The Economic Costs of Cyber Risk

Aniket Baksy
Daniele Caratelli

2026 Asian Meeting of the Econometric Society, June 2026

Motivation

- Cybersecurity: widespread threat, increasingly key concern for policymakers

  central banks and financial regulators, national security agencies, etc.

- Despite importance, consequences of rising cyber risk poorly understood
  - existing lit on effects of cyber risk: empirical and descriptive, focus on individual firm choices
  - nascent theory lit: incentives of firms and attackers *taking other's behavior as given*

Motivation

- Cybersecurity: widespread threat, increasingly key concern for policymakers

  central banks and financial regulators, national security agencies, etc.

- Despite importance, consequences of rising cyber risk poorly understood
  - existing lit on effects of cyber risk: empirical and descriptive, focus on individual firm choices
  - nascent theory lit: incentives of firms and attackers *taking other's behavior as given*
  - what's missing: **strategic considerations** in **general equilibrium**
    - firms can reduce exposure to cyber risk by investing in cybersecurity
    - and this, in turn, affects the incentives of *attackers* to target specific types of firms

Motivation

- Cybersecurity: widespread threat, increasingly key concern for policymakers

  central banks and financial regulators, national security agencies, etc.

- Despite importance, consequences of rising cyber risk poorly understood
  - existing lit on effects of cyber risk: empirical and descriptive, focus on individual firm choices
  - nascent theory lit: incentives of firms and attackers *taking other's behavior as given*
  - what's missing: **strategic considerations** in **general equilibrium**
    - firms can reduce exposure to cyber risk by investing in cybersecurity
    - and this, in turn, affects the incentives of *attackers* to target specific types of firms

- *This matters for the evaluation of cyber risk mitigation policies!*
  - without a GE model incorporating interactions, policy analyses subject to Lucas Critique

This Project literature

- Cyber risk: an **equilibrium outcome** of **strategic** interactions b/n firms and attackers
  - firms can reduce exposure to cyber risk by investing in cybersecurity
  - and this, in turn, affects the incentives of *attackers* to target specific types of firms
- **What we do**: **provide a framework formalising this idea**
  - tractable model with firm dynamics augmented with search/matching framework for cyber risk
  - attackers target firms of different sizes in search of bounty, which rises with firm size

This Project literature

- Cyber risk: an **equilibrium outcome** of **strategic** interactions b/n firms and attackers
  - firms can reduce exposure to cyber risk by investing in cybersecurity
  - and this, in turn, affects the incentives of *attackers* to target specific types of firms
- **What we do**: **provide a framework formalising this idea**
  - tractable model with firm dynamics augmented with search/matching framework for cyber risk
  - attackers target firms of different sizes in search of bounty, which rises with firm size
  - firms make costly cybersecurity investments to reduce likelihood of an attack succeeding

This Project literature

- Cyber risk: an **equilibrium outcome** of **strategic** interactions b/n firms and attackers
  - firms can reduce exposure to cyber risk by investing in cybersecurity
  - and this, in turn, affects the incentives of *attackers* to target specific types of firms
- **What we do**: **provide a framework formalising this idea**
  - tractable model with firm dynamics augmented with search/matching framework for cyber risk
  - attackers target firms of different sizes in search of bounty, which rises with firm size
  - firms make costly cybersecurity investments to reduce likelihood of an attack succeeding
  - reduced form modeling of spillovers from cyber risk: TFP falls with share of firms under attack
  - equilibrium: *fixed point* between attack intensities and cybersecurity investments

This Project: Counterfactuals and Policy Exercises

- **Counterfactuals**: show that GE effects critically affect implications of rising risk
  - Consider different sources for rising cyber risk: more *intense* vs more *frequent* attacks
  - Show that the two have very different implications for investments and aggregate outcomes!
    - more intense attacks $\Longrightarrow$ more cyber investments by largest firms: modest labour mkt effects
    - more frequent attacks $\Longrightarrow$ generate large spillover effects, severe labour mkt consequences

This Project: Counterfactuals and Policy Exercises

- **Counterfactuals**: show that GE effects critically affect implications of rising risk
  - Consider different sources for rising cyber risk: more *intense* vs more *frequent* attacks
  - Show that the two have very different implications for investments and aggregate outcomes!
    - more intense attacks $\implies$ more cyber investments by largest firms: modest labour mkt effects
    - more frequent attacks $\implies$ generate large spillover effects, severe labour mkt consequences
- Use model to evaluate policies *accounting for attacker responses*
  - Study two policy responses: (i) subsidies for cyber investment, (ii) bailouts for affected firms
  - Big picture: subsidise investment, don't bailout firms once attacked
  - Standard intuition: subsidies fix externalities, bailouts generate moral hazard

Cyber Risk: What You Need to Know

1. Cyber Risk Has Increased Dramatically

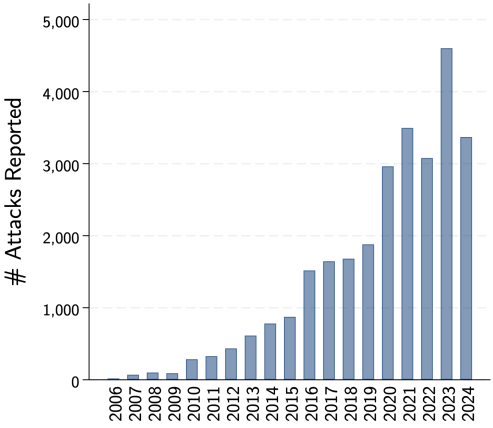


Figure: Left: number of data breaches reported in DBC dataset. Right: median size of data breaches (in terms of records compromised) in DBC dataset. Data for attacks on US-based private business organisations only. # records normalised to annual basis.

Takeaway: increases in **number** (left) since 2006.

▸ data details ▸ CISSM data ▸ All countries ▸ By org type ▸ By attack type

1. Cyber Risk Has Increased Dramatically

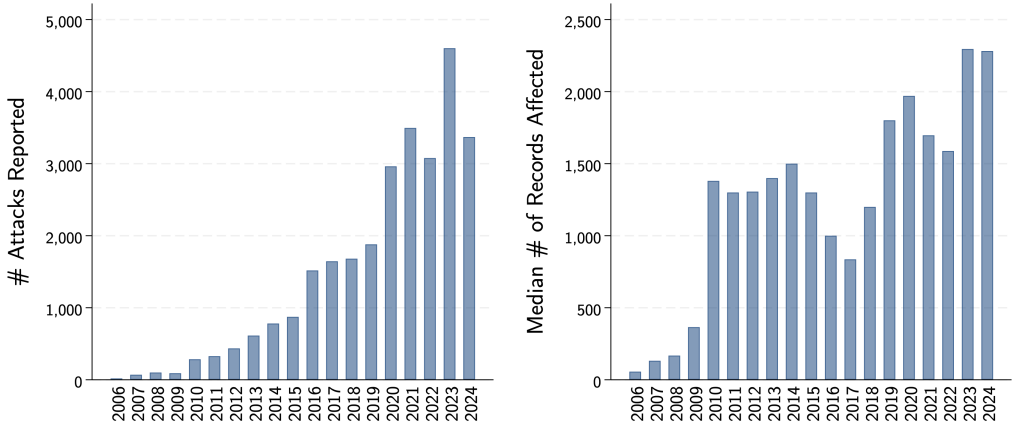


Figure: Left: number of data breaches reported in DBC dataset. Right: median size of data breaches (in terms of records compromised) in DBC dataset. Data for attacks on US-based private business organisations only. # records normalised to annual basis.

Takeaway: increases in **number** (left) and **severity** (right) of attacks since 2006.

