2024 Spring Seminar

Systemic Cyber Risk and Aggregate Impacts

Department of Industrial and Management Engineering, POSTECH
Actuarial modeling, Insurance and Risk Management Laboratory

Keywoong Bae

Information

- **Title:** Systemic Cyber Risk and Aggregate Impacts
- **Authors:** Jonathan W. Welburn, Aaron M. Strong
- **Journal:** Risk Analysis
- **Year:** 2021

목차

1. Introduction
2. Efforts to understand Systemic Cyber Risk
3. Quantitative Model
4. Cyber Incident Analysis
5. Implications for Cyber Insurance and Cyber Policy
6. Conclusions

1. Introduction

- **Cyber incidents** have risen both in prevalence and significance in their disruptions to individuals, businesses, and governments.
  - It have spread across **dependent systems**. (DDoS attack on Dyn in 2016, WannaCry and Notpetya in 2017)
  - These incidents, resulting in outsized effects and often ill-understood cascading failure, **exemplify the potential for systemic risk in cyberspace.**
- This article addresses the emerging form of cyber risk called systemic cyber risk.
  - elucidate the scale of systemic cyber risks and, specifically the potential economic consequences of systemic cyber failures.
  - understand systemic cyber failure and potential impacts.
- In doing so, this article gives specific attention to the question of whether cyber insurance is a sufficient tool for managing cyber risks, or whether systemic cyber risk warrants new conversations on cyber policy are needed.

2. Efforts to Understand Systemic Cyber risk

- De Bandt and Hartmann (2000) have defined systemic risks as follows
  - **Systemic risk** is an event, where the release of 'bad news' about a financial institution, or even its failure, or the crash of a financial market leads in a sequential fashion to considerable adverse effects on one or several other financial institutions or markets
  - **Domino effect** following a limited idiosyncratic shock or the result of simultaneous adverse effects due to widespread systemic shocks.
  - Following the 2008 global financial crisis, numerous studies were conducted on systemic risk in finance
- Like financial networks, cyberspaces presents a system of heavily interdependent organizations connected through network ties
  - The deliberate combination of fields – systemic risk and cyber risk
  - It builds on the fields of cyber security, finance, economics, and risk analysis
- Under the assumptions that all cyber incidents can be categorized as either **data breaches** and **cyber attacks**.
  - Data breach: the 2017 cyber incident at Equifax
  - Cyber attack: the 2016 cyber incident disrupting the Ukrainian power grid

• De Bandt, O., & Hartmann, P. (2000). Systemic risk: a survey. Available at SSRN 258430.

2.1 Approaches for Characterizing Systemic Cyber Risk

- **Systemic Cyber Risk** is defined as follows (*World Economic Forum, 2016*)
  - Systemic cyber risk is the risk that a cyber event at **an individual component** of a critical infrastructure ecosystem will cause **significant delay, denial breakdown, disruption or loss**, such that services are impacted not only in the originating component but consequences also **cascade into related ecosystem components**, resulting in **significant adverse effects** to public health or safety, economic security or national security
- Identification of 11 systemic cyber attack patterns (*Bodeau & McCollum, 2018*)
  - Common mode/repeated attacks, common mode/scattershot attacks, common mode/pervasive attacks, rolling attacks, transitive attacks, cascading attacks, shared resource consumption attacks, critical function attacks, regional attacks, service dependency attacks, and coordinated supply chain attacks.
- Understanding of the potential impacts of systemic cyber incidents
  - Systemic cyber risk can be a source of systemic financial risk where a cyber event on systemically important firms could lead to substantial spillover effects, or outward propagations (*Office of Financial Research, 2017*)
  - OECD started to identify specific types of systemic cyber incidents that could serve as a potential drivers of country-level and global-level shocks. (*Sommer & Brown, 2011*)

- Bodeau, D. J., McCollum, C. D., & Fox, D. B. (2018). Cyber threat modeling: Survey, assessment, and representative framework. Mitre Corp, Mclean.
- Sommer, P., & Brown, I. (2011). Reducing systemic cybersecurity risk. Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS (2011), 3.

2.2 Approaches for Modeling the Economic Impact of Cyber Risk

- The modeling of economic consequences cyber risk for is an evolving field and has leveraged methods from risk analysis in different ways
  - **Complexities** involved in quantifying the full range of cyber risks, companies, and insurers have tended to take a relatively rudimentary approach to modeling (*Swiss Re, 2017*)
  - There are samples of cyber incidents from Advisen data set, however there is the uncomfortable reality that such data may miss the full distribution, and the upper tail in particular (*Aldasoro et al, 2016*).
  - Some incidents can be unobserved, unreported, or have yet to occur.
  - **Descriptive statistics over partially observed incidents risks underestimating tail risk.**
- The use of **structural models** has been largely under explored for estimating the **economic impact** of cyber incidents (*Dreyer et al, 2018*)
  - To estimate systemic costs, they used sector level input-output analysis to estimate the propagation across backward linkages or upstream supply chain linkages of costs following a cyber incident.
  - Acknowledging that **downstream costs could exceed upstream costs**, the authors leave this as an area for future work.

- Re, S. (2017). World insurance in 2016: the China growth engine steams ahead. sigma, 3(2017).
- Abad, J., Aldasoro, I., Aymanns, C., D'Errico, M., Rousová, L. F., Hoffmann, P., ... & Roukny, T. (2016). Shedding light on dark markets: First insights from the new EU-wide OTC derivatives dataset. ESRB: Occasional Paper Series, (2016/11).
- Choy, G., Khalilzadeh, O., Michalski, M., Do, S., Samir, A. E., Pianykh, O. S., ... & Dreyer, K. J. (2018). Current applications and future impact of machine learning in radiology. Radiology, 288(2), 318-328.

