

What the Hack: Systematic Risk Contagion from Cyber Events

Shaen Corbet

DCU Business School, Dublin City University, Glasnevin, Dublin 9, Ireland

shaen.corbet@dcu.ie

Constantin Gurdgiev

Middlebury Institute for International Studies at Monterey, California

Trinity Business School, Aras an Phiarsaigh, Trinity College, Dublin 2, Ireland

cgurdgiev@miis.edu

SEPTEMBER 2017

ABSTRACT:

This paper examines the impact of cybercrime and hacking events on equity market volatility across publicly traded corporations. The volatility influence of these cybercrime events is shown to be dependent on the number of clients exposed across all sectors and the type of the cyber security breach event, with significantly large volatility effects presented for companies who find themselves exposed to cybercrime in the form of hacking. Evidence is presented to suggest that corporations with large data breaches are punished substantially in the form of stock market volatility and significantly reduced abnormal stock returns. Companies with lower levels of market capitalisation are found to be most susceptible. In an environment where corporate data protection should be paramount, minor breaches appear to be relatively unpunished by the stock market. We also show that there is a growing importance in the contagion channel from cyber security breaches to markets volatility. Overall, our results support the proposition that acting in a controlled capacity from within a ring-fenced incentives system, hackers may in fact provide the appropriate mechanism for discovery and deterrence of weak corporate cyber security practices. This mechanism can help alleviate the systemic weaknesses in the existent mechanisms for cyber security oversight and enforcement.

Keywords: EGARCH, Financial Markets, Cybercrime, Regulation.

JEL classifications: G15, G32, G38.

We wish to thank Professor Allison Christians of McGill University for helpful suggestions on edits and positioning of this paper.

1. INTRODUCTION

Asymmetric information refers to a decision-making environment in which one party to an economic transaction possesses superior information to that of another party, resulting in economic outcomes that are skewed in favour of the former to the detriment of the latter. One such example is that of consumers and business counter-parties, who rely on companies to safeguard their personal and company-specific data, without explicit knowledge or understanding of the internal safeguards and standards placed by the data-holding company on their data protection infrastructure (e.g. Moore, 2010). It is a relationship mostly based on trust between data providers (consumers or business counterparties) and the company, and it can serve as a channel for data loss to cyber security violations. Another source of market re-allocations from consumers and end-users of data services to cybercriminals is the asymmetric nature of cybersecurity threat timing. Here, companies subjected to external cyber threats are forced, by the nature of these threats, to be reactive to attacks, and attackers possess first mover advantages (see, for example, Be'ery, 2014).

In theory, the risk to corporate reputation and the prospect of breach-related legal judgements and awards can act as a key deterrent against cyber-security strategies and practices that can lead to a data loss or breach or can facilitate or enable external attacks (Farrell, 2016 and NCI, 2016). Unfortunately, in practice, this may not be enough as the level, the intensity and the complexity of cybercrime events continue to grow (Klop, 2016 and Drinkwater, 2016).¹ Crucially, as the scale and frequency of cyber-attacks rise, the negative reputational and direct costs of such attacks

¹ One recent example of growing complexity of cyberattacks is provided by a series of coordinated attempts on French banking institutions that involved simultaneous attempts to distribute email-based malware and illegally collect customer's data using traditional phone systems (see Mawad and Valentini, 2017).

increase, generating material shocks to individual companies valuations and, potentially, spilling over to broader financial markets.

Figure 1 presents data on the frequency of cybercrime events impacting on publicly traded companies. As we note below, modern cybersecurity environment is characterised by increasing frequency, severity and complexity of cyber threats. One specific form of cybercrime that is becoming ever more prevalent, is a breach where a hacker, who may possess more technological information and knowledge than that of the target company (Moore, 2010), or have an advantage of the first mover, relative to the company security (Be'ery, 2014), breaches the company's firewall to steal client data.

Not surprisingly, cybersecurity crimes and risks are now the focal points of attention amongst policymakers, regulators, supervisors and enforcement officials across a range of economic sectors. A key example, and probably the most advanced relative other sectors, is the financial services. This fact is reflected in rapidly expanding regulatory and supervisory efforts to address the key risks of cybersecurity from multinational and international financial regulation bodies (e.g. the Bank for International Settlements), national legislators, Central Banks and financial regulatory authorities (e.g. the U.S. Fed and the ECB) as well as industry-own collective representative bodies (e.g. American Banking Association Cyber and Information Security Working Group).

In one example, OFR (2016) focuses the discussion of systemic threats to the U.S. and global financial stability on a range of cybersecurity risks. OFR (2016: page 4) defines three main categories of cybersecurity impacts on financial stability, namely “the lack of substitutability for the services that many financial companies provide; the potential loss of confidence in a financial company by customers; and the threat to data integrity”. The OFR (2016: 38) goes on to state that

the U.S. Treasury “ranked vulnerability to malicious cyber activity as a top threat with substantial potential impact.”

While the growing severity of cybersecurity risks to the global financial system and broader corporate institutional systems is a matter of consensus, as described below, little is known about the systemic channels for cybersecurity contagion across financial markets (see map in the Appendix), especially the equity markets and bond markets. We intend to fill this gap in the present research while focusing on equity markets.

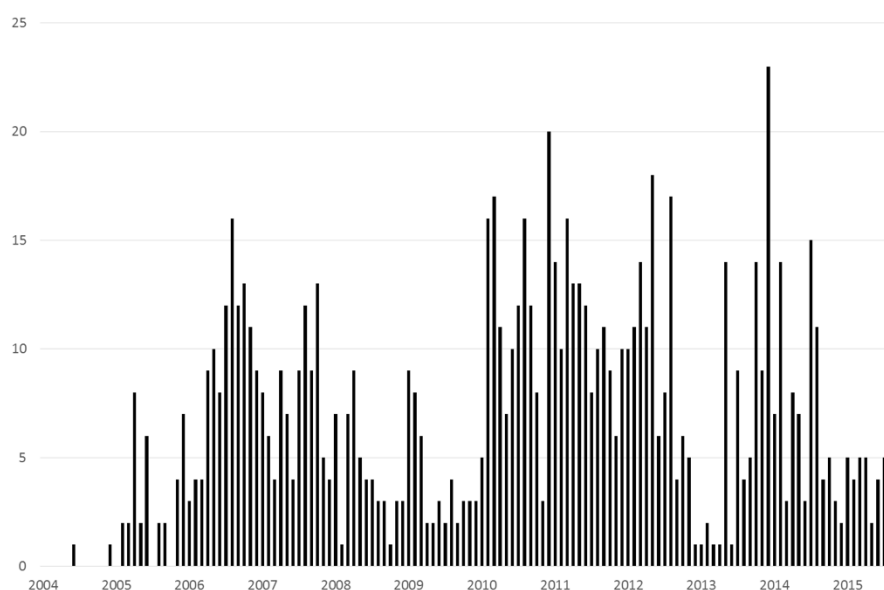


Figure 1: The frequency of cybercrime events targeting publicly traded companies.