▸ data details ▸ CISSM data ▸ All countries ▸ By org type ▸ By attack type

2. Incidence Has Risen Sharply for medium-sized firms

▸ data details ▸ dbc attack sizes

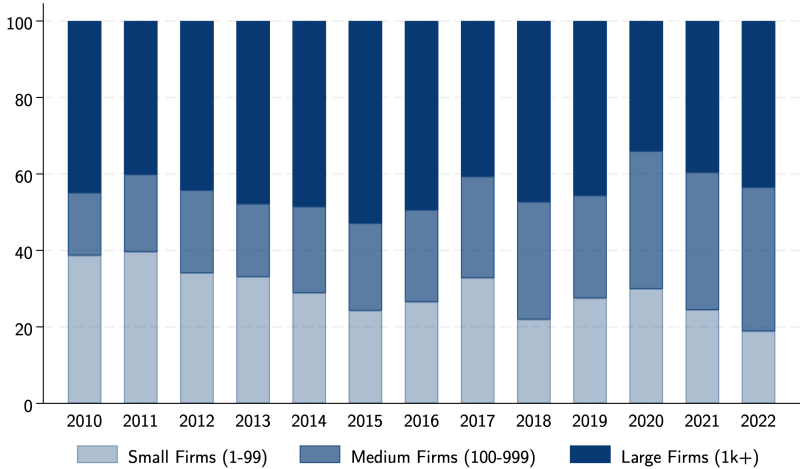


Figure: Number of data breaches reported in DBIR dataset, by firm size category. Data for attacks on US-based private business organisations only.

Takeaway: incidence of attacks risen sharply for **medium-sized** firms, 16→36% of attacks

3. Investments in Cybersecurity Scale Rapidly with Firm Size

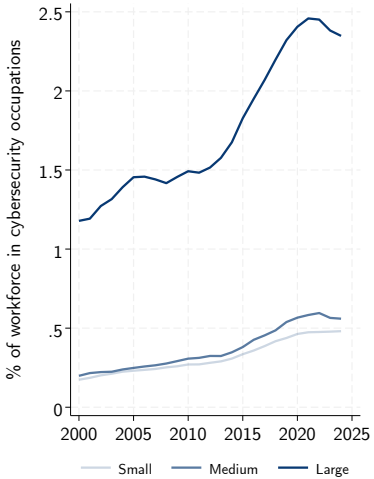


Figure: Share of workers in cybersecurity roles, by firm size category. Small, Med, Large = 1-99, 100-999, 1000+ employees. Revelio Labs data (Oct '24 vintage). Includes only positions in the US.

Variable	Share of cybersecurity-related employment		
log(EmpSize)	0.0128*** (0.0002)	0.0092*** (0.0002)	0.0167*** (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 $\geq$ 1 US employee with valid industry code & firm ID. Firm size =# employees of firm recorded in Revelio Labs data.

▸ data details ▸ detailed size category

4. Cyberattacks Are Largely Motivated by Financial Gain

data details

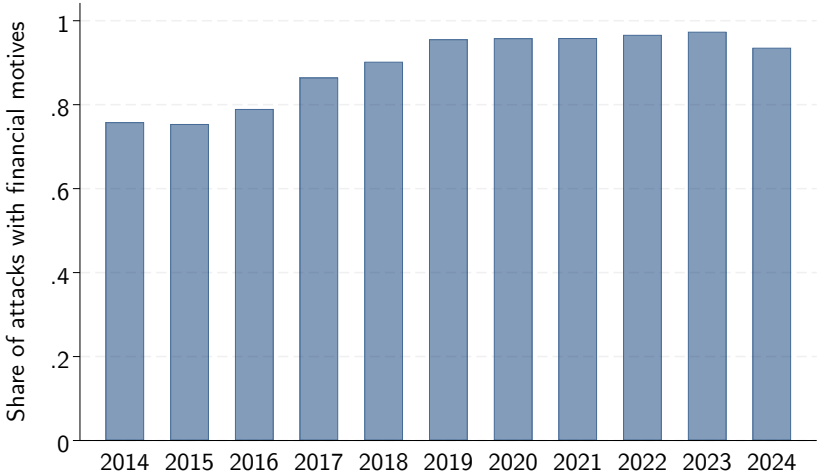


Figure: Share of attacks with financial motives, by attack type. Data from the Center for International and Security Studies at Maryland. Data for attacks on US-based private business organisations only.

5. Successful Cyberattacks Can Be Extremely Disruptive

- Shockingly little actual data on the economic consequences of cyberattacks
  - regulatory disclosures contain numbers of records compromised, but not financial losses
  - cyber events are often bundled, confounding identification using eg high-frequency methods
- The best *survey data* we are aware of: the *Cost of a Data Breach Reports*
  - annually produced by IBM and the Ponemon Institute, based on bespoke survey
  - report an annual $4.4 million average cost of a data breach (2025 report)
  - average time to identify and contain a breach: 241 days
- The best *event-based/microeconometric* work we are aware of:
  - Kamiya et al (2021): matching estimator using subset of DBC data, find effects last 1-3yrs
  - Crosignani et al (2023): study NotPetya, 4x amplification of direct losses thru' supply chain

1. Cyber risk has increased dramatically over the last 20 years
2. Incidence has risen sharply for medium-sized firms
3. Investments in cybersecurity scale rapidly with firm size
4. Cyberattacks are largely motivated by financial gain
5. Successful cyberattacks can be extremely disruptive

A Model of Cyber Attacks

Environment

- 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

- 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.
  - **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

- 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.
  - **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, choose investment in attacking that firm (attack intensity $a \geq 0$)

Environment

- 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.
    - anticipating the chance of an attack, make cybersecurity 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, choose investment in attacking that firm (attack intensity $a \geq 0$)

Environment

- 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.
    - anticipating the chance of an attack, make cybersecurity 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, choose investment in attacking that firm (attack intensity $a \geq 0$) *given cyber invt!*
- Attacks **succeed** with probability $\Lambda(a, x)$: increases in a, decreases in x ▸ func form
  - 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

Firms: Timing of Events ▸ flowchart ▸ entry/exit

- Start of period: firms observe productivity φ and predetermined cyber investment x

Firms: Timing of Events

flowchart | entry/exit

- Start of period: firms observe productivity φ and predetermined cyber investment x
- Cyberattacks occur. Modeled as a search/matching problem with firms and attackers
  - Let $L(\varphi)$ and $X(\varphi)$ be measures of firms of type φ and attackers targeting them
  - By analogy to search models: define *cyber tightness* $\theta(\varphi) \equiv L(\varphi)/X(\varphi)$
  - Assume a CRS matching function $\mathcal{M}(L, X) \implies$ contact rate $q(\varphi) = \mathcal{M}/L(\varphi) = q(\theta(\varphi))$

Firms: Timing of Events

flowchart | entry/exit

- Start of period: firms observe productivity φ and predetermined cyber investment x
- Cyberattacks occur. Modeled as a search/matching problem with firms and attackers
  - Let $L(\varphi)$ and $X(\varphi)$ be measures of firms of type φ and attackers targeting them
  - By analogy to search models: define *cyber tightness* $\theta(\varphi) \equiv L(\varphi)/X(\varphi)$
  - Assume a CRS matching function $\mathcal{M}(L, X) \implies$ contact rate $q(\varphi) = \mathcal{M}/L(\varphi) = q(\theta(\varphi))$
  - If contact occurs, attacker chooses attack intensity $a \geq 0$
  - Attack **succeeds** with probability $\Lambda(a, x)$, increasing in a, decreasing in x

Firms: Timing of Events

flowchart | entry/exit

- Start of period: firms observe productivity φ and predetermined cyber investment x
- Cyberattacks occur. Modeled as a search/matching problem with firms and attackers
  - Let $L(\varphi)$ and $X(\varphi)$ be measures of firms of type φ and attackers targeting them
  - By analogy to search models: define *cyber tightness* $\theta(\varphi) \equiv L(\varphi)/X(\varphi)$
  - Assume a CRS matching function $\mathcal{M}(L, X) \implies$ contact rate $q(\varphi) = \mathcal{M}/L(\varphi) = q(\theta(\varphi))$
  - If contact occurs, attacker chooses attack intensity $a \geq 0$
  - Attack **succeeds** with probability $\Lambda(a, x)$, increasing in a, decreasing in x
- Based on the events above, firms are hence assigned an *attack status*

Firms: Timing of Events

flowchart | entry/exit

- Start of period: firms observe productivity φ and predetermined cyber investment x
- Cyberattacks occur. Modeled as a search/matching problem with firms and attackers
  - Let $L(\varphi)$ and $X(\varphi)$ be measures of firms of type φ and attackers targeting them
  - By analogy to search models: define *cyber tightness* $\theta(\varphi) \equiv L(\varphi)/X(\varphi)$
  - Assume a CRS matching function $\mathcal{M}(L, X) \implies$ contact rate $q(\varphi) = \mathcal{M}/L(\varphi) = q(\theta(\varphi))$
  - If contact occurs, attacker chooses attack intensity $a \geq 0$
  - Attack **succeeds** with probability $\Lambda(a, x)$, increasing in a, decreasing in x
- Based on the events above, firms are hence assigned an *attack status*
  - no matches, or matched + failed attack: safe firms, value $V^s(\varphi)$. Mass $S(\varphi)$.