2.3 A Framework for Characterizing Systemic Cyber Risk

- This paper introduced a framework for understanding and modeling systemic cyber risk parsimoniously.
- Three categories of systemic failures: (*i*) cascading, (*ii*) common cause, and (*iii*) independent.
  - **Cascading cyber failures** are the result of one cyber incident propagating outward and causing many disruptions like domino effect across firms and organizations (*DDoS cyber attack on Dyn on 2016*)
  - **Common cause cyber failures** are the result of one cyber exploit triggered at many firms causing many cyber incidents, exploiting a common vulnerability held by multiple organizations causing numerous cyber incidents. (*WannaCry on 2017*)
  - **Independent cyber failures** are the result of cyber incidents exploiting independent vulnerabilities at individual firms and organizations, and this type of event is currently unlikely.
- Cascading and common cause failures are not mutually exclusive.
- This article puts a specific **focus on cascading cyber failures.**

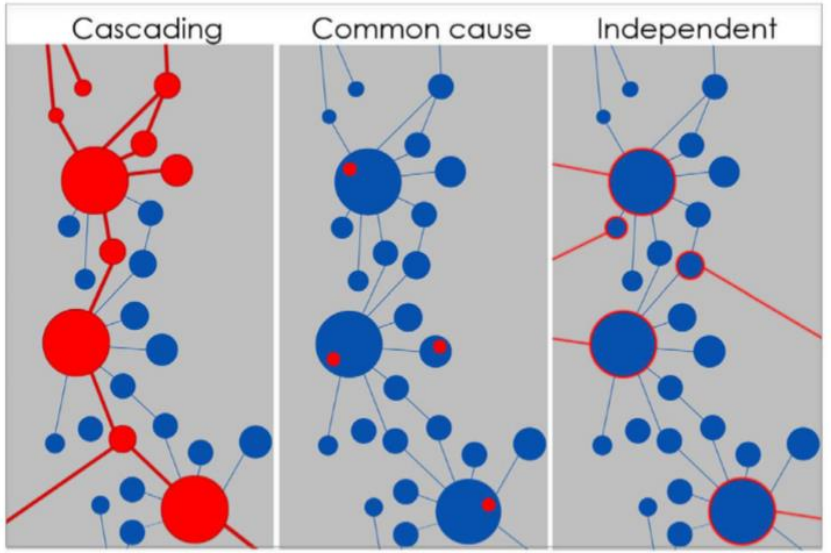


Fig 1. Types of systemic cyber risk
Figure 1 visualizes the three categories of systemic cyber failures. Cascading failures result from the propagation of disruptions across network connections following a cyber incident on a given firm, common cause failures result from the exploitation of common vulnerabilities shared by many firms, and independent failures result from the simultaneous individual and isolated cyber incidents occurring at many firms.

3. Quantitative Model

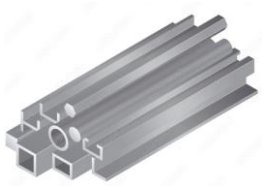
- **Sector-specific** models have been **inadequate** in bringing the costs and consequences of cascading failure to light (*Brenner et al, 2017*)
  - Challenges in applying traditional structural modeling approaches to firm-level risks.
  - The **lack of firm-level data** a likely cause for scant research of firm-level production networks.
  - Recent review of the literature underscoring this reality (*Carvalho and Tahbaz-Salehi, 2019*).
- This challenge has been addressed in different ways, especially **sector-level computable general equilibrium (CGE) models** to estimate the economic impacts.
  - Assumption that following a significant disruptions, an economy instantaneously moves to a new equilibrium with price adjusting.
  - However, it may not be appropriate to assume that an economy is in an equilibrium following a disruption.
- So, this paper approached as follows
  - Only considers shocks that are small enough so that firms cannot recontract.
  - Require **a different approach** than traditional CGE models.

- Fitzmaurice, C., Allen, C., Barber, R. M., Barregard, L., Bhutta, Z. A., Brenner, H., ... & Satpathy, M. (2017). Global, regional, and national cancer incidence, mortality, years of life lost, years lived with disability, and disability-adjusted life-years for 32 cancer groups, 1990 to 2015: a systematic analysis for the global burden of disease study. JAMA oncology, 3(4), 524-548.
- Carvalho, V. M., & Tahbaz-Salehi, A. (2019). Production networks: A primer. Annual Review of Economics, 11, 635-663.

3. Quantitative Model

- **Input-output (I/O) modeling** for **estimating the immediate economic impact** of an idiosyncratic shock (cyber attack)
  - To estimate the economy wide impact of sectoral fluctuations.
  - **A traditional I/O modeling approach** does **not capture downstream impacts.**
  - In contrast, **computable general equilibrium** analysis **does capture these downstream supply chain impacts** though changes in prices.
- Firms have varying abilities to maintain operations during and recover from cyber attacks, an ability henceforth referred to as **resilience**.
  - Resilience of firms depends on numerous factors (cyber maturity, nature of their business…)
  - Many of these factors are unknown, so **estimating the resilience of individual firms is nontrivial.**
- How can we estimate average resilience at the level of economic sectors?
  - Investigation on the impact of a terrorist attack driven power outage (*Rose et al, 2007*).
- This article defines **a structural model** for estimating the potential impacts of cyber incidents at individual firms using **quantitative model**.
  - incorporate a firm level resilience that control for temporal substitution and other business operations that minimize the impacts of business interruptions on firm output and revenue.

