Hacking the market: Systemic contagion from cybersecurity breaches

Virtually not a month goes by without a new disclosure of major cybersecurity breaches at organisational and corporate levels. An unrelenting flow of news in this area takes us from financial services companies to regulators' offices, from major utilities to transport corporations. No one seems to be secure, no one is out of reach for cyber criminals.

In this year alone we have learned about the Uber hack that affected as many as 7 million U.S. drivers' records and 57 million customers records. In this case, we also know the price companies pay to 'remedy' the hacks: Uber reportedly transferred $100,000 to the hackers in exchange for a promise to delete stolen data. Whether or not they complied in the end, we simply do not know: once stolen, data is virtually impossible to trace, even after a ransom is paid in full.

This September we have also witnessed the discovery of the SEC hack. The Securities and Exchange Commission – much feared watchdog of the U.S. financial markets – had experienced a massive breach of its non-public corporate data storage system, known as the Electronic Data Gathering, Analysis and Retrieval system, EDGAR. Only two weeks before that, Equifax disclosed that in a massive hacking attack, the company lost personal information of some 143 million Americans.

In its August 2017 annual report, the National Infrastructure Advisory Council (NIAC) noted that "Cyber is the sole arena where private companies are the front line of defence in a nation-state attack on U.S. infrastructure. When a cyber attack can deliver the same damage or consequences as a kinetic attack, it requires national leadership and close coordination of our collective resources, capabilities, and authorities." Despite this realisation, according to NIAC, today, the U.S. authorities and private sector players "are falling short" of what is needed to "support the cyber security of high-risk assets."

Ironically, while the governments and private sector leaders across the OECD countries appear to be aware of the magnitude of the cyber security threats to private and regulatory markets infrastructure, official reports on cyber threats appear to be unconcerned with two key aspects of the risks and uncertainties surrounding these attacks: their systemic nature and the potential for contagion from cyber security threats against a specific organisation or enterprise to other organisations and companies and broader markets. In fact, the two key words "systemic" and "contagion" do not feature together in the literature relating to cyber security.

Date originally posted: 2017-11-28

Permalink: http://blogs.lse.ac.uk/businessreview/2017/11/28/hacking-the-market-systemic-contagion-from-cybersecurity-breaches/

Blog homepage: http://blogs.lse.ac.uk/businessreview/

This is a major oversight on behalf of all parties potentially affected by cyber security threats, from the government security agencies, to regulatory and supervisory agencies, to investors trading in the public markets.

In our recent paper, we looked at the systemic contagion effects from all disclosed cybersecurity events experienced by the publicly listed companies over the period starting with January 2005 and ending April 2015. We use Exponential GARCH methodology to explore two hypotheses relating to cybersecurity breaches:

(1) Whether cybersecurity events can cause enough shocks to corporate finance fundamentals of traded companies to trigger significant devaluations of the traded equities; and

(2) Whether such events pose systemic threats to the broader financial markets, both domestic (the markets on which the impacted company is listed) and international (financial exchanges linked to the domestic exchange).

Our findings are striking and some are novel to the literature on the financial implications of the cybersecurity threats.

Firstly, we show that hacking events are becoming more prevalent and severe in terms of numbers of clients' record impacted since 2010, when compared to other cyber security breaches, such as loss of hardware, theft of data or hardware, and accidental releases of data, to name but a few. Extending our data to cover the period of May 2015 through September 2017 confirms this trend.

Secondly, our Cumulative Abnormal Returns (CAR) analysis shows that the average stock market reaction to cyber attacks in the ten-day window following the events has become increasingly negative. Whereas between 2005 and 2008 the average CAR may fall by 3 per cent, since 2010 the same abnormal returns have fallen over 5 per cent, with 2014 and 2015 presenting the largest average falls of over 10 per cent associated with hacks. Again, extending the data to 2017 confirms the trend, with average CAR declines rising in magnitude to 12 per cent.

Thirdly, our CARs analysis shows that stock markets increasingly efficiently price the specific risk associated with hacking events, representing the perceived reputational, legal and regulatory costs associated with a breach in regulatory platforms.

Our main results, however, concern potential spillovers of volatility from cybercrime events to the affected company stock, to the exchange on which the company stock is traded and beyond that, to other exchanges.

