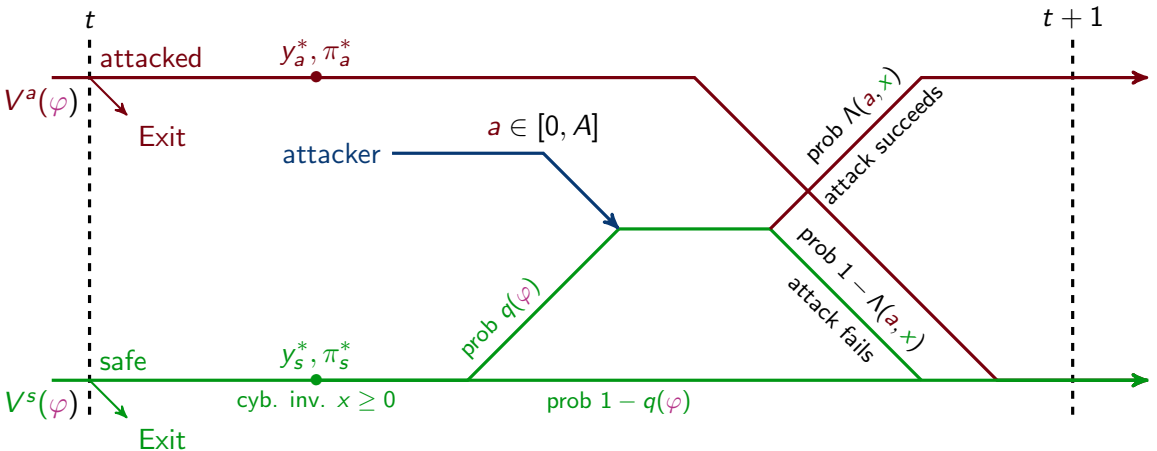
Timing of Events



Timing of Events



Timing of Events



How Attacks Work

back

- When attacker and firm meet, they each draw a random shock
  $\epsilon_a, \epsilon_f \sim$ Type I Extreme Value
- We assume that both shocks have mean 0 and common scale parameter ϱ
- The attack succeeds if $a + \epsilon_a > C(x) + \epsilon_f > 0$

$$\Lambda(a, x) = \frac{\exp\left[\frac{a - C(x)}{\varrho}\right]}{1 + \exp\left[\frac{a - C(x)}{\varrho}\right]}$$

Economic Feature	Model Ingredient

Economic Feature	Model Ingredient
▶ Firm decisions: entry/exit, profit max, cybersecurity investments	▶ Firm dynamics + cyber investment Hopenhayn '92

Economic Feature	Model Ingredient
Firm decisions: entry/exit, profit max, cybersecurity investments	Firm dynamics + cyber investment (Hopenhayn '92)
Firms choose cybersecurity before attackers choose targets, intensity	Stackelberg structure in model timing (Ebel-Mitra '22)

Economic Feature	Model Ingredient
Firm decisions: entry/exit, profit max, cybersecurity investments	Firm dynamics + cyber investment (Hopenhayn '92)
Firms choose cybersecurity before attackers choose targets, intensity	Stackelberg structure in model timing (Ebel-Mitra '22)
Attackers choose their targets, yet firms of all sizes are attacked	"Directed search and congestion": only one attacker at a time

Economic Feature	Model Ingredient
Firm decisions: entry/exit, profit max, cybersecurity investments	Firm dynamics + cyber investment (Hopenhayn '92)
Firms choose cybersecurity before attackers choose targets, intensity	Stackelberg structure in model timing (Ebel-Mitra '22)
Attackers choose their targets, yet firms of all sizes are attacked	"Directed search and congestion": only one attacker at a time
Similar attacks may succeed/fail	probabilistic attack success

Economic Feature	Model Ingredient
Firm decisions: entry/exit, profit max, cybersecurity investments	Firm dynamics + cyber investment (Hopenhayn '92)
Firms choose cybersecurity before attackers choose targets, intensity	Stackelberg structure in model timing (Ebel-Mitra '22)
Attackers choose their targets, yet firms of all sizes are attacked	"Directed search and congestion": only one attacker at a time
Similar attacks may succeed/fail	probabilistic attack success
Attacks propagate (eg via supply chains) consequences beyond attacked firm	spillovers: TFP depends on attacked share (Crosignani et al. '21)