(Example) Traditional Leontief Input/Output Model



Iron 7t

Water 4t

- The amount of both goods (iron, water) supplied to the market is less than production, so we need to produce more than this.
- All industries are connected.
- In order to determine the output of a factory, factory needs to determine how much one industry is related to another. ➔ **Input-Output Tables**

Example for Leontief I/O Model

- $1 Iron = $0.5 iron + $0.2 water
- $1 water = $0.4 iron + $0.1 water

$$M = \begin{bmatrix} 0.5 & 0.2 \\ 0.4 & 0.1 \end{bmatrix}$$

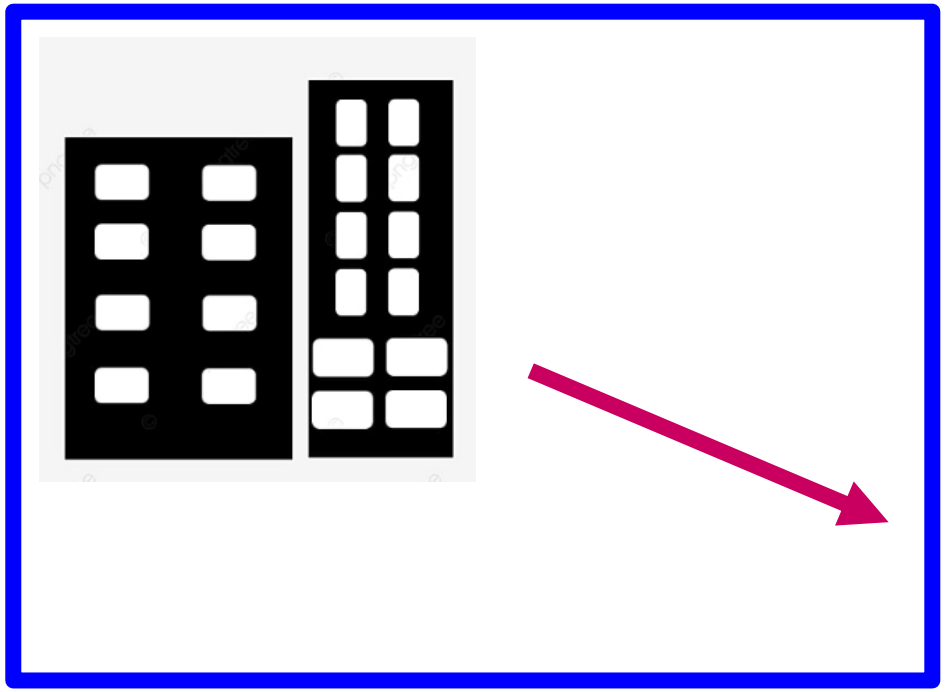
➔ **Leontief matrix**

$$x = Mx + D$$
$$(I - M)x = D$$
$$x = (I - M)^{-1}D$$

$$x = \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 0.5 & 0.2 \\ 0.4 & 0.1 \end{bmatrix}\right)^{-1} D = \left(\begin{bmatrix} 0.5 & -0.2 \\ -0.4 & 0.9 \end{bmatrix}\right)^{-1} \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \left(\begin{bmatrix} \frac{90}{37} & \frac{40}{37} \\ \frac{20}{37} & \frac{50}{37} \end{bmatrix}\right) \begin{bmatrix} 7 \\ 4 \end{bmatrix} = [19.18 \quad 12.97].$$

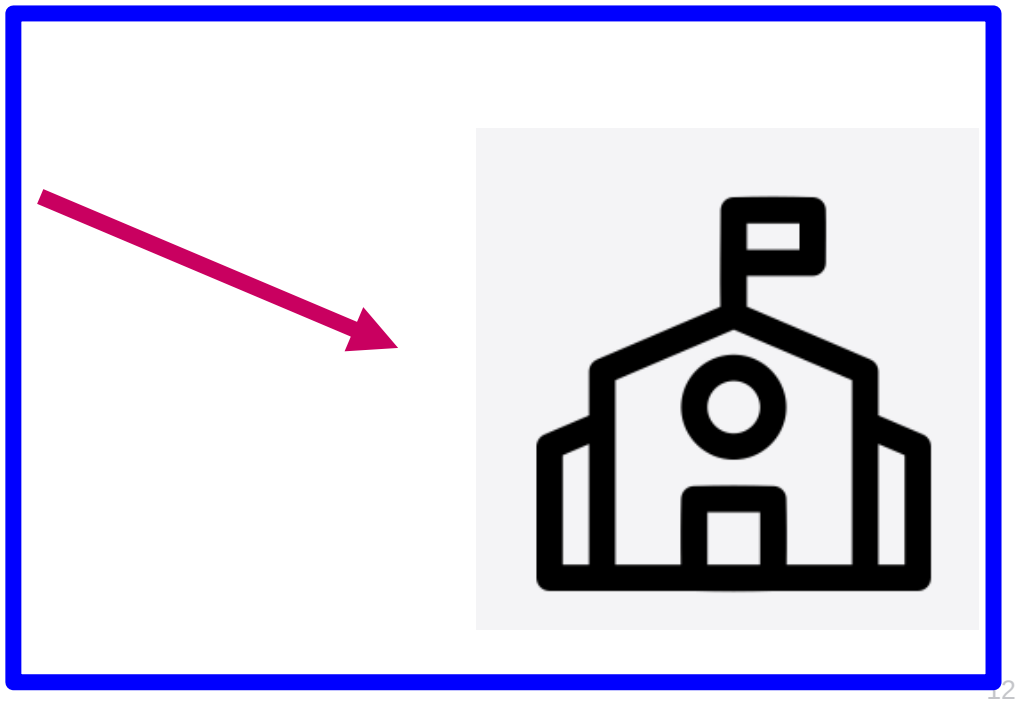
- Therefore, based on the Input-Output table above, to produce 7 tons of iron and 4 tons of water, we need to produce **19.18 tons of iron** and **12.97 tons of water.**