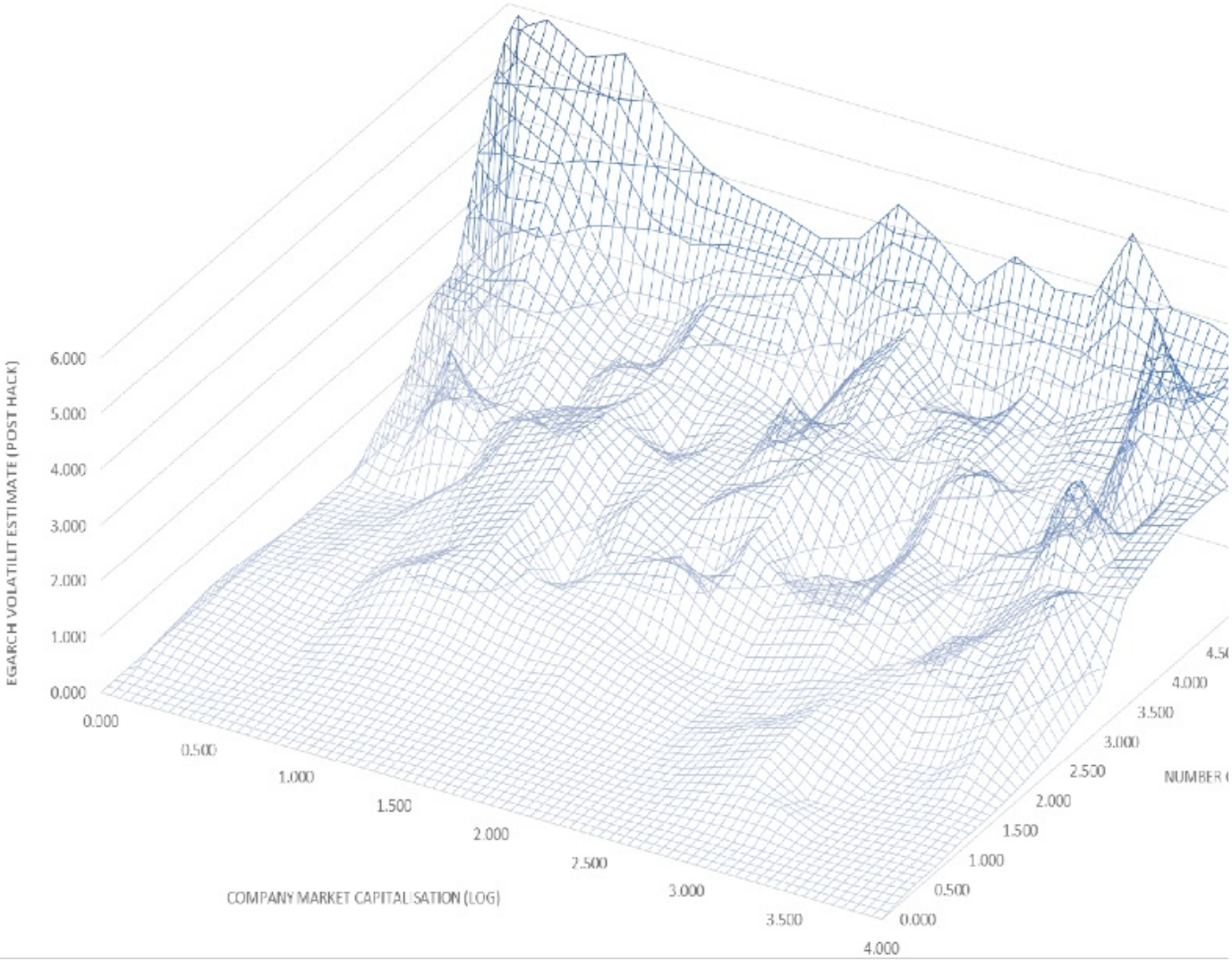
In Figure 1 below, we present an analysis of the volatility effects that have transferred to companies based on the number of clients' records exposed and the market capitalisation of the company that has suffered from the cybercrime. The data makes it clear that there is a significant positive correlation between the volatility impact and the cybercrime and the number of clients' records exposed: the larger the scale of the event, the larger the contagion transmission. It is also notable that smaller companies (in terms of market capitalisation) appear to be more susceptible to the cybercrime.