Calibration, Step 1: Targeted Distributions

back

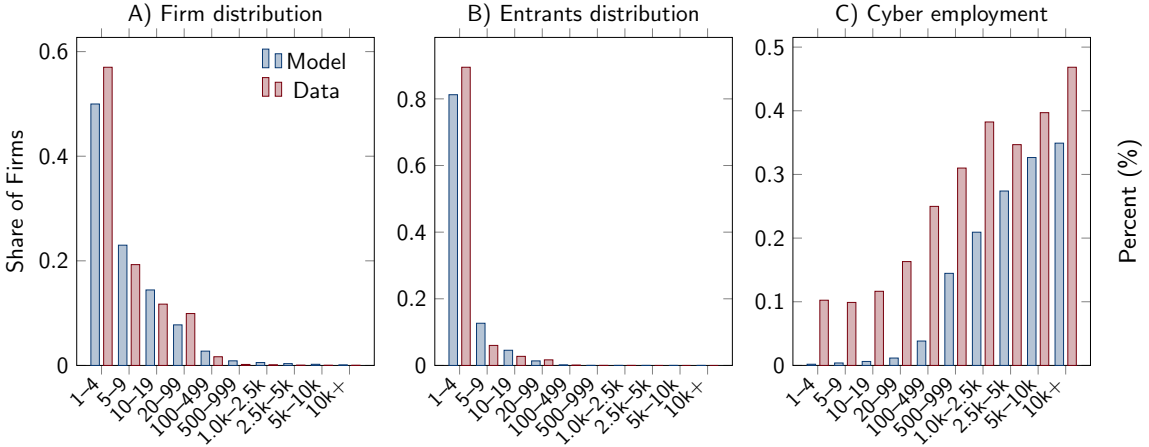


Figure: Panel A shows the firm distribution by firm size in the data (red) and the model (blue). Panel B shows the distribution of entering firms by firm size in the data (red) and the model (blue). Empirical distribution reflects the year 2000. Model represent the calibrated model without cyber-attacks. Source: Compustat and authors' analysis.

Calibration, Step 2: Targeted in Moments, Not Distributions

back

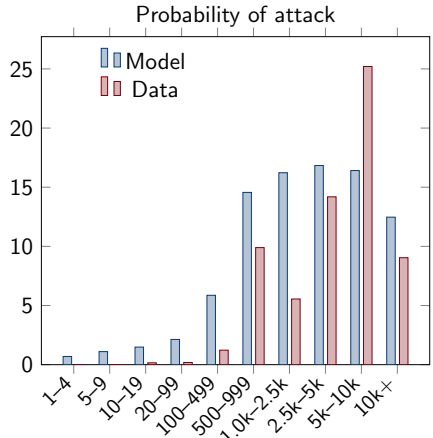


Figure: Distributional moments. Panel A shows the average cybersecurity share of employment by firm size in the data (2024 data) and the model. Panel B displays the annual probability of realised, successful attacks in model and data across the firm size distribution. Source: Business Dynamics Statistics, LinkedIn, Coveware, and authors' analysis.

Attack Probabilities, Counterfactuals

back

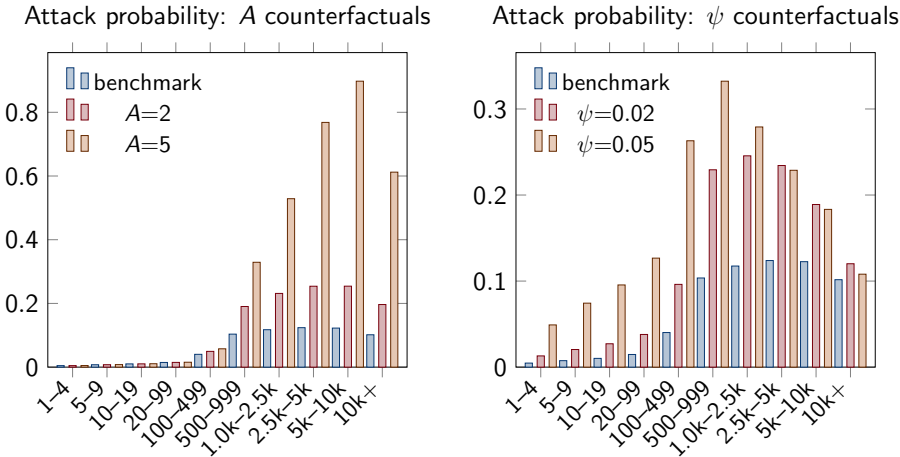


Figure: Attack success probability by firm size under changes in attacker capacity A (left) and matching efficiency ψ (right). Bars show the benchmark and two counterfactual values for each experiment.