Quantitative model's flow of this article



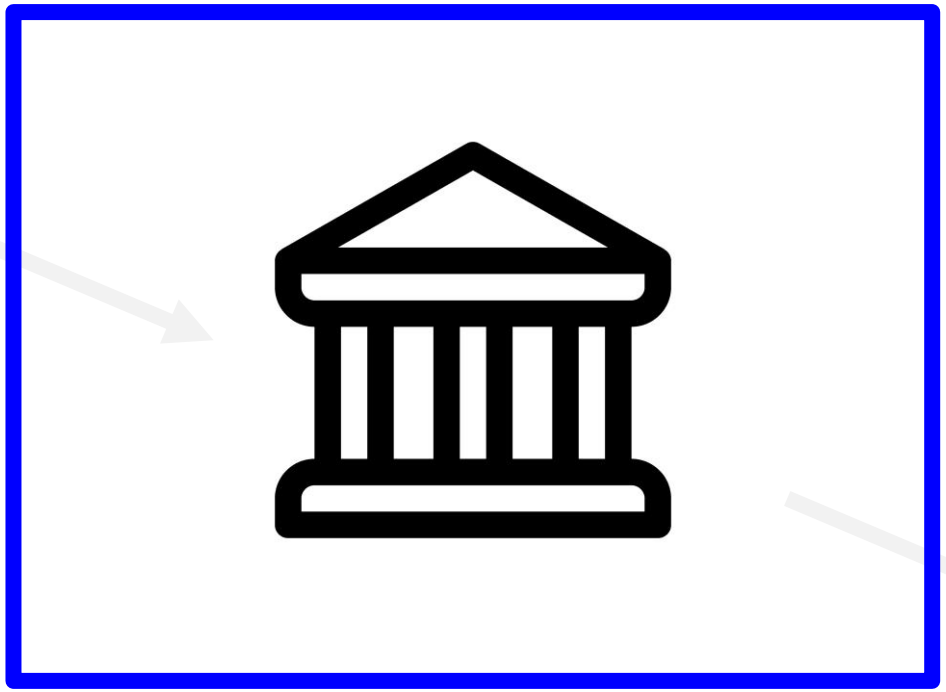
Upstream Impact

Downstream Impact



Quantitative model's flow of this article

Direct Impact (3.1)