Firms: Timing of Events

flowchart | entry/exit

- Start of period: firms observe productivity φ and predetermined cyber investment x
- Cyberattacks occur. Modeled as a search/matching problem with firms and attackers
  - Let $L(\varphi)$ and $X(\varphi)$ be measures of firms of type φ and attackers targeting them
  - By analogy to search models: define *cyber tightness* $\theta(\varphi) \equiv L(\varphi)/X(\varphi)$
  - Assume a CRS matching function $\mathcal{M}(L, X) \implies$ contact rate $q(\varphi) = \mathcal{M}/L(\varphi) = q(\theta(\varphi))$
  - If contact occurs, attacker chooses attack intensity $a \geq 0$
  - Attack **succeeds** with probability $\Lambda(a, x)$, increasing in a, decreasing in x
- Based on the events above, firms are hence assigned an *attack status*
  - no matches, or matched + failed attack: safe firms, value $V^s(\varphi)$. Mass $S(\varphi)$.
  - matched + successful attack: attacked firms, value $V^a(\varphi)$. Mass $A(\varphi)$.

Firms: Timing of Events

flowchart | entry/exit

- Start of period: firms observe productivity φ and predetermined cyber investment x
- Cyberattacks occur. Modeled as a search/matching problem with firms and attackers
  - Let $L(\varphi)$ and $X(\varphi)$ be measures of firms of type φ and attackers targeting them
  - By analogy to search models: define *cyber tightness* $\theta(\varphi) \equiv L(\varphi)/X(\varphi)$
  - Assume a CRS matching function $\mathcal{M}(L, X) \implies$ contact rate $q(\varphi) = \mathcal{M}/L(\varphi) = q(\theta(\varphi))$
  - If contact occurs, attacker chooses attack intensity $a \geq 0$
  - Attack **succeeds** with probability $\Lambda(a, x)$, increasing in a, decreasing in x
- Based on the events above, firms are hence assigned an *attack status*
  - no matches, or matched + failed attack: safe firms, value $V^s(\varphi)$. Mass $S(\varphi)$.
  - matched + successful attack: attacked firms, value $V^a(\varphi)$. Mass $A(\varphi)$.
  - given attack status, choose exit/stay, labour n, and (if safe) cyber investment x for next period

Safe Firms

$$V^s(\varphi) = \max \left\{ \underbrace{\mathbf{0}}_{\text{Exit}} \quad , \quad \max_{n,x \geq 0} \underbrace{\varphi n^\alpha - wn - f}_{\text{Flow Profits}} - \underbrace{wx}_{\text{Cyber Investment}} + \beta \mathbb{E}_{\varphi'|\varphi} \left[\underbrace{q(\varphi') V^m(\varphi', x)}_{\text{meets an attacker}} + \underbrace{(1 - q(\varphi')) V^s(\varphi')}_{\text{no meetings with attackers}} \right] \right\}$$

- Safe Firms choose labour n and cyber investments $x \geq 0$
  - Choice of n is still static; we'll denote this $n_s^*(\varphi)$. Corresponding output, profits $y_s^*(\varphi), \pi_s^*(\varphi)$
- $q(\varphi')$ is the probability that a firm of productivity φ' meets an attacker
- $V^m(\varphi', x)$ is the value of being matched to an attacker in the next period
- Let $x^*(\varphi)$ be the firm's policy function for cyber investment

Attacked Firms

$$V^a(\varphi) = \max\left\{ \underbrace{\mathbf{0}}_{\text{Exit}} \quad , \quad \max_{n \geq 0} \underbrace{(1-\ell)\varphi n^\alpha - wn - f}_{\text{Flow Profits}} + \beta \underbrace{\mathbb{E}_{\varphi'|\varphi}\left[V^s(\varphi')\right]}_{\text{Return to Safe Status}} \right\}$$

- Attacked firm faces a one-period reduction in productivity by a factor of $\ell \in (0,1)$
  - Choice of n is static; we'll denote this $n_a^*(\varphi)$. Corresponding output, profits $y_a^*(\varphi), \pi_a^*(\varphi)$
- Return to safe status after one period

The value of meeting an attacker

$$V^m(\varphi, x) = \underbrace{\Lambda(a^*(x,\varphi), x) \cdot V^a(\varphi)}_{\text{Successful Attack}} + \underbrace{(1 - \Lambda(a^*(x,\varphi), x)) \cdot V^s(\varphi)}_{\text{Unsuccessful Attack}}$$

- When an attacker and firm meet, the attack succeeds with probability $\Lambda(a^*(x,\varphi), x)$
- This probability depends both on
  - cybersecurity investment x chosen by a firm of type φ
  - attack intensity $a^*(x,\varphi)$ chosen by attacker when targeting a firm with security investment x
- x predetermined: firms choose it *taking attack intensity schedule* $a^*(x,\varphi)$ *into account!*
  - Behave like a Stackelberg leader

Gordon-Loeb '02, Ebel-Mitra '24

The economics of cybersecurity investment

$$\underbrace{w}_{\substack{\text{marginal cost}\\ \text{of}\\ \text{cyber investments}}} = \beta \mathbb{E}_{\varphi'|\varphi} \left[\underbrace{q(\varphi')}_{\substack{\text{contact rate}\\ \text{with attackers}}} \times \underbrace{\frac{\mathbf{d}\Lambda(a^*(x,\varphi),x)}{\mathbf{d}x}}_{\substack{\text{“Total” sensitivity}\\ \text{of } \Lambda \text{ to } x}} \times \underbrace{\left\{ V^s(\varphi') - V^a(\varphi') \right\}}_{\substack{\text{extent of loss}\\ \text{from a}\\ \text{successful attack}}} \right]$$

Attackers

- Each period, a large number of attackers start out as *unmatched*.
  - unmatched attackers can spend κ units of goods to gain *attack capacity* $A > 0$
  - Choose which firm types φ to target, meeting such a firm with probability $\lambda(\varphi)$
  - Upon meeting, choose attack intensity $a \in [0, A]$ to max prob of a successful attack net of costs
  - Attackers know the investment schedule $x^*(\varphi)$ when choosing attack intensity

Attackers

- Each period, a large number of attackers start out as *unmatched*.
  - unmatched attackers can spend κ units of goods to gain *attack capacity* $A > 0$
  - Choose which firm types φ to target, meeting such a firm with probability $\lambda(\varphi)$
  - Upon meeting, choose attack intensity $a \in [0, A]$ to max prob of a successful attack net of costs
  - Attackers know the investment schedule $x^*(\varphi)$ when choosing attack intensity
- Free entry into attacking implies that for all firm types φ,

$$\kappa \geq \lambda(\varphi) \cdot \left[\max_{a \in [0,A]} \left\{ -a + \underbrace{\Lambda(a, x) \cdot \zeta(\varphi) \cdot \ell \varphi n^{\alpha}}_{\text{Successful Attack}} + \underbrace{(1 - \Lambda(a, x)) \cdot 0}_{\text{Unsuccessful Attack}} \right\} \right]$$