Note: The full sample period extends from January 2004 to August 2015. Only events where company statements and mainstream media reports have been issued are included.

To this end, this paper starts by empirically examining the evidence for the unexpected transmission of cybercrime events to equity markets valuations during the period of 2005-2015.

We show that starting with 2014, these transmissions reach beyond the impact on stock prices of the company subjected to cybercrime in a variety of jurisdictions. Specifically, we show that

cybercrime events have an impact that crosses exchanges and borders. In effect, trading or portfolio links or institutional structures such as international subsidiaries help propagate risk contagion effects, including for cyber-security risk spillovers. To the best of our knowledge, this is the first paper in the literature on cyber-security that provides concrete evidence and empirical tests for systemic contagion channel transmitting cyber-security risk from one company share price to other sectorally or market-related companies as detailed in the Appendix.

Even absent direct evidence of systemic contagion from individual attacks to broader exchanges to-date, some regulatory studies, white papers and public statements by regulatory and supervisory officials have warned about the importance of the potential systemic contagion channel relating to such breaches. CPMI-IOSCO (2016) warns about the potential for cyber security risk to monetary and financial institutions (MFIs) becoming systemic through contagion effects and call for pre-emptive testing of MFI systems as “an integral component of any cyber resilience framework” (CPMI-IOSCO 2016, page 18, paragraph 7.1). Similarly, Dahlgren (2016a) warns that “cyber threats pose a potential systemic risk to financial stability through the disruption or corruption of critical payment, clearing and settlement systems and related data.” A glaring and obvious omission on this list is a failure to include other potential channels for systemic risk transmissions, including exchanges and over-the-counter markets. Our study fills this empirical gap by providing direct evidence of systemic contagion that sees the propagation of share price volatility from the company directly impacted by cyber security event to the company-listing exchange and the exchanges linked to the listing exchange. We detail these and other channels for impact transmission in the Appendix.

Beyond the systemic nature of the threat, the magnitude of costs and disruptions imposed on the economies by cyber-attacks is growing. According to the EU authorities, as reported by Stearns

(2016), “network security incidents resulting from human error, technical failures or cyberattacks cause annual losses of 260 billion euros (\$288 billion) to 340 billion euros.” Our findings, presented in this study, suggest that these figures are likely to underestimate the full impact of cybersecurity breaches by excluding the costs of contagion. Moreover, despite the common perception that cyber security vulnerabilities apply primarily to private sector companies, the evidence is mounting that central banks and regulators themselves are not immune to cybercrime. In spring 2016, the Bangladeshi Central Bank became a victim of a cyber-attack resulting in a theft of \$81 million (Finkle and Spicer, 2016). Whereas, in May 2016, the Greek Central Bank became a victim of a hack by the Anonymous group (The Economist, 2016).

It is worth stressing here, once again, that despite this evidence, to-date, no empirical study documented the extent of the cybersecurity risks impact on equity valuations across individual impacted firms (e.g. corresponding to Cumulative Abnormal Returns, CARs, related to cybersecurity risks) or the extent of the individual events spill over to broader markets valuations. We provide such evidence below.

OFR (2016) identifies not only a range of cybersecurity threats faced by modern enterprises, but also key channels for transmission of these threats within corporate financial functions, and crucially for our study, to other companies linked to the target of the threat through counterparty and other arrangements. As stated in the CFR (2016: 39) “Cybersecurity threats impose direct costs on firms. These costs include the loss of funds or customer records, added IT spending, remediation costs, reputational costs, and legal expenses.” However, OFR (2016) does not provide an empirical analysis of these risk transmission effects. We directly model the internal effects of cybersecurity events onto firm valuations through the concept of CARs, referenced above.

Furthermore, as noted by OFR (2016), regulators and supervisory authorities have recognised the potential for contagion from a cybersecurity threat to one enterprise to broader markets. We provide direct evidence of such contagion effects through our analysis of volatility spillovers tied to cybersecurity incidents. Our research adopts an EGARCH methodology to investigate the stock market volatility of publicly traded companies generated in the immediate aftermath of a hacking or other cybersecurity breach event over a period from 2000 to 2015. We directly examine these events regarding the size of the target company, the type of cybercrime that has occurred and the number of client's records that have been released to the public. The key channels through which such spillovers manifest themselves publicly (see Appendix for details), in our opinion, are:

- The channel of changes in equity prices dynamics for the impacted firms (own impact),
- Spillover to other companies linked to the impacted firm through shares listings on the same exchange (own exchange impact) and, more broadly,
- Spillover from the impacted firm to other exchanges (cross-exchanges impact).

All three effects are consistent with the views for potential impact propagation and contagion expressed by regulatory and supervisory authorities, e.g. OFR (2016).²

The remainder of the paper is organised as follows. Section 2 discusses the relevant literature on the influence of cybercrime on financial markets. Section 3 addresses the methodology used in our research. Section 4 focuses on the data and descriptive statistics while providing evidence of growing complexity, frequency and severity of cybersecurity events. Section 5 introduces the

² It is worth mentioning here that according to OFR (2016:40) “cybersecurity incidents could have macroeconomic consequences”. While we leave this hypothesis unaddressed in our research, our results concerning emerging evidence on cross-exchanges transmission of cybersecurity events make a first step toward providing support for this statement.

results of the EGARCH methodology identifying the stock market volatility effects of the identified cybercrime events on publicly traded companies. Section 6 concludes.