$\varepsilon = \{S, W, \epsilon\}$

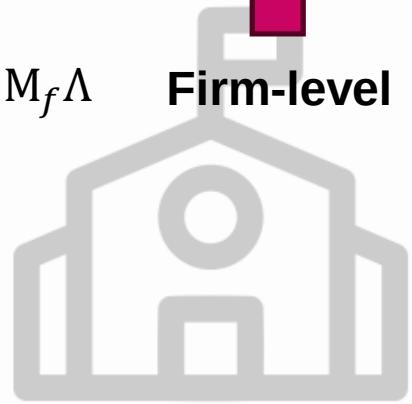
$\epsilon_i = \phi' \omega_i$

$\phi_f = \left(\frac{y_f}{365}\right) \mathrm{M}_f \Lambda$

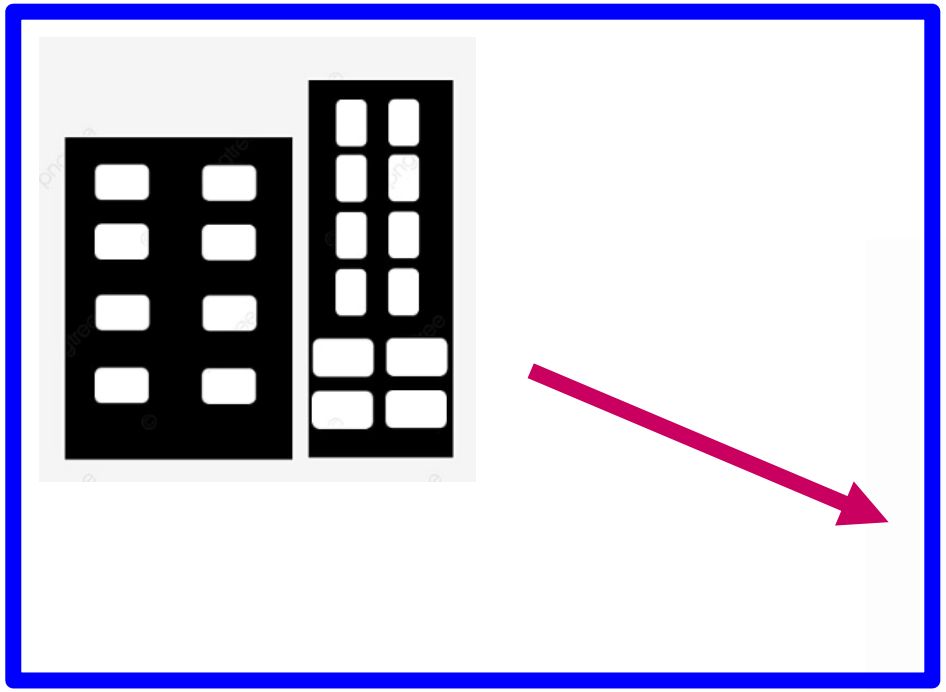
Economy-level

Sector-level

Firm-level



Quantitative model's flow of this article



Upstream Impact

$$x = Wx + d$$

$$x = (I - W)^{-1}d = L^{-1}\boldsymbol{d}$$

$$\Delta x = L^{-1}\boldsymbol{\epsilon}$$

Upstream Impact

Sector-level shock

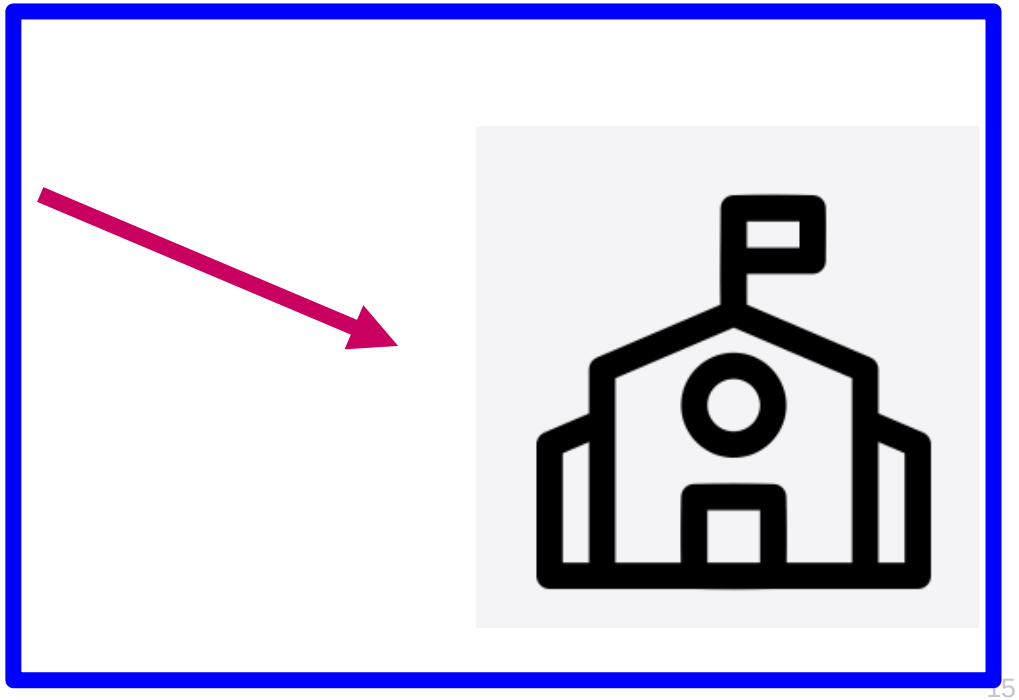
Leontief Input/Output Model

Propagation of shocks originating at the sector-level

Quantitative model's flow of this article

$$\Delta Y_i = Y_i \left(\frac{\Delta X_{ij} X_{ji}}{X_{ji}} \right) = \mathrm{Y_j} \frac{\epsilon_i}{\Sigma_s X_{si}} = Y_j \frac{\boldsymbol{\epsilon_i}}{\Sigma_s X_{si}} = Y_j \frac{\boldsymbol{y_f M_f \Lambda \omega_{fi}}}{\mathbf{365}\ (\Sigma_s X_{issi})}$$

Downstream Impact



3.1 Cyber attack Foundations of Idiosyncratic Firm Risk

- To understand the aggregate impacts resulting from a cyber attack-driven outage at individual firms, they model the **economy** as a tuple $\varepsilon = \{S, W, \epsilon\}$
  - S: Sector type, W: Weighted adjacency matrix, ϵ: Vector of sector-level shocks.
  - Each sector is made up of firms each firm f produces output y_f.
  - Total output of sector i is Y_i, determined by the sum of its firms $(\mathrm{Y_i} = \Sigma_{f \in i}\, y_f)$.
  - Aggregate output Y is determined by the sum of all firms $(\mathrm{Y} = \Sigma_f^m y_f)$.
- To model the economy of ε, they focus on the **microorigins** of aggregate shocks.
  - Estimating the microfoundations of aggregate shocks stemming from firm-level outages using a model of firms with representative sectoral ties.
- This approach is based on the following assumption: important contribution to the estimation of aggregate losses from firm-level shocks

Assumption 1. Representative firm linkages

We assume that the flows in and out of each sector are representative of the firms in that sector. That is, each firm is a representative firm in that sector that only differ in output but not the underlying production process.

Assumption 1 implies that for any given firm f in sector i, its flows to and from all other sectors j are proportional to its share of sector level output as follows:

$$u_{fj} = \omega_{fi} w_{ij} \; \forall f \in i, \quad j \in S, \qquad (1)$$

- w_{ij}: the flows from sector i to sector j.
- ω_{fi}: firm f's output share of sector i.
- u_{fj}: output flows from firm f used as inputs to production in sector j.

3.1 Cyber attack Foundations of Idiosyncratic Firm Risk

- By introducing idiosyncratic firm-level shocks, ϕ_f, sector-level shocks ϵ_i can therefore be explained by microfoundations as follows: $\epsilon_i = \phi' \omega_i$
  - $\omega_i = [\omega_{1i}, \dots, \omega_{mi}]$ is the vector of firm output shares
  - $\phi = [\phi_1, \dots, \phi_m]$ is the vector of idiosyncratic m firm-level shocks.
- They define the idiosyncratic firm-level shocks as the result of a cyber attack lasting for a duration Λ days: $\phi_f = \left(\frac{y_f}{365}\right) \mathrm{M}_f \Lambda.$
  - $\frac{y_f}{365}$: firm f's annual revenue divided by 365.
  - **M_f: a sector resilience multiplier attached to each firm f**. It is estimated in a model calibrated to the effects of a power outage.
  - If **$M_f = 0$**, firm f is perfectly resilient and is unaffected by shock, and if **$M_f = 1$**, it receives the entirety of the shock.
- Based on the assumption 2, that the firm is large relative to other firms in the sector since the supply chain for a small firm may only include a few sector.
  - I/O models assume that production takes place with a recipe and does not allow substitution across inputs when inputs are note available, or prices changes.

Assumption 2. The duration of each attack is sufficiently short

We assume that the duration Λ of each cyber attack driven is sufficiently short as to not allow for re-contracting of business relationships keeping network ties static.