  - $\zeta(\varphi)$: indicator for whether a firm of type φ chooses to stay upon being attacked
  - $\ell \varphi n^{\alpha}$ is the flow payoff to a successful attack: a share ℓ of firm revenues

Equilibrium details

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

- $a^*(x), x^*(\varphi)$ are best responses in the Stackelberg game b/n firms, attackers
- All markets clear, stationary distbns of firms consistent with policies and transition laws

Taking Stock

- We've built a dynamic GE model of cyber risk with firm heterogeneity φ
  - directed attacks with attack intensity a & cybersecurity investments x
- In equilibrium, attack intensities and cyber investments satisfy a fixed point
  - attackers choose attack intensities knowing the cyber investments of firms
  - firms φ know the prob of an attack $q(\varphi)$ and the intensity $a^*(x, \varphi)$ of attacks they'll face
  - as Stackelberg leaders, choose cyber invt x knowing attackers will take them into account

Taking Stock

- We've built a dynamic GE model of cyber risk with firm heterogeneity φ
  - directed attacks with attack intensity a & cybersecurity investments x
- In equilibrium, attack intensities and cyber investments satisfy a fixed point
  - attackers choose attack intensities knowing the cyber investments of firms
  - firms φ know the prob of an attack $q(\varphi)$ and the intensity $a^*(x, \varphi)$ of attacks they'll face
  - as Stackelberg leaders, choose cyber invt x knowing attackers will take them into account
- Two extensions we add to the model before we can quantify it:
  - exogenous exit shocks, effectively reducing firm patience
  - reduced form TFP spillovers: agg productivity given by $Z = \left[\int S(\varphi)d\varphi / \int L(\varphi)d\varphi\right]^{\epsilon}$

Quantification

Quantification

▸ parameters ▸ calibration step 1 ▸ calibration step 2

1. "No Cyber Equilibrium" AD 2000-04. We set $\ell = 0$ (no losses/bounty)
   - Key params: productivity process, entry and fixed operating costs, entrant TFP distbn
   - Target firm size distbn, entrant size distbn, exit rates

Quantification

▸ parameters ▸ calibration step 1 ▸ calibration step 2

1. "No Cyber Equilibrium" AD 2000-04. We set $\ell = 0$ (no losses/bounty)
   - Key params: productivity process, entry and fixed operating costs, entrant TFP distbn
   - Target firm size distbn, entrant size distbn, exit rates
2. "Cyber Equilibrium" AD 2020-24. Fix stage 1 params, choose cyber-related params:
   - 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

Quantification

▸ parameters ▸ calibration step 1 ▸ calibration step 2

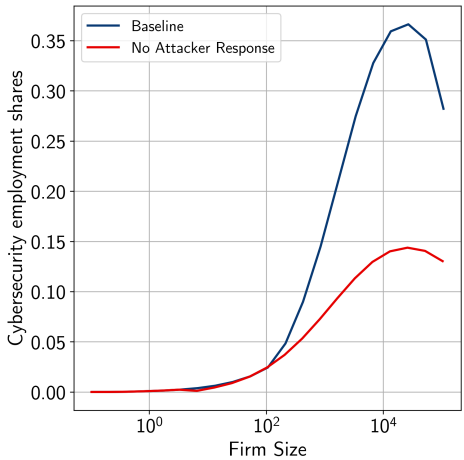
1. "No Cyber Equilibrium" AD 2000-04. We set $\ell = 0$ (no losses/bounty)
   - Key params: productivity process, entry and fixed operating costs, entrant TFP distbn
   - Target firm size distbn, entrant size distbn, exit rates
2. "Cyber Equilibrium" AD 2020-24. Fix stage 1 params, choose cyber-related params:
   - 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

- Comparing the two equilibria allows us to quantify the costs of cyber risk
  - attacks lead to higher exit and lower entry rates, reducing mass of firms by 3.6%
  - about 0.6% lower TFP, due to spillovers, further reducing labour demand
  - overall, aggregate output is about 1.8% lower, wages about 1.6% lower

Counterfactuals

Counterfactuals, Part 1: 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, Part 2: The Source of Rising Cyber Risk Matters!

- **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
- **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

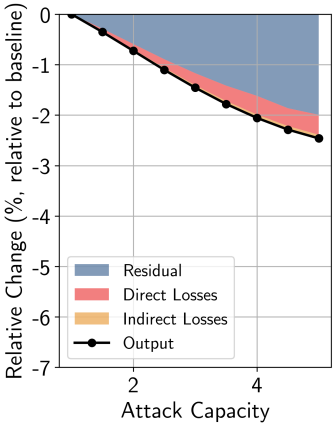
$$\Delta Y = \underbrace{\Delta Y^{direct}}_{\text{Direct Losses}} + \underbrace{\Delta Y^{indirect}}_{\text{Indirect Losses}} + \underbrace{\Delta Y^{Residual}}_{\text{Residual Change}}$$

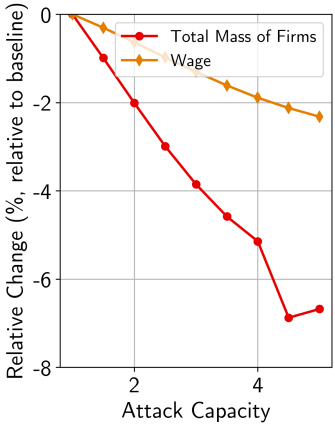
Counterfactuals, Part 2: The Source of Rising Cyber Risk Matters!

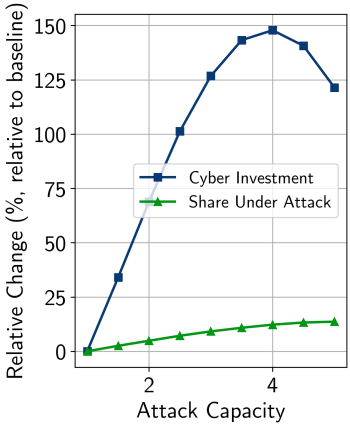
- **Our goal**: show that GE effects emphasized affect the economics of rising cyber risk
  - We consider two shocks that raise the level of cyber risk in the economy
  - capture plausible forms of technological change that favour attackers
- **Our approach**: solve for the model's steady state under 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

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

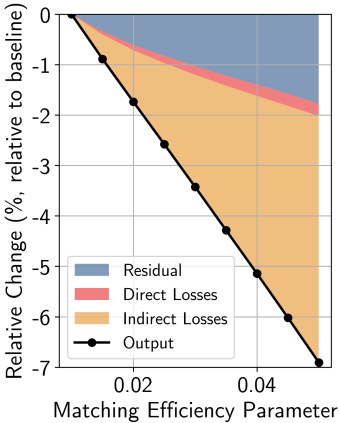
Higher Attack Capacity has modest effects

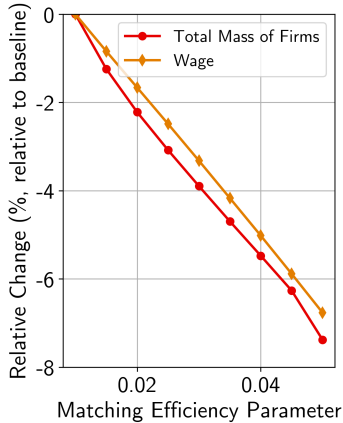


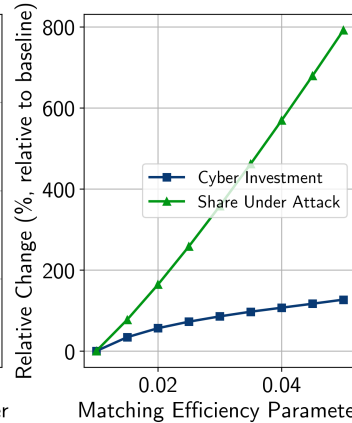




Higher Matching Rates have drastic consequences







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*
  - Leads to weaker entry incentives and higher cyber investments among incumbents

