The effects of cyberattacks on intangibles of firms and critical sectors

The high economic stakes which worth measuring

June 2019

In knowledge-based and globalized economy, the importance of cyber-security, which signifies well-functioning infrastructure integrated in the Internet, is increasingly growing. The networked society has also exacerbated the risks of data integrity, data confidentiality and data accessibility. Statistics shows that over the last few years, the number of cyberattacks has significantly grown. Furthermore, cyberattacks become more and more sophisticated, which increases the complexity in global costs estimation of such attacks. Such sophistication also makes it difficult to assess their consequences for firms, industries and economy as a whole, as well as identify perpetrators to be able to better estimate risks and foresee negative events.

Economic performance and competitiveness is heavily based on non-material production factors, or intangible assets, related to knowledge and competences, technology, research and development, among others. In case of a cyberattack, such intangibles have high probability of being harmed, consequently inducing financial losses to organizations. To analyze the effects of cyberattacks on intangibles, HERMENEUT study focuses on a variety of intangible assets (Table 1), developed based on the prior literature and expert knowledge in cybersecurity and intangible assets.

Table 1. HERMENEUT taxonomy of intangible assets.

Intangible	**Description**
IPR	Firms' existing copyrights, patents, IP in progress internally etc.
Innovation	Firms' trade and business secrets, industrial process, on-going R&D, new product and services, business models
Key competence and human capital	Firms' personnel key technical and business competences, firms' personnel soft skills, organizational knowledge, learning capabilities, etc.
Organizational capital	Firms' digital supported process, non-digitised functional and interfunctional processes, firms' strategic capabilities, royalty, coperation and commercial agreements
Reputation	Organizatin reputation with clients, stakeholders and firms' ecossytems. Reputation of managers and employees. Cyber-thrustworthiness.
Brand	Brand value with customers, stakeholders and firm/organisations' ecosystem, brand reputation.
Data	Data on clients, on personnel, on business ecosystem etc.

The research helped provide new insights and answer questions on the following aspects of the topic, including the impacts of cyber-security events on firms' intangible assets, macro economy, and financial markets, as well as the profiling of cyber-criminals. These results are summarized below.

- ### How big are estimated intangible asset losses from cyber-security events?

The purpose of this study was to reveal the impact of cyber-security events on firms' intangible assets. In order to estimate losses on intangibles that occur after a cyber-breach, the study has built a counterfactual panel of not attacked firms, applied the event study methodology to assess the damages, and conducted a natural language processing (NLP) analysis of press releases after the data breach to estimate the percentage of loss with respect of different intangible assets. The impact of a cyberattacks on intangibles was estimated by obtaining the difference of attacked vs. non-attacked firms' intangible evaluation.

Overall results demonstrate high level of losses that are observed in the sample. For example, for the sampled firms in healthcare sector, the amount of losses reached almost US $50 billion in 2011. With regard to intangible assets, the results are provided for key three aggregated types of intangibles, i.e. intellectual property (IPR and innovation), key competence, and organizational capital (reputation and brand), and for four sectors, i.e. finance and insurance, healthcare and social assistance, information, and professional scientific and technical services (Figure 1). By applying the NLP approach to analyzing 133 cyberattacks published in press, the impacts of cyberattacks on intangible assets in various industries were estimated. In particular, results show that the biggest losses for the studied firms were in key competences in most sectors (up to 63.3% in healthcare and social assistance industry), followed by organizational capital (up to 44.7% in information industry), and IP (up to 27.5% in information industry).