3.2 Upstream Impacts

- Exploit the I/O model through the use of **traditional I/O modeling** to estimate the backward linkages or **upstream supply chain linkages** in the economy ε through the implied multipliers: $x = Wx + d$
  - W: the sector-level weighted adjacency matrix, w_{ij} are the flows from sector $i - j$.
  - $x = [x_1, \dots, x_n]$: sector level output vector
  - $d = [d_1, \dots, d_n]$: sector level demand vector
- Manipulation via matrix operations yield the following relationship: $x = (I - W)^{-1}d = L^{-1}d$
  - L^{-1}: inverse Leontief matrix.
  - the indirect effects associated with an exogenous output change in one sector and **how it affects other sectors through upstream interactions.**
  - If we reduce in sector j by $\bar{x_j}$, then indirect effects are given by $L^{-1} = [0, \dots, 0, \bar{x_j}, 0, \dots, 0]$.
- Based on this relationship, they estimate the shocks originating at the sector level and the aggregate costs of their propagation across sectors of the economy: $\boldsymbol{\Delta x = L^{-1}\epsilon}$
  - $\epsilon = [\epsilon_1, \dots, \epsilon_n]$: vector of sector-level shocks.

3.3 Downstream Impacts

- Not only do firms purchase goods and services from other firms for production through the upstream supply chain, but they are **also providers of goods and services to other firms**. So does shock affect.
  - To identify the sector that as a reduction of output and the corresponding sectors that use that output as an input, they used the **NAICS** (North American Industry Classification System) code.
  - To see how much a reduction in output due to a shock in one sector affects the inputs of other sectors
- The shock of ϵ_i **leads to proportional reduction in sector i's outputs** to production going to all other sectors j $(= X_{ji})$.
  - Allocate the lost output to each of the sectors.
  - ΔX_{ji} is equal to the production of the shock ϵ and the percentage of sector i's inputs to production from sector j
  - $\Delta X_{ji} = \epsilon_i \, {}^{X_{ij}X_{ji}}/_{\Sigma_s X_{is}X_{si}}$
  - **ΔX_{ijji} drives a reduction in the output of sector j, Y_j.**
- Each sector experiences a cascading shock equal to the relative importance of firm f to the overall economy.
  - Thus, a firm may have a large impact on the overall economy if it is large within its sector or the sector plays an important role in the overall economy.

4.1 Analysis of Potential Incidents

- They analyze the potential impact of a cyber attack on large and likely targets.
  - They chose a large telecommunications firm (AT&T), a hardware firm (Cisco Systems), retail banking firm (JP Morgan Chase), and a point-of-sale firm (Visa).
  - Additionally, include Ford, as a comparison to AT&T, due to their similar sizes but different sectors.
  - Used revenue (y_f), sector (i), duration (Λ), and resilience (M_f) as input values.
  - Assume a stoppage of all operations and services of each company lasting **one day**.
  - Through this values, they estimates the potential losses associated with each incident rather than the statistical expectation of losses where **actual losses could be small** due to the cyber risk management strategies and resilience of individual firms.

Table I. Input Data for Analysis

	Visa	Cisco Systems	JP Morgan Chase	AT&T	Ford Motors
2017 Revenue (millions), y_f	$ 18,358	$ 48,005	$ 93,689	$ 160,546	$ 156,800
NAICS Sector, i	44–45 Retail trade	51 Information	52 Finance & insurance	51 Information	31–33 Manufacturing
Duration (days), Λ	1	1	1	1	1
Resilience multiplier, M_f	0.661	0.700	0.217	0.700	0.712

Table I displays all input values – revenue, sector, duration, and resilience – used to analyze the potential impact of a one-day cyber attack on Visa, Cisco, JP Morgan Chase, AT&T, and Ford. We use the North American Industry Classification System (NAICS) for sectors. For the sector specific resilience multiplier, we use the calibration results of Rose et al. (2007). That is, while Rose et al. (2007) estimates resilience multipliers at the sector level, not the firm level, firms are assumed to have the same resilience multipliers as their sectors. As a result, while the analysis considers an attack which disrupts the entire business operations of each firm for one day, each firm has some level of resilience preventing complete outages. Data on firm revenue is taken from S&P Capital IQ NetAdvantage. The authors chose firm sectors to most closely alight to the immediate impact of their respective shocks.

4.1 Analysis of Potential Incidents

- Direct cost, Upstream impact, and Downstream impact
- The direct impact of the cyber attack of 1 day, ϕ_f, is largely proportional to revenue.
- The effects of a cyber attack propagate down from each firm to their customers, with important implications.
- The exercise of estimating losses following a **one-day** cyber attack on each of the four firms reveals the staggering potential impacts of systemic cyber risk.
  - Direct losses are large but manageable
  - However, **cascading failures** could result in **sizeable damages** incurred by other firms, organizations, and individuals.
- The differences between direct and systemic losses vary significant based on the type of firm, its sector, and how interconnected it is.