- 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*
  - Leads to weaker entry incentives and higher cyber investments among incumbents
  - These higher investments mean that overall, the share of attacked firms rises, but modestly

- 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*
  - Leads to weaker entry incentives and higher cyber investments among incumbents
  - These higher investments mean that overall, the share of attacked firms rises, but modestly

- 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*
  - Leads to weaker entry incentives and higher cyber investments among incumbents
  - These higher investments mean that overall, the share of attacked firms rises, but modestly

- 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*
  - Leads to weaker entry incentives and higher cyber investments among incumbents
  - These higher investments mean that overall, the share of attacked firms rises, but modestly

- 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*
  - Leads to weaker entry incentives and higher cyber investments among incumbents
  - These higher investments mean that overall, the share of attacked firms rises, but modestly
  - 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

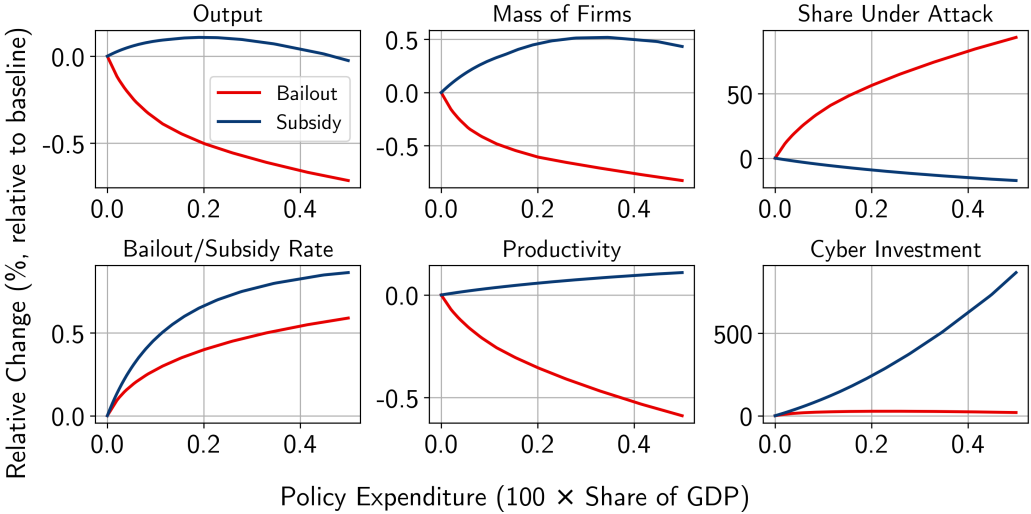
Policy Exercises

How should we respond to rising cyber risk?

- We evaluate two policy responses to rising cyber risk:
  - Bailouts for affected firms details
    - government finances a constant fraction ι of direct losses for attacked firms
    - effectively reduces proportional loss from attack from $1 - \ell$ to $1 - \ell(1 - \iota)$
  - Subsidies for cybersecurity investment details
    - government pays for a share τ of firms' cyber investments
    - effectively reduces cost of cyber investment from wx to $(1 - \tau)wx$
- Financed by proportional revenue taxes on all firms; impose budget neutrality

Subsidies are More Effective than Bailouts!

state-contingency



Why do Subsidies Outperform Bailouts?

- Subsidies directly incentivise cyber investments, reducing ex-post likelihood of attacks
  - reduces the expected profitability of attacking, leading to fewer attackers in the first place
  - firm entry becomes more attractive $\implies$ more firms; lower attacked share $\implies$ lower spillovers
  - due to effects of spillovers, output initially increases relative to benchmark!
  - eventually (at subsidy rate $\approx 65\% \equiv$ tax/GDP of $\approx 20\%$), distortionary taxation dominates
- Bailouts, by contrast, generate moral hazard - *especially for the largest firms*
  - small firms don't benefit from bailouts but are hurt by taxes, leading to exit and lower entry
  - large firms benefit from bailouts, reducing cyber investments and raising risk exposures
  - massive increase in share of firms under attack leads to large spillover-driven losses

Conclusion

- We develop a model of the interactions between firms and cyberattackers
- We show that accounting for strategic interactions between firms and attackers is crucial for understanding the economic consequences of rising cyber risk
- We evaluate two policy responses to rising cyber risk:
  - subsidies for cybersecurity investment (policymakers in audience: do this)
  - bailouts for affected firms (policymakers in audience: don't do this)
- TO DO: *Lots of further work!*
  - Detailed microfoundations for spillovers from cyber risk
  - In general, superior microdata collection on cyber risk exposure and consequences

Appendix

Our Contribution back

1. **Cyber risk and its economic consequences:** 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)
   - Micro 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
  - Our findings: cyber risk accounts for about 3.6% lower TFP and 1.8% lower output
  - Policy: subsidise cyber investment, don't bailout firms once attacked

1. Cyber Risk Has Increased Dramatically

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 since 2005, a nonprofit research group
  - 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

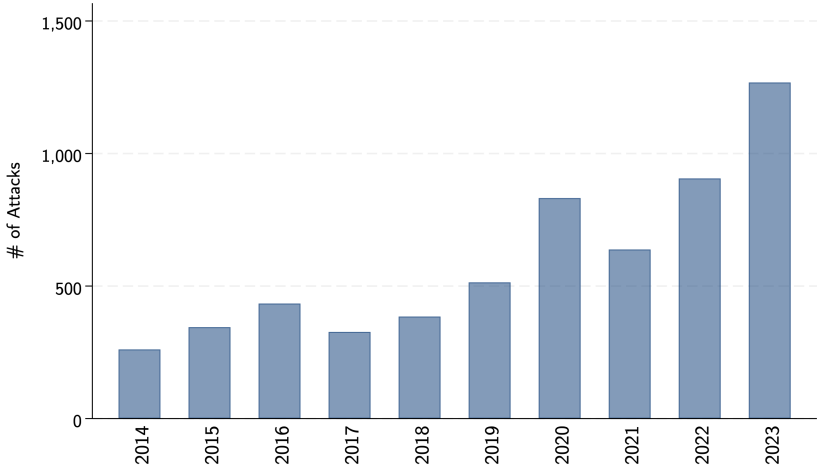


Figure: Number of cyberattacks reported to the Center for International and Security Studies in Maryland, 2014-2023. Data for attacks on US-based private business organisations only.

The Rising Number of Attacks: DBC Data, All Countries

back

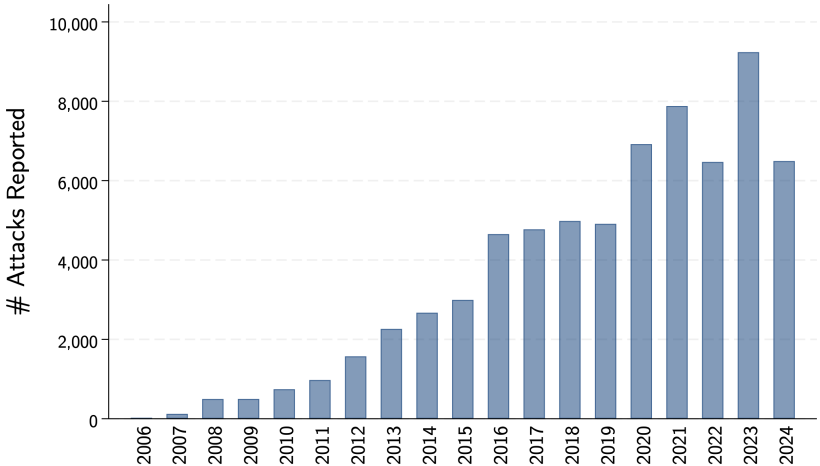


Figure: Number of data breaches reported in DBC dataset. Data for attacks on private business organisations only.