2. CURRENT EVIDENCE ON MARKETS IMPACT OF CYBERSECURITY RISKS

To date, there has been no research identified that focuses specifically on the interlinkages between the differing types of cybercrime and financial market volatility, spillovers or contagion from cybersecurity breaches to financial markets, or systemic stability risks (McKendry and Macheel, 2015 and Gurdgiev, 2016). However, there has been some research conducted in the areas of changing nature, frequency, severity and impact of cybercrimes, on channels through which cybercrime can impact share prices of firms directly affected by cybersecurity events, and on possible channels for contagion from cybersecurity events to broader markets. In this section, we provide a systematic review of research to-date and link it to our analysis. As such we look at three areas of relevance in the current literature on cybersecurity risks, as relevant to the financial markets and financial risks: the changing nature of cybersecurity risk environment, channels through which cybersecurity risks can impact firms' valuations, and any indicative or actual evidence of contagion.

2.1. Changing Environment of Cybersecurity Risks

The extent of the threat posed by cybersecurity risks is hardly a matter of controversy. In the early literature, Haines and Johnstone (1997) identify the numerous methods through which cybercrime can occur, finding that advances in communications, information systems and cyber electronic innovations increasingly dispel the myth that crime stops at the border. A decade later, Rollins and

Wilson (2007) warned that if prevalent trends in cybercrime continue, computer attacks will become more numerous, faster and more sophisticated. Moreover, as far back as in 2010-2011, the Government Accountability Office stated that U.S. government agencies might not in the future be able to respond effectively to such attacks. Further, Ionescu, Mirea and Blăjan (2011) found that the economic crisis created the incentives and preconditions for a substantial increase in computer crime and fraud, with incidents of illegality presenting exponential growth in the period 2007 to 2011. Overvest and Straathof (2015) “results suggest that a ten percent increase in the number of internet users worldwide raises the number of attacks by about eight percent. Bandwidth in the country of origin and economic ties are also significantly related to attacks.”³

Regarding markets infrastructure, numerous research papers identify the ease with which stolen data can be purchased and sold through a network of illicit, secretive and easily accessible mechanisms (Holt and Lampke, 2010). Similarly, cybersecurity breaching tools are now also available to a broader range of players (starting with Holt, 2003). In one recent example, earlier in 2016, cybersecurity firm Kaspersky Labs has uncovered an online marketplace for trading in illegally obtained data, and sales of access to more than 70,000 hacked corporate and government servers for as little as \$6 each (Khrennikov, 2016). Based on Khrennikov’s report, hackers trading in “the market, called xDedic, ...have ditched their traditional business model of just selling passwords and have graduated instead to earning a commission from each transaction on their black market.” In other words, expansion in illicit data and software markets is now being matched by growing strategic sophistication of hackers.

³ An added threat, not explicitly discussed herein, but also subject to the even greater potential costs, risks, systemic uncertainty and enforcement problems, is the evolution of the Artificial Intelligence (AI) (see Yampolskiy (2016)).

Per CGI (2017), crucially, the negative impact of cybersecurity breaches is growing over time. Cybersecurity violations of 2013 vintage resulted, on average, in 0.2% drop in the affected companies' shares on the Friday following disclosure of the event. In 2014 the average drop was 1.5%, and in 2015 and 2016 - 2.7%. This is consistent with our findings reported below both regarding the severity of own-firm impacts and the spillovers across firms listed on the same exchange and across exchanges. At the industry level, this is reflected in growing regulatory recognition of the rising importance of these threats, as exemplified by Norton, Rose and Fulbright (2016) in the context of continuously evolving and expanding corporate directors' responsibilities relating to cybersecurity threats.

2.2. Firms Valuations and Cybersecurity Risks

Cybersecurity risk transmits to firm equity valuations across a causal chain of shock pathways. At the starting node of these pathways, threat actors that may originate a cybersecurity event include nation states, organised crime, activist hackers or hacktivists, as well as insider threats (including insider negligence, intent to harm or intent to benefit from cybersecurity breaches). Successful cybersecurity breaches or actions by these actors generate one or several key financial risks to enterprise impacted by their actions, including, as identified in OFR (2016: 41):

- Direct financial costs and costs arising from physical damages
- Theft of intellectual property
- Software and data destruction or deletion
- Business disruption and post-attack/post-breach remediation costs
- Loss of customers and pricing power

- Costs of regulatory fines and legal settlements, as well as costs of increases in future insurance premiums
- Third parties liabilities.

All of the above costs would have a material impact on share prices, as consistent with a range of traditional factor models, rational valuations theory, as well as arbitrage pricing theory. In line with this, according to OFR (2016: 42): “some U.S. financial firms reported cyber-security as a key risk in 2015 10-K filings reviewed by the OFR. Cybersecurity references in 2015 Form 10-Ks were nearly double those in 2013 10-Ks”. 10-K risk filings reflect factors that are deemed material to equity valuations and firm’s financial performance.

According to the data from PricewaterhouseCoopers (2016), more than 20 percent of all large corporations and organisations across all sectors, except for Education & Non-Profit and Transport & Logistics have budgeted in excess of USD10 million or more on information security and cybersecurity protection in 2015. This further highlights the fact that a significant number of larger size enterprises (USD 1 billion or more in gross revenue) in the U.S. are viewing cybersecurity risks as material to their shareholder's values.

Finally, SEC’s Regulation SCI, since November 2015, treats cybersecurity risk as material, on par with operational risks, and has produced a set of rules to establish cybersecurity compliance for investment advisers and intermediaries (FSOC, 2016). In line with regulatory concerns, cybersecurity breaches have attracted the attention of academic and practitioner research into the links between cybercrime and stock market valuations of the impacted firms. Taking the most recent evidence, a recent study by CGI Group and Oxford Economics (CGI, 2017) documented the effect of large scale cybersecurity events on an affected firms’ share prices. The study looked at 315 events over the 2013-2016 period and focused on events that are rated as “severe” or

“catastrophic” on the Gemalto Breach Level Index. Those “severe” or “catastrophic” events affected 65 publicly traded companies, listed on one or more of seven global stock exchanges. Per CGI (2017), in the wake of a severe breach in cybersecurity, share prices of listed companies fall on average 1.8% (and up to 15% in some cases) within the first week following the breach. Two-thirds of the companies that were the subject of a severe cybersecurity breach experienced a decline in their shares prices when compared to other companies in their peer group. Crucially, the study suggests that the declines in stock prices resulting from cybersecurity breaches are permanent, as repricing of company shares may reflect investors’ expectations of future profitability. It is worth noting that CGI (2017) study was conducted using Difference-In-Difference (DID) methodology that does not permit the authors to draw any conclusions as to the volatility contagion from cybersecurity breaches in one listed company to other companies traded on the exchange (within-exchange contagion) or to other exchanges (cross-exchange contagion). Our study addresses this issue. Also, the CGI study was based on a severely limited data set relating to companies listed on FTSE exchange and encompassing only 65 cases of severe breaches over a short term horizon. We also address these issues in our research below.