Figure 1. Volatility spillovers due to data breaches compared to the company market capitalisation and number of clients records affected

Date originally posted: 2017-11-28

Permalink: http://blogs.lse.ac.uk/businessreview/2017/11/28/hacking-the-market-systemic-contagion-from-cybersecurity-breaches/

Blog homepage: http://blogs.lse.ac.uk/businessreview/



In our data, we find that the vast majority of the stock market contagion stemming from the information release of a cybercrime event was based on idiosyncratic contagion (instances where the cybercrime event has been identified as unique to the company rather than the wider stock market).

However, since late 2014 over 12 per cent of cybercrime events resulted in systematic contagion to the wider national stock exchange in which the company was traded. This key finding can be explained through the increased sophistication of cyber-attacks, increases in abnormal cumulative losses to the targeted company, and a significant rise in the number of client records that have been illegally exposed. In addition, the rise of the Darknet/web created an international market in which this data can be readily sold.

Date originally posted: 2017-11-28

Permalink: http://blogs.lse.ac.uk/businessreview/2017/11/28/hacking-the-market-systemic-contagion-from-cybersecurity-breaches/

Blog homepage: http://blogs.lse.ac.uk/businessreview/

Systemic contagion due to cyber events, first detected in 2014, remains a feature of the market's risk environment today. Both, the Equifax breach and the Uber hack represent the cases that by volume of client accounts affected and the size of company in market capitalisation terms serve as prime examples of the cybersecurity events that pose such risks. While the jury is still out on whether Uber disclosure will trigger volatility spillover to other U.S.-listed companies, Equifax data clearly fits our model. Within the first week of the hack disclosure, Equifax stock dropped almost 32.3 per cent. Thereafter, the share price recovered, but 3 weeks after the attack, Equifax shares were still trading at 25.5 per cent discount on pre-event price. Bid-ask spread on shares also experienced substantial widening, with the spread rising by more than 50 per cent within the first week of post-event trading. Share price volatility rose and there was a clearly detectable contagion from Equifax price dynamics (volatility) to the New York Stock Exchange. Two and a half months after the cyber breach, Equifax shares continue to trade at a 23 per cent discount.

As noted by NIAC 2017 report, "The scale, scope, and frequency of cyber attacks on digital and physical infrastructure systems is growing rapidly. Threats are escalating as more sophisticated and organized attackers are designing targeted attacks to damage or disrupt vital services and critical physical systems." While the authorities continue to focus much of their resources on protecting physical infrastructures, such as the national grids and vital public services provision platforms, empirical evidence points to the rising threat of financial impact contagion from cybersecurity breaches and hacks.

♣♣♣

Notes:

- *This blog post is based on the authors' paper What the Hack: Systematic Risk Contagion from Cyber Events (September 7, 2017)*
- *The post gives the views of its authors, not the position of LSE Business Review or the London School of Economics.*
- *Featured image credit: Cybersecurity, by typographyimages, under a CC0 licence*
- *When you leave a comment, you're agreeing to our Comment Policy.*

Constantin Gurdgiev is Professor of Finance with the Middlebury Institute of International Studies at Monterey, California and an Adjunct Professor of Finance with Trinity College Dublin in Ireland. Professor Gurdgiev works in the areas of investment markets, with specialisation on macroeconomic and geopolitical risk impacts, and heads the Middlebury Institute's Impact Hub – an experiential learning and research program in environmental, social, and governance risk impact. He advises a range of institutional and corporate clients on macroeconomic risks in European and Russian financial markets, and writes a popular blog on economics and finance at http://trueeconomics.blogspot.com/

Shaen Corbet is a lecturer in finance at Dublin City University Business School in Dublin, Ireland. Dr. Crobet specializes in empirical research in finance and has previously worked as a commodities and equities trader and with the Financial Stability Department at The Central Bank of Ireland.

Date originally posted: 2017-11-28

Permalink: http://blogs.lse.ac.uk/businessreview/2017/11/28/hacking-the-market-systemic-contagion-from-cybersecurity-breaches/

Blog homepage: http://blogs.lse.ac.uk/businessreview/