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

back

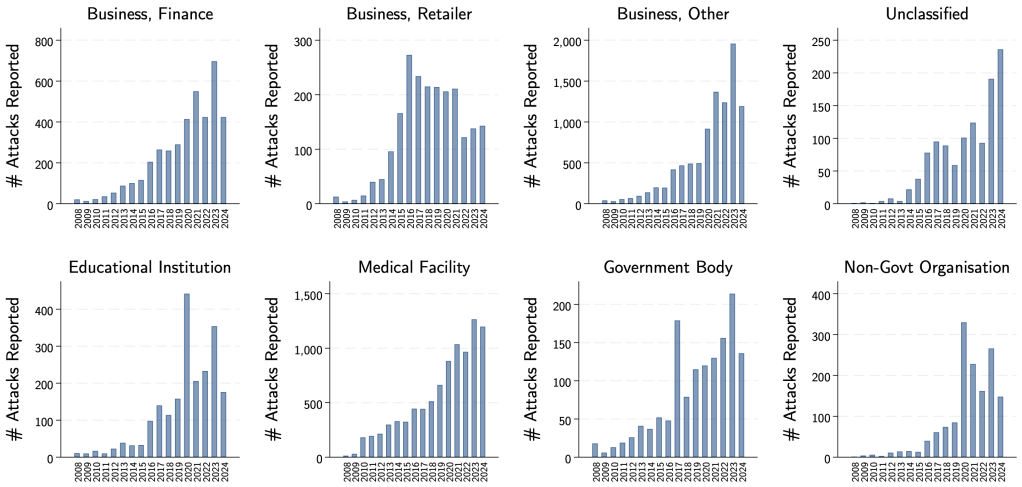


Figure: Number of data breaches reported in DBC dataset, by organization type. Data for attacks on US-based businesses only.

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

back

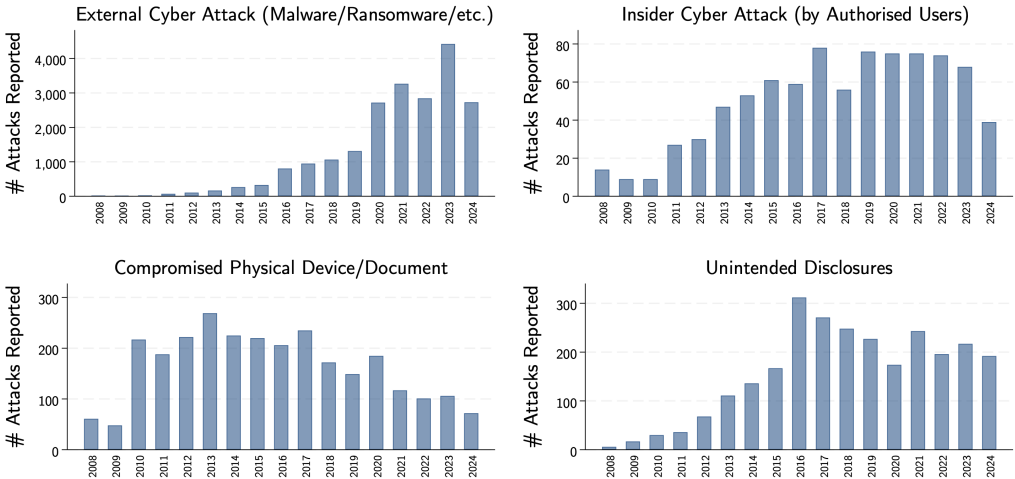


Figure: Number of data breaches reported in DBC dataset, by broad breach type. Data for attacks on US-based businesses only.

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

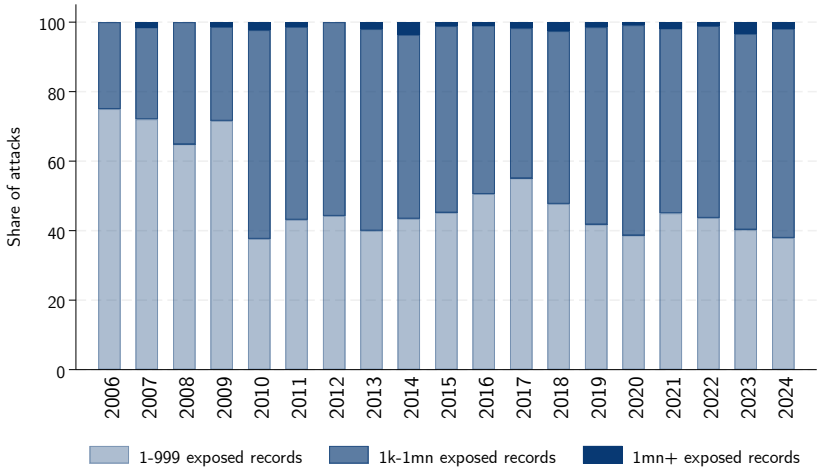


Figure: Number of data breaches reported in DBC dataset, by size category (in terms of records compromised). Data for attacks on US-based private business organisations only.

3. Investments in Cybersecurity Scale Rapidly with Firm Size

back

- No publicly available data on cybersecurity investments or 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

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

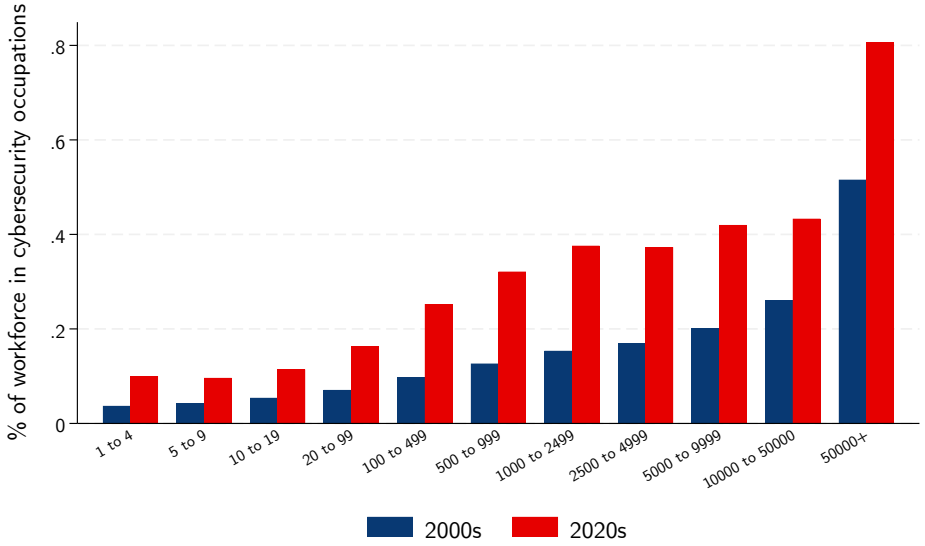


Figure: Share of workers in cybersecurity roles, by firm size category. Revelio Labs data (Oct '24 vintage). Includes only positions in the US.