Before CGI (2017) research, some academic studies produced a range of insights into cybersecurity risks’ adverse effects on share prices of the directly impacted firms (Gwebu et al., 2014). These include Gatzlaff and McCullough (2010), Goel and Shawky (2009), Telang and Wattel (2007), Acquisti et al. (2006), Ko and Dorantes (2006), Cavusoglu et al. (2004) and Garg et al. (2003). However, a small number of other studies have disputed the conclusion of generally adverse long-term impact from cybersecurity risks on share prices (e.g. Kannan et al., 2007, Campbell et al., 2003 and Hovav & D’Arcy, 2003). Gwebu et al. (2014) look directly at profitability performance of companies affected by cybersecurity breaches and find that data

breaches negatively impact firm profitability, perceived risk and information transparency. They suggest that direct costs are more significant in generating profitability declines than indirect costs.

As an example of a less-conclusive research, Gordon, Loeb, and Zhou (2011) examined 121 security incidents involving 85 firms during the period 1995 to 2007. The authors found a significant impact of the news of cyber security breaches on the stock price of the involved company before 2001 and a significant decrease in the negative share prices' reaction to security breaches post-2001. That said, the authors recognise that in some cases, breaches continued to exert a significant impact on the market capitalisation of the individual firms even post-2001.

In summary, much of the research on the potential direct impact of cybersecurity breaches on firm's equity valuations suggests that cybersecurity events do hurt share prices of the firms subject to the attack or data loss. Furthermore, the channels through which cybersecurity risks impact stock prices are broadly defined in the literature and are consistent with traditional financial valuations models. However, despite this evidence, no study to date has examined the potential share prices volatility spillovers from the cybersecurity event to firm-own share prices, to the share prices of other firms related to the attacked enterprise through sectoral or exchange links, or spillovers to individual exchanges and across the exchanges. We intend to fill this gap in the literature below.

2.3 Evidence of Contagion

To-date, there is no significant empirical research literature on contagion properties of cybercrime and cybersecurity attacks and breaches in the context of the financial (equity or bonds) markets valuations. This is surprising, especially considering the evolving nature of the threats identified in the literature surveyed in the previous two sections on the review. It is also surprising in the

light of individual events and literature on operational and technological aspects of cybersecurity, as discussed below. The potential for systemic contagion, in fact, defines the very nature of the threat posed by cybersecurity risk (DTCC, 2014 and OFR, 2016).

Broadly-speaking, our review of the literature on cybersecurity risk contagion identifies four key channels through which cyber event risk can be transmitted from one company to the other and broader markets (see Appendix for more details). These are technology-centric channels, correlated risks channel, network contagion and increasing complexity of business operating and strategic environments.

Technology-centric channels for contagion of cybersecurity threats from one impacted organisation to other organisations related to it either through networks of counterparty relations or less directly through shared information and value chains (e.g. supply chain partnerships and co-shared technology platforms) has been well-established in academic and practitioner research. For example, Baldwin et al. (2016: 1) provide vector equation estimates of the threats to a range of IP services, over January 2003 - February 2011 period, showing “strong evidence of contagion between such attacks”. Acemoglu et al. (2013) link the technologically-networked transmission channels to the potential systemic contagion of cyber risks across networked organisations and the existence of incentives for organisations facing contagion risks to underinvest in shared risk mitigation strategies.

Similarly, the risk of cybersecurity breach contagion - technologically-driven and unrelated to asset valuations - has been long established as a key point of concern for regulatory and supervisory authorities in the financial services sector. Previously mentioned and referenced regulatory studies attest to this, and some other recent regulatory studies have focused explicitly on such risks. For example, Tendulkar (2013) provides an in-depth discussion of technology and operations-related

contagion channels for potential cybersecurity risks propagation within the financial exchanges. These concerns are echoed in the U.S. Office of Financial Research study from 2016 (Gulino, 2016). Heal and Kwnreuther (2004) and Heal and Kwnreuther (2007), followed by Felt and Grossklags (2009) set out some foundations for thinking about the contagion properties of different types of computer networks. Correlated and cascading risks - another channel for the propagation of cybersecurity risks - were identified and explored from a theoretical perspective in Schwartz and Sastry (2014). Notably, those studies do not cover shocks to equity prices.

Laszka and Schwartz (2016) link network contagion and security to incentives for engaging in cyber criminality, completing the dual causality argument from technological pathways for contagion to attacks incentives and back to contagion risks. Empirically, in a most recent example, contagion from a global malware or ransomware Wannacry event provides a clear picture of technologically-enabled propagation of cyber risks through networks of seemingly unrelated, widely distributed organisations. Following Kaplan, Sharma, and Weinberg (2011) view of expanding contagion threat being fueled by evolving operating and strategic environments, Jang-Jaccard and Nepal (2014: 973) note that: “significant growth of cyber attack incidents often with disastrous and grievous consequences” and specifically discuss “new attack patterns in emerging technologies such as social media, cloud computing, smartphone technology, and critical infrastructure” that act as potential channels for propagation and contagion.