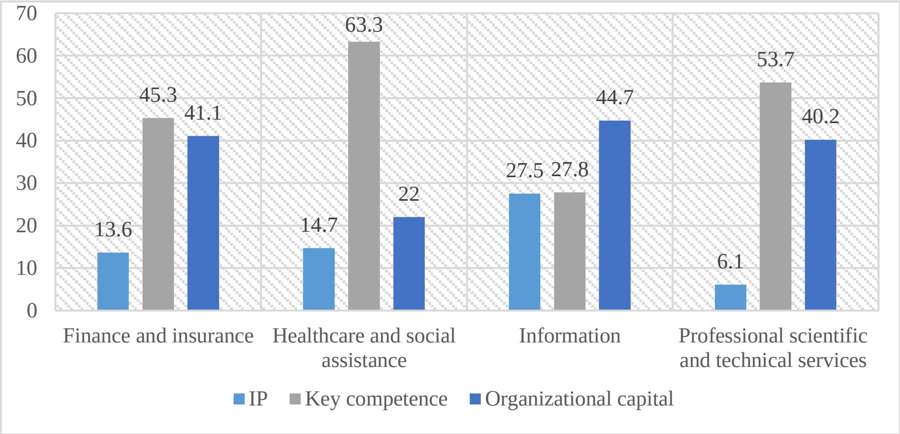


Figure 1. Splitting the loss into three intangible assets in four economic sectors

What are macroeconomic consequences of cyber-security events?

This study analyzed macroeconomic impacts of cyber-security events. The data on the inventory of cyberattacks were obtained from Advisen database, and financial data were retrieved from Compustat database. The macroeconomic approach adopted in the study was based on Dynamic input-Output Model (DIIM) and assumed that cyberattacks perpetrated in one sector result in a certain level of inoperability (production dysfunction) that cascades over other sectors through their input-output relationships. The World Input Output Database was used with the information on 56 sectors in 43 countries and a model for the Rest of the World. A number of simulations have been performed with different scenario-based inoperability levels.

The analysis revealed estimates of inoperability and losses at the macro level associated with cyber-attacks. In particular, economic losses for attacks that originated in the ICT sector, account for between 5% and 15% of the industry added value for initial inoperability of 40% (Figure 2). Results confirmed significant cascading effects of cyberattacks resulting from sector inoperability. To illustrate, in the US in 2013,

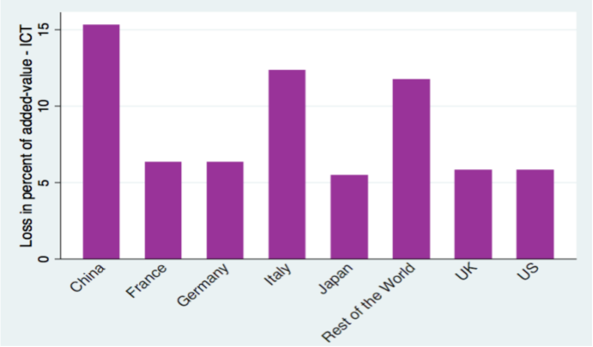
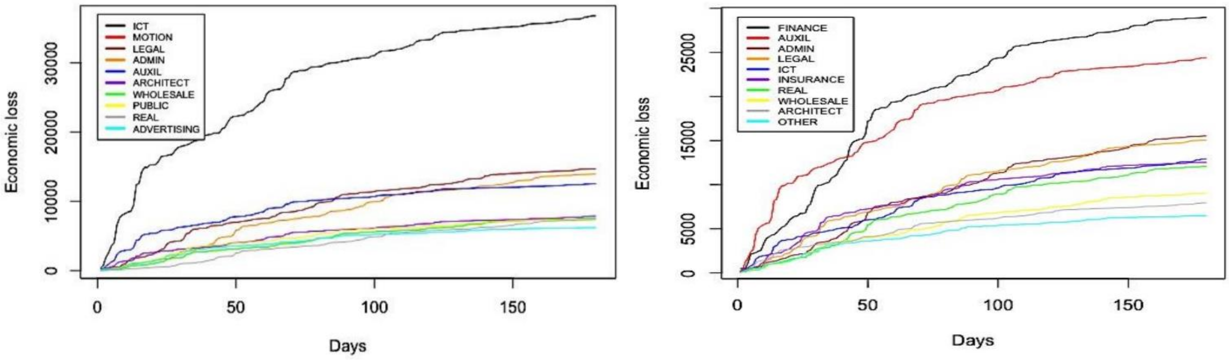