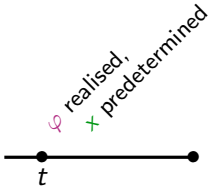
4. Cyberattacks Are Largely Motivated by Financial Gain

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

back



- start period with predetermined cyber investment x, observe productivity φ

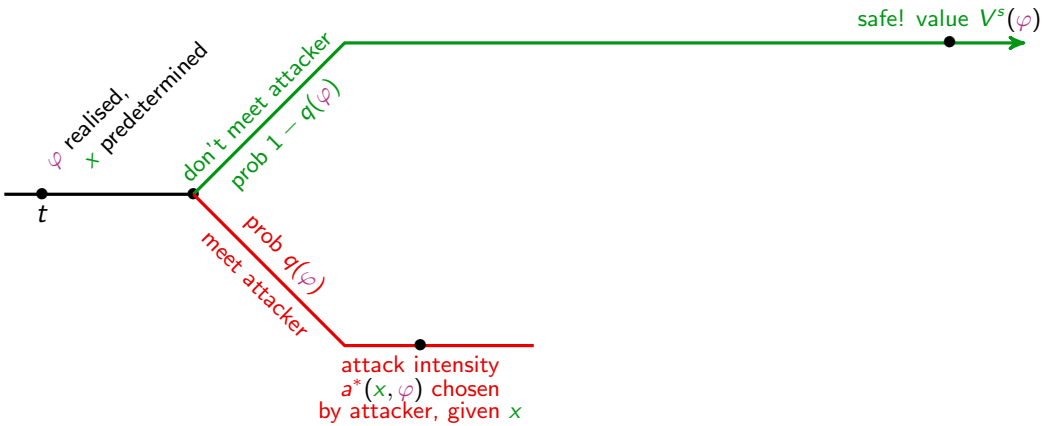
Timing of Events

back

- with probability $1 - q(\varphi)$, don't match with an attacker $\implies$ *safe*, $V^s(\varphi)$

Timing of Events

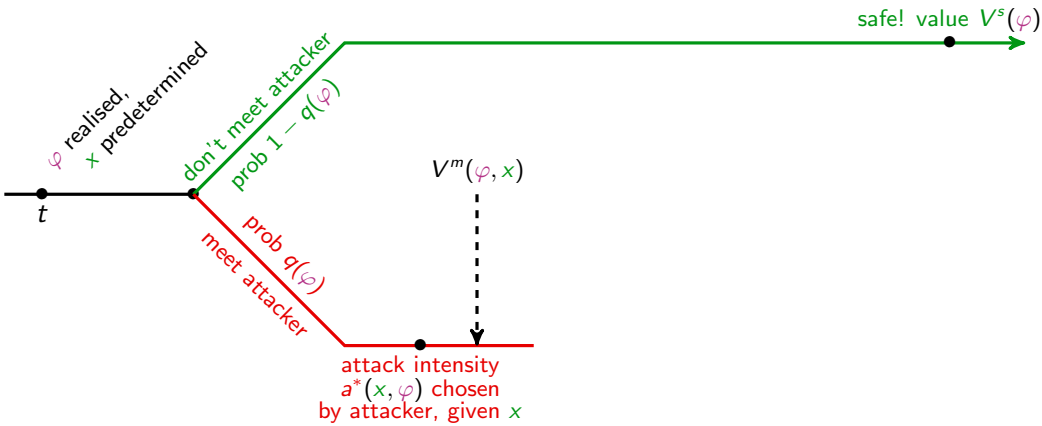
back



- with probability $q(\varphi)$, match with an attacker who chooses attack intensity $a^*(x,\varphi)$

Timing of Events

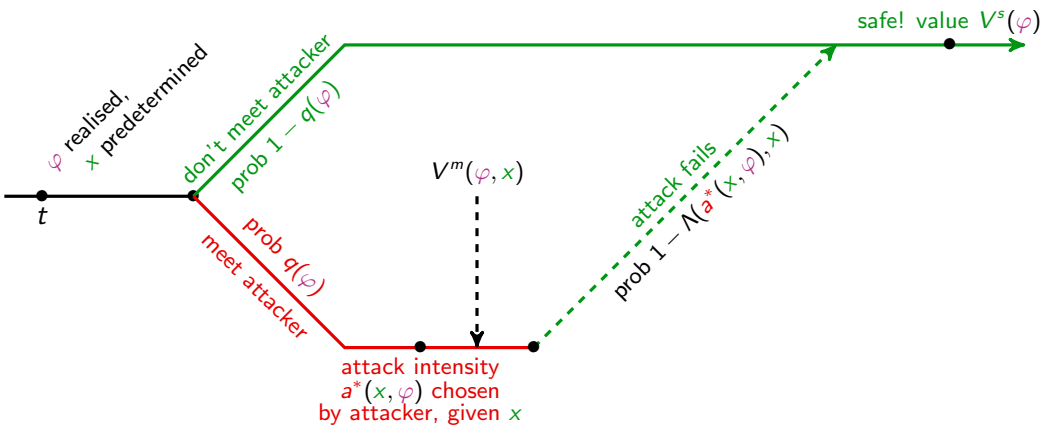
back



- value of firm matched to an attacker, taking choice $a^*(x, \varphi)$ into account: $V^m(\varphi, x)$

Timing of Events

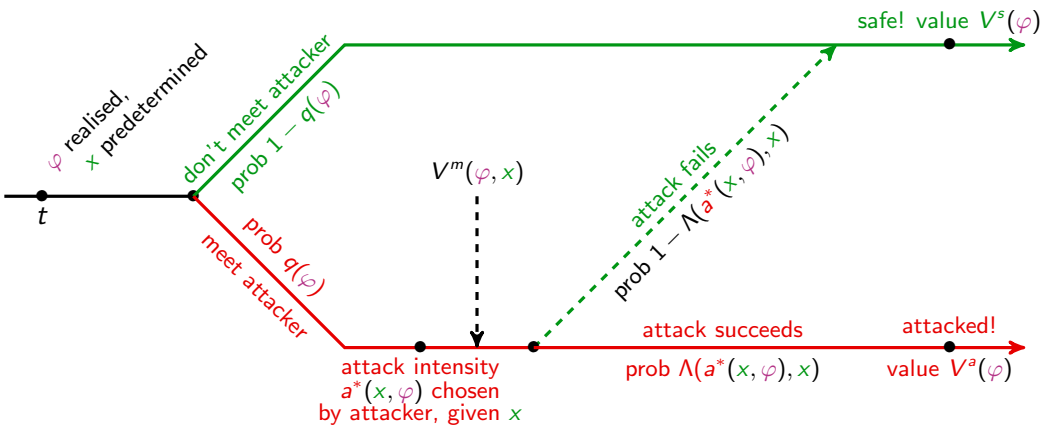
back



- Attack fails with prob $1-\Lambda(a^*(x,\varphi),x)$: return to safe status, value $V^s(\varphi)$

Timing of Events

back



- Attack succeeds with prob $\Lambda(a^*(x,\varphi),x)$: under attack for 1 period, safe tomorrow

How Attacks Work

back

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

- 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 $a + \epsilon_a > C(x) + \epsilon_f > 0$

Firms: Entry and Exit back

- We allow for entry/exit in an extremely standard way:
  - Each period, a large mass of potential entrants can pay a fixed entry cost f_e to draw $\varphi \sim G(\cdot)$
  - After drawing φ, decide whether to enter or not
  - We assume that entering firms always enter as safe firms, produce in period of entry
- Free entry by firms requires that

$$f_e \geq \int \max\{\mathbf{0}, V^s(\varphi)\}\, dG(\varphi)$$

Equilibrium details

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

back

1. 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 back

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

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

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

back

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.