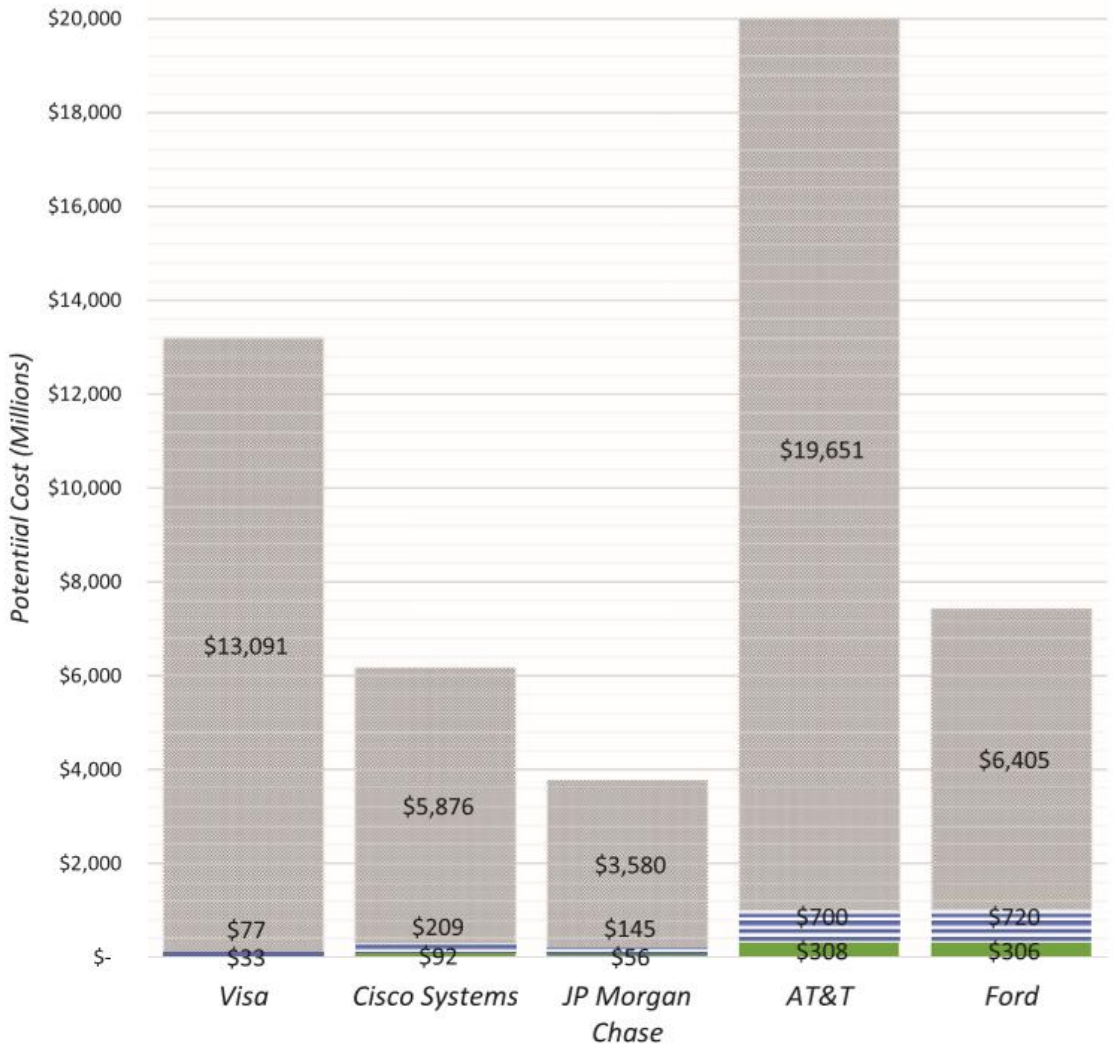


Fig 4. Potential impact of 1-day cyber attack.
Figure 4 displays the potential impact of a one-day cyber attack on Visa, Cisco, JP Morgan Chase, AT&T, and Ford. The direct, upstream, and downstream costs are shown for each scenario as a stacked chart. On bottom, the direct cost to the firm is shaded as a solid orange region. In the middle, the total upstream costs to suppliers is shaded in horizontal blue lines. On top, the total downstream costs are shaded with gray dots.

4.2 Maersk Case

- They now look to the 2017 NotPetya cyber attack that disrupted Maersk's operations as a case for comparing model with a real incident.
  - **10 days** from the beginning of the attack to fully rebuild their information systems, and **two months** for fully recovered
  - Incurred between $250 and $300 million in lost revenue due to the incident (Maersk, 2018).
- By using quantitative model in previous, they want to estimate the potential loss as a case of Maersk outage.
  - The true resilience of Maersk to a cyber attack driven outage (M_f) **is unknown**.
  - So, they estimate the range of potential impacts.
  - Lower bound: $M_i = 0.052$ (value of transportation sector resilience calibrated by Rose et al, 2007)
  - Upper bound: $M_i = 1$ (the value of no resilience)

