This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740322

The effects of cyberattacks on listed firms

November 6 2018

This blog post summarizes the main findings of the work we conducted on the evaluation of the impact of cyberattacks on financial markets.

The effects of an economic event on firms' value is a recurring theme in economics and management sciences. Finance theory suggests referring to financial market data in order to measure the impact of a specific event on the value of a firm through event study methodology. This methodology attempts to measure informative relevance of an event and to analyze stock prices reaction following the release of new information. According to this perspective, with a conjunction to the theory of signals, favorable (unfavorable) information generates an increase (decrease) in prices and therefore positive (negative) abnormal returns. Since the work of Dolley (1933) in which he investigated the effect of stock splits on stock prices, event study methodology had been adopted in different fields such as accounting and finance, management, marketing and information systems.

Event study

Our study is subsequent with prior ones covering event studies under the absence of abnormal return assumptions. The rejection of this hypothesis implies a modification of investors' expectations for one or several companies. However, the non-reaction of financial markets may arise from the lack of new information incorporated by the event or market inefficiency. Defined as the difference between the observed and theoretical profitability, the abnormal return is the crucial measure for event studies. In fact, a security performance and/or profitability may only be considered as “abnormal” relative to a defined benchmark or a theoretical model generating ex ante expected return.

In event study analysis there are two important definitions; event windows and estimation period. The event window refers to the period surrounding the event's date, during which the event's influence is being observed on the market price. Although the chosen window varies in the literature, the trend is towards shortening it to ensure that measured effects are due to the analyzed event. Moreover, measuring the impact of an event for a large sample of companies and in different moments might isolate the impact of an event. The estimation period refers to the window prior to the analyzed event based on which researchers will predict normal return according to a chosen model. The length of the estimation period plays a crucial role in event studies since it may affect estimated model parameters and therefore the power of statistical tests. However, there is no specific rule related to the length of the estimation period. The estimation period is usually promoted between five and eight months for daily studies and between twenty and sixty months for monthly studies to avoid estimation bias.

In this study, in order to control for potential leakage of information prior to the announcement, we include the preceding day of the event. Consequently, we define [-1, 3] as our event window. Furthermore, we opt for the market model with a data from 120 trading day estimation period. Two stock markets are studied; first the NASDAQ which is considered as a high-tech exchange market including various startups and Internet and electronic firms. Its stocks are considered more volatile and growth oriented. The second, the NYSE (Auction market) which is considered to be an exchange market for well-established companies and it is less volatile compared to NASDAQ.

We have conducted three different analysis which takes into account as the day zero;

- the first accident date
- the first notice date of the cyberattack
- original loss start date

First accident date

Our results show that during the accident window with day 0 as the first accident date referring to the beginning of the cyberattack, American companies were expected to generate a mean return of 0.49% for NASDAQ-listed companies and almost 0.42% for NYSE-listed ones. However, due to cyberattacks we notice a cumulative abnormal return of -0.03% and 0.48% for NASDAQ and NYSE markets respectively. In order to deepen our analysis of the impact of cyberattacks on financial market valuation of attacked companies, we opt for the counterfactual analysis methodology for the NASDAQ market. In that sense, we notice that counterfactual not attacked firms generates 0.9% of cumulative abnormal returns against -0.75% for attacked ones. As a result, cyberattacks lead 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. Figure 1 shows the cumulative average abnormal return (CAAR) obtained from NASDAQ data.

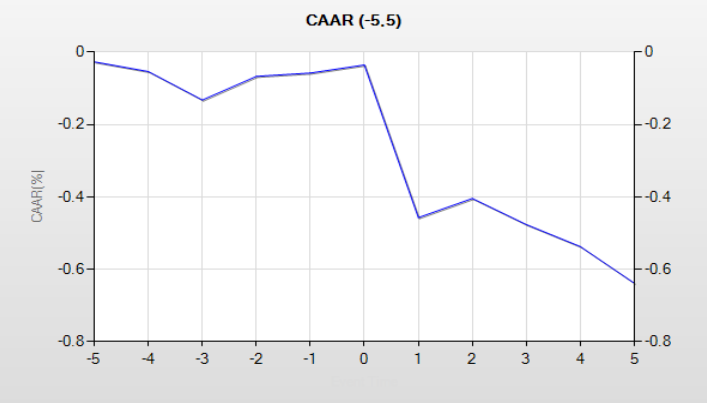

Figure 1: Cumulative average abnormal return after the first accident date in NASDAQ.

First notice date

Our second analysis takes into account the first notice date which is the date on which the case was initially reported or a notice was received. Based on the market model, we expect that investing in our panel would generate a cumulative total return of 0.83% on average for the NASDAQ and cause a loss of 0.53% for the NYSE market. However, an investment realized during the first notice date of a cyberattack engender in reality 1.37% and 0.125% respectively. In fact, detecting that the company was a victim of a cyberattack reveals her performance on the high-tech stock market (NASDAQ) ensuing a cumulative abnormal return of 0.54%. However, in the NYSE such news is perceived adversely through an average loss of 0.17% during the notice day and the following one too. As a

result, a cumulative loss of 0.65% on average would be generated during the event window. This result is consolidated through the counterfactual analysis according to which the not attacked firms generate a cumulative total return of almost 1.3% instead of a cumulative loss of 0.15% for the attacked ones.

Original loss start date

The last analysis is based on the original loss start date represent the date on which a loss began due to a cyberattack. For the NASDAQ, despite an average abnormal return of 0.016 during the event day, such events generate negative returns which are amounted to -0.015 during the following day and -0.003 the day after. This observation is consolidated through the counterfactual analysis. In fact, the beginning of loss is reflected in a fall of average abnormal returns from 0.192 down to -0.213. Moreover, we notice that the average cumulative abnormal returns of not attacked firms (0.19%) overcome attacked firms (-0.73%). However, the NYSE-listed companies seems to be less sensitive to theses events. In fact, the original loss start date might lead to a mean cumulative abnormal returns of 0.4% during the event window and a spread of 0.3% through the counterfactual analysis. By the end of loss issued from cyberattacks, financial market generates 0.22% and 0.39% average cumulative abnormal returns for both NASDAQ and NYSE successively during the event window.

European context

Extending our results for EU countries (France, Germany and the UK) gives a negative cumulative abnormal returns of 0.77% during the event window [0.3] for UK companies. Moreover, we notice that the average total return of attacked French firms drop during the event window [0.3] from 0.006 to -0.001 for and from 0.0001 to -0.006 for German firms. Furthermore, as soon as the cyberattack is reported, the average total return drops to 0.0002 (from 0.00435). This observation is confirmed for French and German companies where we notice a cumulative abnormal return of -0.445% and -0.98% successively.

In France, the announcement of the original loss period (start and end dates) is associated with two major observations. On the first hand, a decrease in the cumulative average abnormal returns of almost 0.37% during the original loss start date windows. On the other hand, a decrease of 0.2% on the cumulative abnormal returns average during the original loss end date windows. However, we notice that the German and UK financial markets do not react immediately to such announcements. In that sense, the analysis of the original loss start (end) dates reveal a positive cumulative abnormal return of 0.76% (-0.54%) and 0.34% (0.2%) for Germany and the United Kingdom.

Acknowledgement: This is the second of a set of blog posts which summarize 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