Kuypers, Maillart and Paté-Cornell1 (2016) cover six years’ worth of cybersecurity incidents that span some 60,000 cases within a single large U.S. organisation. The authors find that: 1) The frequency of all cyber incidents is found to be increasing over time, primarily due to increases in frequencies of smaller incidents; 2) By type of incident, (Kuypers, Maillart and Paté-Cornell1, 2016:9) “the number of web browsing/USB incidents recorded over time. The total number of

incidents is slowly decreasing over time (2 events per month), while the number of incidents that require more than 10 hours of investigation remains relatively constant over time”; 3) Infections with “malware incidents occur much more frequently than the loss of devices...” and; 4) “Cyber security and cyber threats are rapidly evolving, with new vulnerabilities announced on a daily basis. Over the six years included in our data, changes in security safeguards, network structure, and security processes have occurred” (Kuypers, Maillart and Paté-Cornell1, 2016: 11). In simple terms, contagion risks are present in the cybersecurity environment, even though research on contagion risks in the financial market's responses to cybersecurity events in the context of equity prices is lacking. As noted earlier, we intend to fill this gap in the literature by looking at the evidence of equity valuations-linked contagion.

3. RESEARCH DESIGN AND METHODOLOGY

This paper empirically examines the effects that cybercrime events have had on the volatility of equity prices of publicly traded companies. The development and expansion of social media have generated an environment where information flows, and associated changes in market sentiment, are altered in seconds rather than minutes and hours. Keeping in mind that there are areas of the internet where hacking events and the tools to carry them out are readily available, it is no surprise that cybercrime events have become more frequent and more sophisticated just as both the impact of the cybersecurity breaches and the speed with which the news of such breaches reaches the markets have both increased.⁴

⁴ An added dimension to this investigation is posited by the predominance of the ‘insure and forget’ model of corporate responses to cyber threats (Egan, 2014 and PWC, 2014).

The question we want to explore here is whether these events can cause enough chaos to the technological capabilities and corporate finance fundamentals of traded companies to merit significant punishment in the form of financial market panic and devaluation of traded equity? Another key question is whether such events pose a systemic threat to the financial markets, both domestic (as the markets on which the particular impacted company is listed) and international (financial exchanges linked to the domestic exchange)?

Both Egan (2014) and PWC (2014) suggest that the prevalent view in the business community is that they indeed pose such a risk. Despite this, little evidence is provided by the authors to the extent of the first effect (relating to the first question), and no evidence is provided to address the second effect (relating to the second question above). To provide empirical answers to the two questions above, we identified the Exponential GARCH (EGARCH) model as the most efficient model to test these hypotheses⁵, using a dummy variable to determine the exact date on which the data breach occurred as stated in the media reports and company statements gathered.

The daily stock return is calculated as: $r_t = (P_t - P_{t-1})/P_t$. The ARCH(p) and GARCH(p,q) models impose symmetry on the conditional variance structure, which may not be appropriate for modelling and forecasting stock return volatility. The EGARCH models capture the most important stylised features of return volatility, namely time-series clustering, negative correlations, log-normality and long memory.

⁵ An intercept and deterministic trend were included in the Augmented Dickey Fuller (ADF) and Phillip Perron (PP) models. The trend was included to capture the reduction in average volatility that took place during the period prior to the data breaches. The ADF model tests whether the stock for each traded company contained a unit root in order to correct for serial correlation. PP tests employ a non-parametric estimator of the variance-covariance matrix with d truncation lags. The models lags structure was identified by sequentially removing the last lag until a significant lag is reached, giving the order of augmentation for the ADF test that minimised the Akaike information criterion. The results indicated rejection of the null-unit root hypotheses at a minimum of the five per cent level of significance. Therefore, the EGARCH(1,1) model was selected as the most suitable model to test the hypothesis established in this paper.

The specification we developed captures the volatility effects of cybercrime as follows:

$$r_{j,t} = b_{0,j} + b_{1,j} f_t^{domestic} + b_{2,j} f_t^{Gold} + b_{3,j} f_t^{oil} + b_{4,j} f_t^{ESTX} + b_{5,j} f_t^{DJI} + \varepsilon_{i,t}; \quad (1)$$

$j = 1, \dots, n - 1 \neq source\ company.$

In (1), the coefficient $b_{1,j}$ represents the domestic exchange returns of the company experiencing the data breach through cybercrime, $b_{2,j}$ represents spot gold prices, $b_{3,j}$ represents West Texas Intermediate oil prices, $b_{4,j}$ represents the Eurostoxx as a measure of EU stock market instability and $b_{5,i}$ represents the Dow Jones Industrial Average as a measure of US stock market instability. The inclusion of the international variables to adapt the model for ‘international effects’ is also found to be beneficial when attempting to segregate and investigate the stock market behaviour of the companies that have experienced cybercrime events.

Another advantage of the EGARCH model is to accommodate potential asymmetry in leverage effects in preference to a Threshold GARCH (TGARCH) specification because we wish to capture the entire distribution in preference to volatility tails in this framework. These asymmetries tend to occur when an unexpected decrease in price due to bad news increases volatility more than an unexpected increase in price because of good news. The model expresses the conditional variance of the variables as a nonlinear function of its past standard innovations.

Following Engle (2004), the variance equation of the EGARCH model to accompany the mean equations above is expressed as:

$$\ln(\sigma_{j,t}^2) = c_{0,j} + c_{1,j} (|Z_{j,t-1}| - E|Z_{j,t-1}|) + c_{2,j} Z_{j,t-1} + c_{3,j} \ln(\sigma_{j,t-1}^2) + \pi_1 \ln(\hat{\sigma}_2); \quad (2)$$

$$z_{i,t-1} = \frac{\eta_{i,t-1}}{\sigma_{i,t-1}}; \quad \eta_{i,t} = \{e_{i,t}, \varepsilon_{i,t}, \xi_{j,t}\}$$

$$\eta_{i,t} \sim Student - t(0, \sigma_{i,t}^2),$$

We include gold and oil price processes in the specification (1) to account for general underlying trends and sentiments in the financial markets. As shown in Ciner, Gurdgiev and Lucey (2013), gold and oil act as long-term hedges and safe havens for a range of financial asset classes, and that these relationships are also existent at the times of extreme stress in the markets and across a range of international markets. The specification (2) enables the testing of contagion effects from the designated company hacking event upon the domestic stock market in which the company is operating. By incorporating π_1 in the variance equation of the EGARCH methodology, we can capture the volatility spillovers from the cybercrime events impacting each company to the stock market reaction across the related exchanges. We follow the approach of Wang and Nguyen Thi (2012) and define the crisis period for each hacking event period endogenously using the iterative cumulative sum of square (ICSS) algorithm based on a CUSUM test to detect the structural change in variance of the individual return series and use the identified break to determine the dummy variables used to estimate π_1 . This is repeated for each event included in our sample.