Output Concentration, Counterfactuals

back

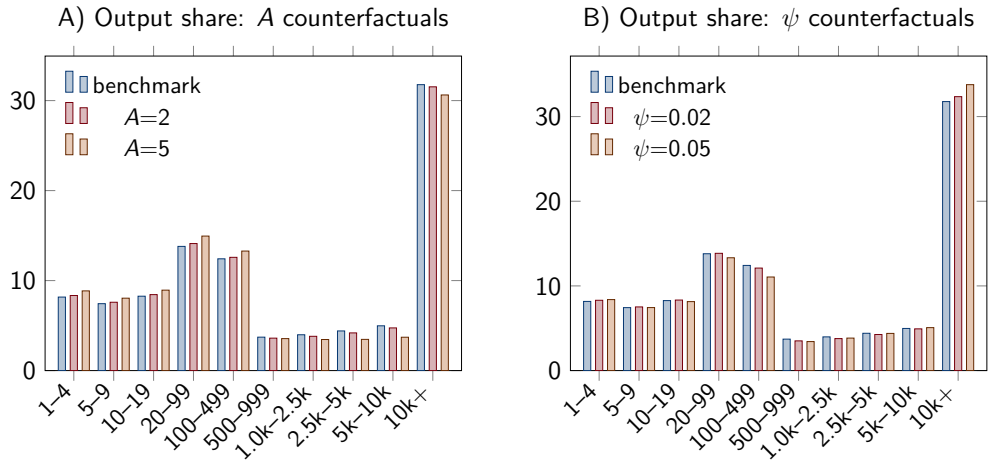


Figure: Output concentration by firm size under changes in attacker capacity A (left) and matching efficiency ψ (right). Bars show the benchmark and two counterfactual values for each experiment.

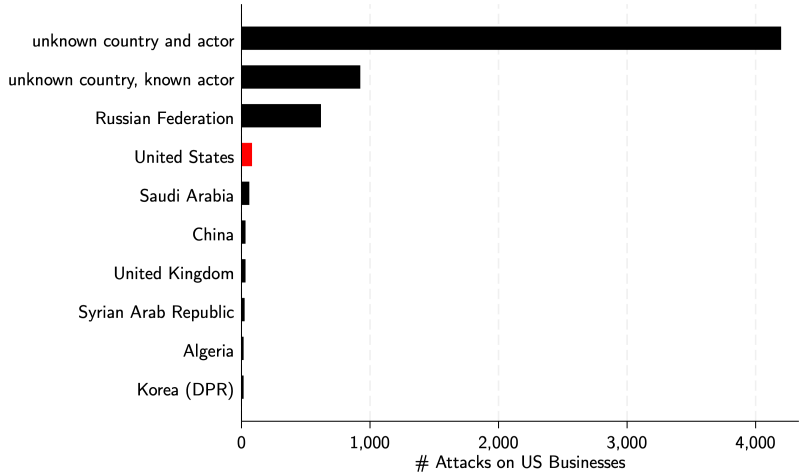
Parameters

back

	Parameter (quarterly frequency)	Value
β	Discount factor	0.96
α	Returns to scale	0.85
ϖ	Pareto distribution scale	0.7
σ	Exit probability (exogenous)	0.00
f	Per-period fixed cost of production	0.183
f_e	Fixed cost of firm entry	3.83
ρ_z	Persistence in productivity	0.925
σ_z	Stdv. of productivity innovations	0.5
ℓ	Firm loss share	0.275
χ	Attacker gain share	0.275
δ	Escape probability	1
η	Elasticity of matching function	0.35
ψ	Scaling matching function	0.01
$K(a)$	Cost of attack function	$\frac{a^{1-0.2}}{1-0.2}$
$C(x)$	Cost of security function	$0.25 \cdot \frac{x^{1-0.825}}{1-0.825}$
κ	Fixed attack cost	0.0002
ϵ_{att}	Romer externality	1.0001

Attacker Countries in the CISSM

back



Subsidies for Cybersecurity Investment

- We levy linear taxes T on all firm revenues to provide a subsidy τ for cyber investments
- Structure of the model is unchanged, except:
  - All firm revenues are scaled by $(1 - T)$, and all cyber investments are scaled by $(1 - \tau)$
  - T and τ are linked by a government budget constraint:

$$\underbrace{T \int y_s(\varphi) S(\varphi) d\varphi + T \int y_a(\varphi) \left[L(\varphi) - S(\varphi) \right] d\varphi}_{\text{government revenue}} = \underbrace{\tau w \int x^*(\varphi) S(\varphi) d\varphi}_{\text{subsidy outlays}}$$

Bailouts

- We levy linear taxes T on all firm revenues to provide a partial bailout for cyber losses ι
- Bailouts raise attacked firm revenues,

$$y_a(\varphi) = (1-\ell)\varphi n_a(\varphi)^\alpha \qquad \rightarrow \qquad \tilde{y}_a(\varphi) = (1-(1-\iota)\ell)\,\varphi \tilde{n}_a(\varphi)^\alpha$$

- Structure of the model is unchanged, except taxation + govt budget constraint:

$$\underbrace{T\int y_s(\varphi)S(\varphi)d\varphi + T\int (1-(1-\iota)\ell)\,\varphi n_a(\varphi)^\alpha\left[L(\varphi)-S(\varphi)\right]d\varphi}_{\text{government revenue}}$$

$$= \underbrace{\int \iota\ell\varphi n_a(\varphi)^\alpha\left[L(\varphi)-S(\varphi)\right]d\varphi}_{\text{bailout payments}}$$