The Anatomy of Cyber Risk

Rustam Jamilov, Hélène Rey, and Ahmed Tahoun

Ishita Sen

Harvard Business School

ECB-RFS Macro-Finance Conference, March 23, 2021

Overview

- Cyber risk is a growing challenge.
  - Staggering amount of malicious activity on the internet, e.g., 80 billion malicious scans daily!
  - Cybercrime costs the world $\sim$\$1 trillion, or 1% global GDP (McAfee, 2020).

Overview

- Cyber risk is a growing challenge.
  - Staggering amount of malicious activity on the internet, e.g., 80 billion malicious scans daily!
  - Cybercrime costs the world ~$1 trillion, or 1% global GDP (McAfee, 2020).
- Open questions:
  - Implications for firm value, corporate policies, and firm operations?
  - How firms do risk management and implications for cyber insurance markets?
  - Whether there is a potential for contagion?

Overview

- Cyber risk is a growing challenge.
  - Staggering amount of malicious activity on the internet, e.g., 80 billion malicious scans daily!
  - Cybercrime costs the world $\sim$\$1 trillion, or 1% global GDP (McAfee, 2020).

- Open questions:
  - Implications for firm value, corporate policies, and firm operations?
  - How firms do risk management and implications for cyber insurance markets?
  - Whether there is a potential for contagion?

- Measurement is a challenge:
  - How to quantify risk exposures accurately at the firm level or aggregate level?
  - Realized losses: (i) not all exposed firms suffer an attack. (ii) firms may under-report attacks.

This paper

- Measure **firm-level exposures** to cyber risk using a text-based approach, as in Hassan, Hollader, Lent, and Tahoun (2019).

- Transcribe earnings conference calls and create a training library of cyber risk related keywords, e.g., "cyber attack", "data breach".

- Measure the share of conversation related to cyber risk between management and participants (e.g., analysts).

$$CyberExposure_{it} = \frac{\text{Total cyber keywords}_{it}}{\text{Total terms}_{it}}$$

(+)
- Over 800,000 calls, highly labor intensive. Lot of effort went into it.
- Extensive coverage: 12,000 firms in 80+ countries over 20 years.
- Lower disclosure biases because of pressure from outsiders vis-a-vis 10Ks.

- Exploit the *CyberExposure* measure for interesting asset pricing tests.

1. Accounting for risk and uncertainty

- Cyber keywords are not counted in conjunction with keywords on **risk** or **uncertainty**.

1. Accounting for risk and uncertainty

- Cyber keywords are not counted in conjunction with keywords on **risk** or **uncertainty**.
- However, a mere mention of cyber terms need not imply high risk and could even mean the opposite.
- Example 1: "*we are heavily guarded against cyber crimes.*", "*large investments in cyber infrastructure*".
- Example 2: IT firms who sell cyber risk software.
  - IT Services account for >40% of all mentions of cyber terms.

1. Accounting for risk and uncertainty

- Cyber keywords are not counted in conjunction with keywords on **risk** or **uncertainty**.
- However, a mere mention of cyber terms need not imply high risk and could even mean the opposite.
- Example 1: "*we are heavily guarded against cyber crimes.*", "*large investments in cyber infrastructure*".
- Example 2: IT firms who sell cyber risk software.
    - IT Services account for $>40\%$ of all mentions of cyber terms.
- Suggestion: use the conditional measure Cyber $\times$ Risk that you already created as the main measure.

2. Accounting for cyber risk management

- Plausible that exposed firms take actions to mitigate cyber risk, e.g. higher expenditure on IT infrastructure or cyber insurance.

- Conditional searches reveal that "insurance" is often mentioned after cyber keywords.

2. Accounting for cyber risk management

- Plausible that exposed firms take actions to mitigate cyber risk, e.g. higher expenditure on IT infrastructure or cyber insurance.