Further, we expand upon the work of Dungey and Gajurel (2015) to estimate the sectoral and domestic contagion that occurs during the identified hacking events. We postulate that in a globally integrated network, e.g. modern financial exchanges, the speed of the hacking event and news of its occurrence would be rapidly disseminated across the investment decisions of investors. This view is further supported by the rapid expansion of social media-based news analysis into financial analysis and trading (Greenfield, 2014). Though the hack may be company-specific, the event in itself may draw significant attention to the technological infrastructures of other similar companies. We must also consider data breaches that merit international attention, that is, events

that have obtained international reputational damage such as that experienced by Sony in November 2014.⁶

Due to the placement of some companies in national indices, a sharp fall in price that can be attributable to a hacking event could potentially destabilise the short term expectations of the exchange in which they operate thus leading to significant contagion effects. To investigate, we build further on the EGARCH specification (2). To capture volatility spillover effects (or contagion channel) in the variance equation of the national exchange in which the company trades, our final specification takes the following form:

$$r_{i,t} = a_{0,i} + a_{1,j} f_t^{domestic} + a_{2,j} f_t^{domestic} I_t + \varepsilon_{i,t}; \quad (3)$$

where I_t is an indicator function that takes value 0 during the normal period before and after the hacking event and 1 during the hacking event. The coefficient $a_{2,j}$ captures the changes in the domestic exchanges risk exposure during the crisis period. As in (1), we have specifically included international factors to capture known relationships between the domestic exchanges and international variables. However, during a period of stress, shocks from the hacked company may impact over and above the spillovers denoted in (3), which can be denoted as idiosyncratic contagion (Dungey et al., 2005; Dungey and Martin, 2007). Our final levels contagion specification to investigate contagion channels is as follows:

$$r_{j,t} = b_{0,j} + b_{1,j} f_t^{domestic} + b_{2,j} f_t^{domestic} I_t + b_{3,j} f_t^{company} + b_{4,j} f_t^{company} I_t + b_{5,j} I_t + \varepsilon_{i,t}; \quad (4)$$

$j = 1, \dots, n - 1 \neq source\ company.$

⁶ A simple explanation and timeline of the Sony hack event is provided here: <http://fortune.com/sony-hack-part-1/>

Where the company factor $f_t^{company}$, is extracted as the residual form, applying (3) to $i =$ *the hacked company*, thus orthogonalizing the country and company-specific factors. In (4), the coefficient b_1 represents a standard CAPM beta coefficient against the domestic exchange, b_2 represents systemic contagion, b_3 measures the general spillover effects of the shocks after a hacking event, b_4 measures the additional effects of the hacking event during the period denoted by the CUSUM test, that is idiosyncratic contagion and b_5 captures any intercept shift in the factor model representation or shift contagion during the period after the hacking event.

To capture the volatility spillovers, the variance equation takes the following form:

$$\ln(\sigma_{j,t}^2) = c_{0,j} + c_{1,j}(|Z_{j,t-1}| - E|Z_{j,t-1}|) + c_{2,j}z_{j,t-1} + c_{3,j}\ln(\sigma_{j,t-1}^2) + \pi_{1,j}\ln(\hat{\sigma}_{dom,t}^2) + \pi_{2,j}\ln(\hat{\sigma}_{dom,t}^2)I_t; \quad (5)$$

In (5), the parameter estimate $\pi_{1,j}$ captures the general spillover effects from the hacking event of company j and $\pi_{2,j}$ captures the additional company j volatility spillover for market I during the period after the hacking event. Robustness tests support this modelling choice⁷. This volatility specification could be extended to include global influences in a similar manner to that applied in (1). However, using this specification, there is widespread evidence supporting the view that a single source is sufficient to capture GARCH effects in global markets (Bekaert et al., 2005; Dungey et al., 2015; Dungey and Gajurel, 2015). A statistically significant and positive systematic comovement with the domestic stock exchange throughout the sample period is uncovered when $b_1 \neq 0$, indicating exposure to domestic systemic risk. We considered a broad range of potential joint tests. Similar to Dungey and Gajurel (2015) we focus on the univariate tests for systematic contagion ($b_2 \neq 0$), idiosyncratic contagion ($b_4 \neq 0$) and volatility contagion ($\pi_2 \neq 0$) stemming

⁷ Robustness tests and all omitted tests results are available from the authors upon a request.

from the hacking events. The null hypothesis of no contagion of any form is given by the joint test for $b_2 = b_4 = \pi_2 = 0$.

4. DATA AND DESCRIPTIVE STATISTICS

Eight hundred and nineteen hacking events with sufficient disclosure are identified between January 1, 2005, and April 30, 2015, which are divided into the categories: data breaches caused by an employee release, data breaches resulting from an external data breach or hack, data breaches resulting from a lost, stolen or discarded internal data device and data breaches caused by unintentional disclosure. The descriptive statistics of the cybercrime events examined year by year are shown in Table 1.

Although the number of cybercrime events appears to have peaked in the sample between 2010 and 2012, the average of cumulative abnormal returns (CARs) has continued to grow⁸. In Figure 2, we see the evidence for CARs relating to hacking. This indicates that financial markets are becoming more aware of the negative sentiment contained within these events and are punishing the companies involved accordingly.

Data for all breaches were obtained through analysis of the Nexis Lexis database, identifying numerous key words throughout all reputable international media sources. This analysis was furthered by an investigation of company media coverage in the days following the identified

⁸ In finance, an abnormal return is the difference between the actual return of a security and the expected return. Abnormal returns are sometimes triggered by events such as mergers, dividend announcements, earning announcements and cybercrime, all of which can generate abnormal returns. These events can typically be classified as information or occurrences that have not already been priced by the market. Cumulative abnormal returns (CARs) refer to the sum of all abnormal returns and are usually calculated over small windows, such as days, weeks and months.

cybercrime event to analyse public statements and admissions made from internal sources.