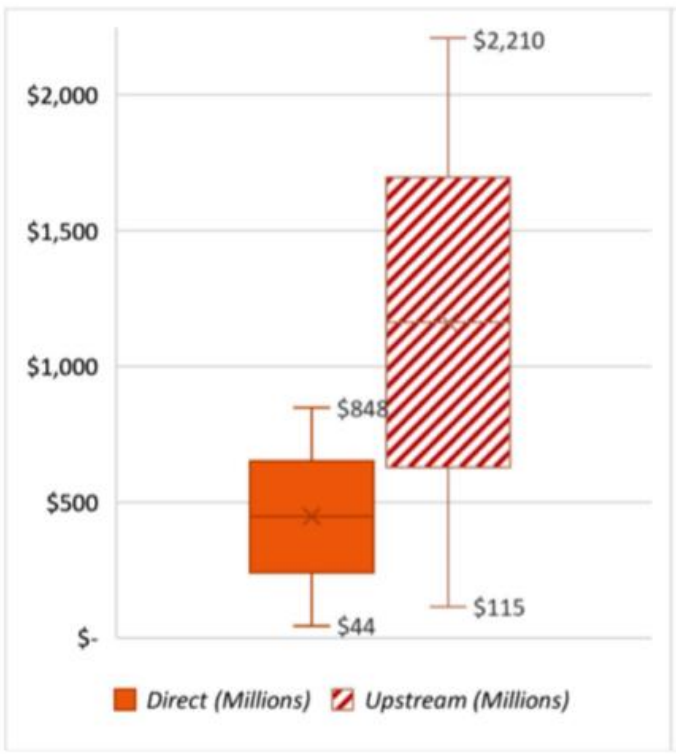
Table II. Input Data for Maersk Case

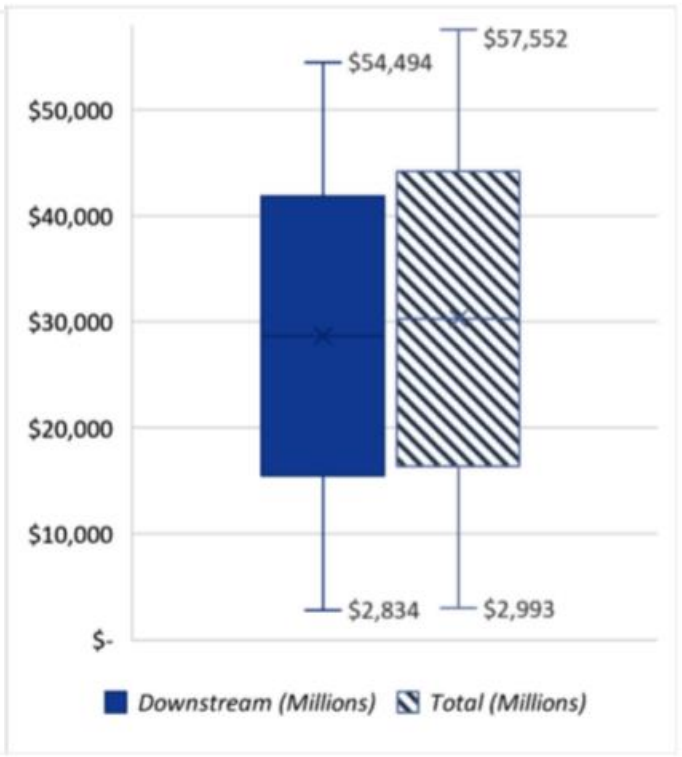
	Maersk
2017 Revenue (millions), y_i	$ 30,945
NAICS Sector, s	48-49 Transportation & Warehousing
Duration (days), Λ	10-60
Resilience measure, M_i	0.052

This table displays all input values—revenue, sector, duration, and resilience—used to analyze the potential impact of a cyber attack ranging from 10–60 days on Maersk where the North American Industry Classification System (NAICS) is used for sectors, and the sector specific resilience multiplier comes from the calibration results of Rose et al. (2007).

4.2 Maersk Case

- The range of direct and upstream impacts and downstream and total impacts.
  - The range of potential impacts conveys the central importance of resilience on varying impacts.
- **The actual lost** revenue (direct cost) from the Maersk case of **$250 ~$300** million falls on the lower end of this window
  - Value of sector level resilience is overly optimistic for this specific case.
  - The values of resilience would be between $\boldsymbol{M_i = [0.3, 0.35]}$ instead of $M_i = 0.052$.
- Firm heterogeneity within sector can plausibly result in significant variation.





4.2 Maersk Case

- We can estimate total losses for the actual Maersk case ($250~$300).
- Given the centrality of Maersk and the large downstream impacts, the results estimate that the total potential losses from the incident, which drove **$300 million in direct revenue losses ($M_f = 0.35$), could total $20 billion.**

Table III. Estimated Total Impact of 2017 NotPetya Cyber Attack on Maersk and Dependent Firms

	Direct	Upstream	Downstream	Total
$M_i = 0.3$	$254.34	$663	$16,348	$17,265
$M_i = 0.35$	$296.73	$773	$19,073	$20,143

Table III displays the range of estimated direct, upstream, downstream, and total costs of the NotPetya attack on Maersk tailored to the resilience values corresponding to direct losses. All values are displayed in millions of 2017 dollars.

- This case does demonstrate the capability of this approach to estimate potential cyber attack impacts
  - the analysis of the Maersk case is consistent with Maersk's reports while providing insights.

5. Implications for Cyber Insurance and Cyber Policy

- One of the motivations of these estimations of the potential costs associated with systemic cyber failures is **to answer these questions.**
  - Whether **cyber insurance is a sufficient** tool for managing cyber risks.
  - Whether systemic cyber risk warrants new conversations on **cyber policy are needed.**
- In creating cyber insurance policies, many insurance carriers manage their portfolio risk through security questions and diversification across portfolios.
  - A wide range of security information collected by different policies, as well as variation in how that information is incorporated into insurance pricing
  - Even more problematic for these carriers is identifying the characteristics of firms that could result in systemic failure, undermining diversification's implicit assumption of independence, and possibly leading to catastrophic loss.
- A small number of firms seek to develop better data modeling techniques in order to understand and predict aggregation risk.
  - Cambridge Centre for Risk Studies and Risk Management Solutions (RMS): try to standardize the information collected for cyber incidents.
  - AIR: developed the VERISK cyber exposure data standard in 2016, which provides a competing framework and analytics of risk from cyber platform

5. Implications for Cyber Insurance and Cyber Policy

- While typical cyber attacks may fit within the realm of insurable losses, insurance companies may be more exposed to systemic losses that it appears.
  - The direct losses would be spread across numerous insurance companies rather than one single portfolio, reducing the exposure of each insurer.
  - However, cascading failures up and downstream may result in hidden portfolio risk for insurers where other contracts are triggered by the initial cyber event.
  - The resulting portfolio risk of simultaneous policy losses following what initially appeared to be a single cyber incident affecting a single policy could be nontrivial
- However, when we look to the aggregate costs of cyber incidents including downstream losses, a need for broader policy discussion emerges.
  - The potential impacts could exceed the scenarios considered in this article, and it reveals a need for additional policy consideration.
- Enhancing resilience may be one of the largest factors for combating systemic cyber risk
  - As the policy discussion surrounding systemic risk in cyberspace grows, efforts to enhance cyber resilience should be considered.