Calibration, Step 1: Targeted Distributions

back

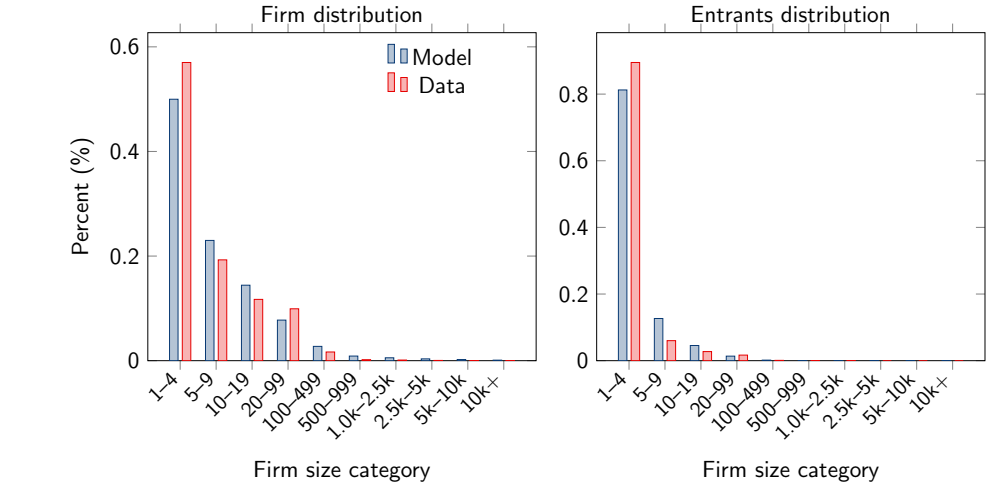


Figure: Panel A shows the firm distribution by firm size in the data (red) and the model (blue). Panel B shows the distribution of entering firms by firm size in the data (red) and the model (blue). Empirical distribution reflects the year 2000. Model represent the calibrated model without cyber-attacks.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

Calibration, Step 2: Targeted in Moments, Not Distributions

back

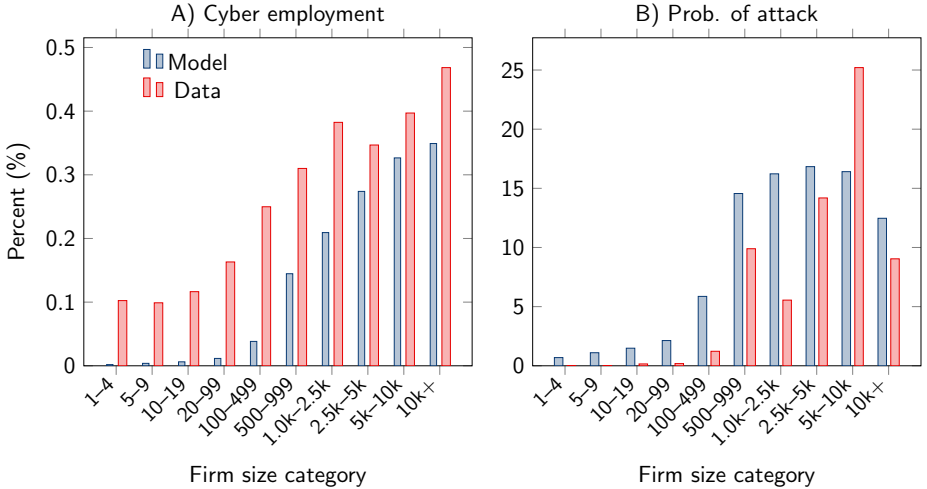


Figure: Distributional moments. Panel A shows the average cybersecurity share of employment by firm size in the data (2024 data) and the model. Panel B displays the annual probability of realised, successful attacks in model and data across the firm size distribution. Source: Business Dynamics Statistics,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

Attack Probabilities, Counterfactuals

back

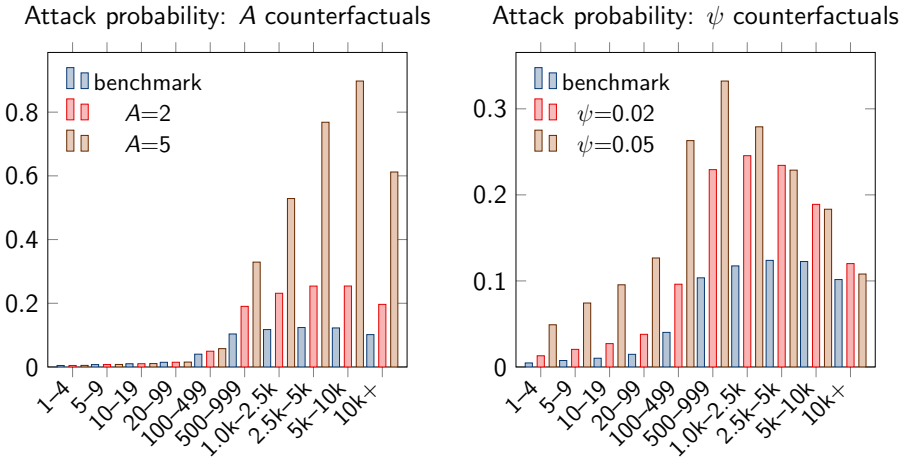


Figure: Attack success probability by firm size under changes in attacker capacity A (left) and matching efficiency ψ (right). Bars show the benchmark and two counterfactual values for each experiment.

Output Concentration, Counterfactuals

back

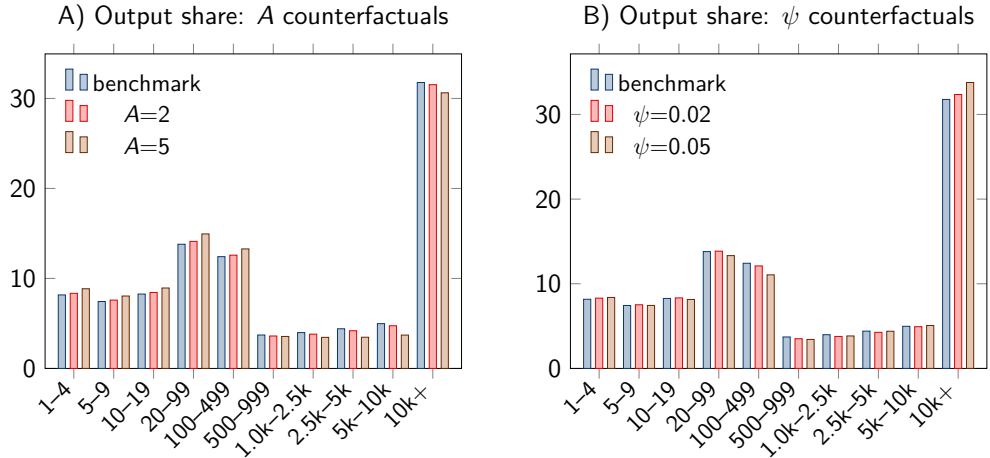


Figure: Output concentration by firm size under changes in attacker capacity A (left) and matching efficiency ψ (right). Bars show the benchmark and two counterfactual values for each experiment.

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

Subsidies for Cybersecurity Investment

back

- 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

back

- 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:

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

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

State-Contingency in policy responses

back

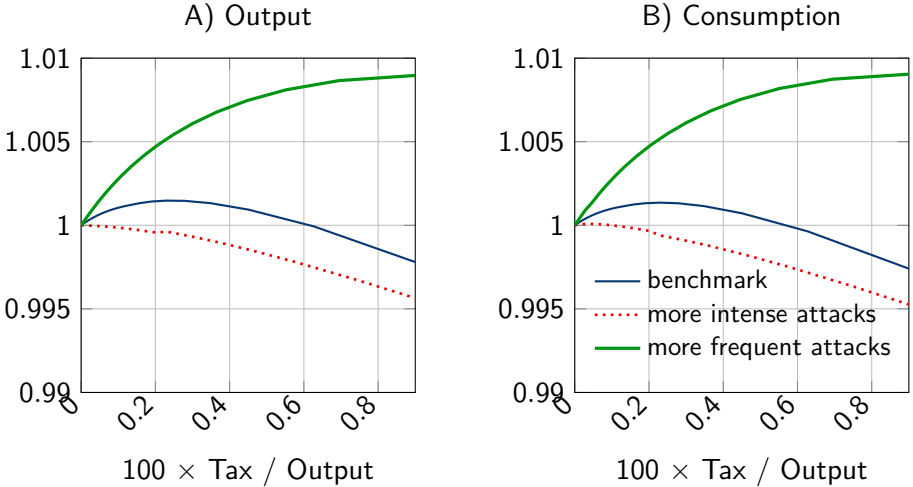


Figure: Equilibrium responses to changes in the subsidy generosity in economies with different severity of cyber risk. Panel (A) reports aggregate output; Panel (B) reports aggregate consumption. Solid blue lines correspond to the benchmark economy, red dotted lines correspond to the economy with high attack capacity ($A = 5$), and green dashed lines correspond to the economy with higher matching efficiency ($\psi = 0.05$).