As the main hypothesis of this paper deals with the potential for systemic spillovers of cybercrime across financial markets, only publicly traded companies were used in this analysis. Removing privately held companies from our initial sample, five hundred and eighty individual international publicly traded companies remained. There are companies in the sample who were targeted more than once. All events were further examined to obtain the number of customer records affected and the size of the company at the time of the cybercrime event. For presentation purposes, this paper only provides the EGARCH results of companies greater than USD\$1 billion in market value at the date of the data breach.⁹

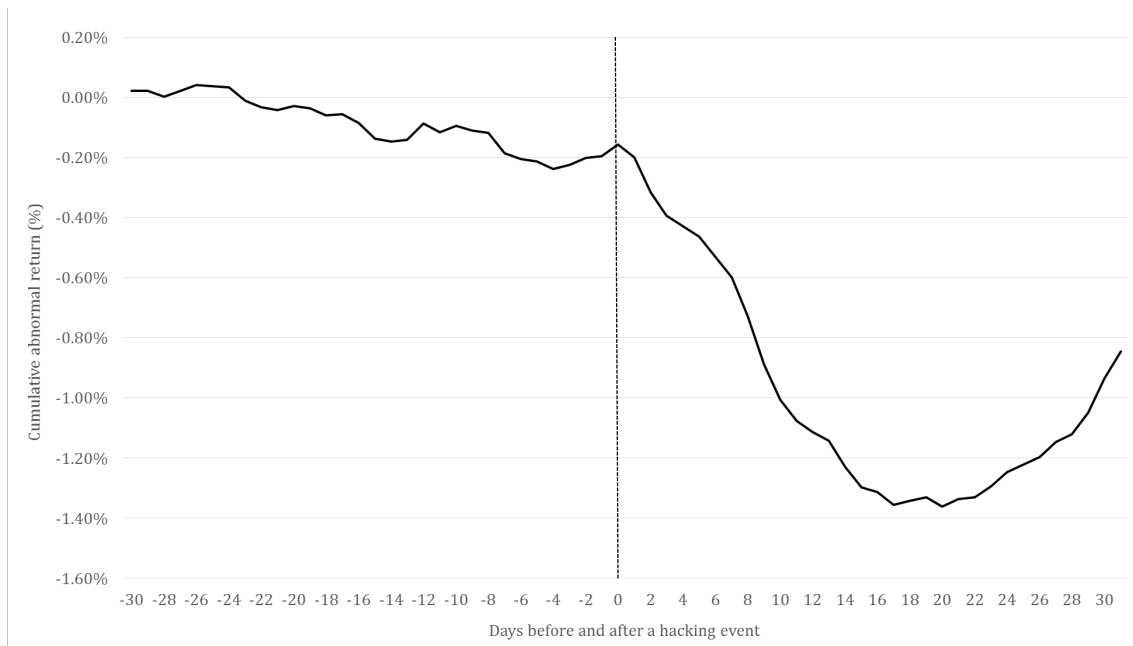


Figure 2: Cumulative Abnormal Returns associated with investigated hacking events.

⁹ Model analysis for other companies is available from the authors upon a request. When it comes to the cybersecurity events impacts on the impacted company equity, the results are qualitatively similar to those for larger market capitalization equities. We focus our attention in this paper on larger companies in order to provide more clarity concerning the empirical evidence of contagion effects that are not present for small cap stocks. This is intuitive as small cap companies have no significant linkages to the exchanges they are traded on or to the global financial markets by the virtue of their small size.

Table 1: Annual summary statistics of the included cybercrime events (2005-2015).

Year	Total number of events	Clients records exposed	Average of CAR
2005	30	677,314,000	-1.59
2006	108	498,330,900	-2.46
2007	85	408,197,900	-1.51
2008	45	326,522,000	-1.76
2009	44	238,973,800	-2.67
2010	134	573,785,700	-3.29
2011	126	1,008,086,300	-2.63
2012	104	264,776,600	-4.36
2013	62	430,011,700	-4.78
2014	56	644,055,000	-6.48
<u>2015</u>	<u>25</u>	<u>120,671,600</u>	<u>-6.19</u>
Total	819	5,190,725,500	

Note: The above events are compiled after a thorough search of company announcements relating to cybercrime and a thorough media investigation using the Nexis Lexis database. The number of clients records exposed is reported based on the estimates released in company statements after the cybercrime events. The average CAR is calculated based on the ten day period following the denoted cybercrime.

In Table 2 we display the annual summary statistics relating to announced hacking events on publically traded companies. In total, 1.9 billion individual records were exposed throughout the 2005-2015 period, with 230 severe hacking events announced and admitted by the companies involved. The frequency of these developments would be of primary interest. There would be concern that numerous hacks may indeed be kept as private as possible due to the reputation damage and other associated issues. However, the rapid growth of social media has generated an instantaneous medium for news based on such events. Furthermore, regulatory disclosure requirements do cover cyber security breaches when the breaches target publicly listed companies. Also, there has been a dramatic rise in the number of hacking organisations that quite simply ‘take responsibility’ for their actions. Taken together, trends in growth in the scale and scope of news dissemination platforms and sources, and concurrent growth in the numbers of hacker-declared breaches suggest that the publicly available data does indeed represent a reasonably accurate measure of the cyber events that impact larger and publicly traded companies. In other words, our data sample is robust to the potential omissions of cybersecurity events.

Table 2: Annual summary statistics cybercrime events denoted as hacks (2005-2015).

Year	Total number of events	Clients records exposed	Average of CAR	Min of 10-day CAR
2005	4	36,480,000	-1.34	-6.46
2006	15	27,402,500	-3.25	-7.55
2007	19	18,690,700	-2.68	-17.77
2008	8	128,056,800	-0.87	-7.99
2009	13	54,655,000	-4.97	-9.77
2010	29	242,697,200	-5.12	-45.55
2011	34	409,421,900	-6.20	-38.97
2012	33	217,769,000	-8.40	-26.29
2013	20	190,794,800	-6.39	-35.25
2014	37	559,620,000	-10.56	-22.15
<u>2015</u>	<u>18</u>	<u>57,186,600</u>	<u>-10.15</u>	<u>-33.85</u>
<i>Total</i>	<i>230</i>	<i>1,942,774,500</i>		

Note: The above events are compiled after a thorough search of company announcements relating to cybercrime and a thorough media investigation using the Nexis Lexis database. The number of clients records exposed is reported based on the estimates released in company statements after the cybercrime events. The average CAR is calculated based on the ten day period following the denoted cybercrime.