- Conditional searches reveal that "insurance" is often mentioned after cyber keywords.
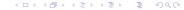
- Ideally we want **net** not **gross** exposures, accounting for cyber risk management.

- Example*: **least exposed**: "*we can adequately deal with cyber risk through preventive measures.*"

- Example*: **most exposed**: "*increasing sophistication of hackers makes defending against cyber attacks difficult, despite investments in preventive systems.*"

2. Accounting for cyber risk management

- Plausible that exposed firms take actions to mitigate cyber risk, e.g. higher expenditure on IT infrastructure or cyber insurance.

- Conditional searches reveal that "insurance" is often mentioned after cyber keywords.

- Ideally we want **net** not **gross** exposures, accounting for cyber risk management.

- Example*: **least exposed**: "*we can adequately deal with cyber risk through preventive measures.*"

- Example*: **most exposed**: "*increasing sophistication of hackers makes defending against cyber attacks difficult, despite investments in preventive systems.*"

- Not trivial to do in a text based measure. Potentially measure tone, longer keyword searches.

* Examples taken from Florackis, Louca, Michaely, and Weber (2020).

3. Digging deeper into zero exposure

- Absence of a cyber keyword mention does not mean no risk!
  - Typical earnings conference call lasts 35-45 mins.
  - Cyber risk could be overlooked due to more salient risks (e.g., banks).
  - Conference call discussions may only happen after salient cyber events.

3. Digging deeper into zero exposure

- Absence of a cyber keyword mention does not mean no risk!
  - Typical earnings conference call lasts 35-45 mins.
  - Cyber risk could be overlooked due to more salient risks (e.g., banks).
  - Conference call discussions may only happen after salient cyber events.

- Understanding and comparing magnitudes:
  - Florackis, Louca, Michaely, and Weber (2020) is an alternative text based measure using 10Ks. [FLMW]

	% mention	% never mention
This paper	5%	95%
FLMW	89%	11%

3. Digging deeper into zero exposure

- Absence of a cyber keyword mention does not mean no risk!
  - Typical earnings conference call lasts 35-45 mins.
  - Cyber risk could be overlooked due to more salient risks (e.g., banks).
  - Conference call discussions may only happen after salient cyber events.

- Understanding and comparing magnitudes:
  - Florackis, Louca, Michaely, and Weber (2020) is an alternative text based measure using 10Ks. [FLMW]

	% mention	% never mention
This paper	5%	95%
FLMW	89%	11%

- Possibility: this measure identifies the most exposed firms, however, it is hard to separate low from medium exposed.

4. Asset pricing tests

- Is *CyberExposure* priced?
  - This paper: Yes, consistent with FLMW.
  - Highlight the difference: aggregate factor (this paper) vs. firm specific measure (FLMW). There is a factor structure.
  - Other interesting avenues: what does the common factor relate to, e.g., business cycle, geo-political factors?
  - Questions: How to construct the aggregate factor? How to go from quarterly to monthly? Only US? Do you control for industries, MOM, QMJ...

4. Asset pricing tests

- Is *CyberExposure* priced?
    - This paper: Yes, consistent with FLMW.
    - Highlight the difference: aggregate factor (this paper) vs. firm specific measure (FLMW). There is a factor structure.
    - Other interesting avenues: what does the common factor relate to, e.g., business cycle, geo-political factors?
    - Questions: How to construct the aggregate factor? How to go from quarterly to monthly? Only US? Do you control for industries, MOM, QMJ...

- Is there potential for systemic risk?
    - This paper: Yes (new).
    - Evidence: Returns of unaffected and **unexposed firm** decline when a peer is attacked.
    - Not entirely convincing yet. **Are unaffected firms indeed unexposed?** *CyberExposure* $= 0 \nRightarrow$ no risk, or do we learn about exposures?

Conclusion

- Important topic and interesting paper!

- Impressive amount of data work.

- Focus on sharpening the measure and tightening the asset pricing findings going forward.