Figure 2. Effects of attacks in the ICT sector per country (40% inoperability)

cyberattacks that hit the ICT sector have also strongly affected other sectors in terms of economic losses, among which ICT, motion picture, video and television program production, as well as legal and accounting activities sectors most suffered. Moreover, the inoperability of 40% in the ICT and the finance sectors which started by a cyberattack also resulted in increased inoperability of other sectors. Furthermore, the economic loss across the affected sectors by an initial inoperability of 40% in the (a) ICT and (b) finance sectors in the US has been steadily increasing over time (Figure 3).



a) US, ICT, 2013

b) US, Finance, 2013

Figure 3. The economic loss (US $ million) in top 10 affected sectors during the initial 180 days. The initial inoperability of 40% starts from the (a) ICT and (b) finance sectors in US in 2013.

- **How is financial market impacted by cyber-security events?**

The aim of this study was to better understand the impact of cyberattacks on financial market. For that, an event study methodology was applied, which attempts to measure informative relevance of an event and to analyze stock prices reaction after the release of new information. According to this approach, favorable (unfavorable) information generates an increase (decrease) in prices and therefore positive (negative) abnormal returns. This study analyzed two stock markets: NASDAQ, considered as a high-tech exchange market including various startups, and NYSE, viewed as an exchange market for well-established companies and thus less volatile. The event window (the period surrounding the event's date) was defined as [-1, 3], i.e., one day before and three days after the event, during which the event's influence was observed on the market price. The market model with data from 120 trading day estimation period (the period prior to the event based on which normal return is estimated) was used. Thee analyses were conducted, related to the first accident date, the first notice date of the cyberattack, and original loss start date.

Results show that during the event window with day 0 as the first accident date, cumulative abnormal returns were of -0.03% and 0.48% for NASDAQ and NYSE markets respectively. The performed counterfactual analysis for the NASDAQ market revealed that not attacked firms generated 0.9% of cumulative abnormal returns against -0.75% for attacked ones. Thus, cyberattacks led to an average deficiency of 1.65% in cumulative abnormal returns and a lack of 0.86% in returns on average during the event window. Furthermore, for the first notice day, results demonstrate that a cumulative loss of 0.65% on average was generated during the event window. Confirmed by the counterfactual analysis, not attacked firms generated a cumulative total return of almost 1.3% compared to a cumulative loss of 0.15% for the attacked ones.

- ### Who are cybercrime perpetrators and what organizations do they target?

This study analyzed the relationship between the characteristics of cybercrime perpetrators, i.e. whether it is an individual or an organization, and the characteristics of their target firms. Focusing on firms' intangible assets, it was assumed that cyberattacks are more likely to occur on firms having more intangible assets. Adopting a quantitative approach, a model was developed, which accounted for several attributes of the attacked entity including proxies for different intangible assets of the attacked firm. A correspondence analysis and a set of logit regressions with a dependent variable as the binary choice of an attack conducted by an organization or an individual and internal and external entity were performed.

The analysis showed that there is an increasing probability that the attack is committed by an organization if target firms have larger number of employees. Similarly, the probability of cyberattack performed by an organization increases for R&D intensive target firms that have higher R&D expenditures. Overall, the probability of an attack carried out by an organization increases as total assets of the target enterprise increase.

Acknowledgement: This blog post summarizes the main findings of the work led by Professor Ahmed Bounfour, European Chair on Intangibles, Université Paris Sud, on the evaluation of the impact of cyberattacks on intangibles both at the firm and macro levels. This scientific work is conducted within the EU H2020 Project HERMENEUT (Enterprises intangible Risks Management via Economic models based on simulatioN of modErn cyber-aTtacks): www.hermeneut.eu

Contact: Ahmed Bounfour, Professor, Paris-Sud University, Scientific coordinator, HEMENEUT, European chair on intangibles. Email: Ahmed Bounfour@u-psud.fr