Hacking has become more prevalent since 2010, with 2014 being the worst year both regarding event numbers and clients exposed as shown in Figure 2. CAR analysis presents evidence that the average stock market reaction in the ten days following the events has become increasingly negative as one would expect. Whereas, between 2005 and 2008, the average CAR may fall by 3%, since 2010 the same abnormal returns have fallen over 5%, with 2014 and 2015 presenting the largest average falls of over 10% associated with hacks. In fact since 2010, after a hacking event, there have been some profound stock price reductions. The minimum of the ten day post-CAR acts as the worst case scenario for the investigated companies. This presents the evidence of dramatic share price falls of more than 45%. Overall, our data provide ample evidence of the corporate risks and losses associated with hacking events.

In recent years, ‘hacktivist’ activity, as exemplified by the rise of WikiLeaks, has increased significantly. Some hackers have taken the onus to hack companies for a variety of reasons in an attempt to expose perceived acts of illegality or perceived illicit corporate gain. In some cases, such activists pursue corporations and organisations that are deemed engaging in generating negative social, environmental or governance impacts. While in a range of such events breaches

are not followed by sales or disclosure of clients' data, in other instances, similar to the 2015 'Ashley Madison' hack, the data is stolen and then made freely available on a platform such as Darknet. There were 107 cases of such cybercrime events between 2005 and 2015, leading to the exposure of almost 600 million individual records. There does not appear to be a specific trend of this style of cybercrime worsening throughout the period, but instead, shows signs of random hacking with particular severe episodes. The worst years include 2008, 2010 and 2012 where average CARs fell more than 3.5%.

Table 3: Annual summary statistics cybercrime events relating to data that has been accidentally disclosed or disclosed from a third party source (2005-2015).

Year	Total number of events	Clients records exposed	Average of CAR	Min of 10-day CAR	Total number of events	Clients records Exposed	Average of CAR	Min of 10-day CAR
		Accidental/Lost				Disclosure from a third party		
2005	1	20,000,000	-0.05	0.05	5	10,314,000	-2.28	-5.05
2006	7	14,876,200	-2.65	-10.13	6	89,535,200	-0.45	-8.69
2007	2	3,400,000	-1.77	-2.36	12	239,216,600	-1.46	-13.46
2008	3	327,900	-1.20	-1.89	5	20,731,300	-3.84	-18.44
2009	4	5,532,900	0.11	-4.65	6	5,168,300	-0.33	-10.91
2010	12	113,296,800	-1.33	-24.17	19	132,800,200	-3.66	-33.81
2011	13	104,346,100	-2.38	-19.48	13	13,815,000	-0.35	-45.00
2012	6	435,000	-1.00	-12.53	17	5,285,900	-5.06	-15.02
2013	7	8,006,700	-4.52	-12.23	17	64,900,000	-1.33	-16.61
2014	1	142,000	-1.60	-10.60	6	3,935,000	-2.20	-15.07
<u>2015</u>	<u>0</u>	<u>0</u>	0.00	0.00	<u>1</u>	<u>110,000</u>	-1.14	-1.14
<i>Total</i>	<i>56</i>	<i>270,363,600</i>			<i>107</i>	<i>585,811,500</i>		

Note: The above events are compiled after a thorough search of company announcements relating to cybercrime and a thorough media investigation using the Nexis Lexis database. The number of clients records exposed is reported based on the estimates released in company statements after the cybercrime events. The average CAR is calculated based on the ten day period following the denoted cybercrime.

In Table 3, we show the annual summary statistics associated with cybercrime events relating to accidental loss of clients' data and client's data exposed from a third party source. Accidental events simply relate to data exposed accidentally in emails or through online platforms due to human error. There have been relatively few of these events when compared to the other types of cybersecurity breaches, but the number of clients records exposed is still significant at 270 million. The average CAR does not appear to be as punishing as that of hacking events, with 2013 acting

as the most negative year at -4.52% loss across all companies claiming responsibility for an accidental disclosure.

Table 4 analyses cybercrime data exposure relating explicitly to physical or insider theft and portable devices being misplaced or stolen. Physical and insider theft is quite prevalent with 181 cases during the investigated period. There was a dramatic peak in activity during the 2010 to 2012 period. There has also been a sharp increase in the average CAR associated with this type of cybercrime with some companies experiencing falls of over 50% during the ten day period after the event.

Table 4: Annual summary statistics cybercrime events relating to data that has been stolen externally or internally, or lost through a portable device denoted as misplaced or stolen (2005-2015).

Year	Total number of events	Clients records exposed	Average of CAR	Min of 10-day CAR	Total number of events	Clients records exposed	Average of CAR	Min of 10-day CAR
		Physical Theft/Insider Theft				Portable device misplaced or stolen		
2005	7	331,500,000	-0.42	-4.65	13	279,020,000	-1.85	-19.38
2006	12	1,146,800	-0.79	-15.04	68	365,370,200	-1.15	-18.96
2007	14	13,723,300	-0.16	-20.79	38	133,167,300	-1.46	-25.48
2008	6	100,413,700	-1.41	-13.39	23	76,992,300	-1.50	-24.50
2009	11	1,130,000	-4.20	-28.41	10	172,487,600	-3.94	-9.37
2010	40	5,264,200	-2.98	-50.95	34	79,727,300	-3.35	-43.85
2011	36	23,936,600	-3.65	-50.30	30	456,566,700	-5.57	-36.14
2012	35	6,100,200	-2.33	-55.56	13	35,186,500	-5.03	-32.76
2013	7	6,938,700	-1.84	-32.23	11	159,371,500	-2.80	-22.23
2014	10	79,961,800	-2.26	-10.26	2	396,200	-2.78	-2.52
<u>2015</u>	<u>3</u>	<u>63,010,000</u>	<u>-2.70</u>	<u>-5.55</u>	<u>3</u>	<u>365,000</u>	<u>-1.96</u>	<u>-2.36</u>
Total	181	633,125,300			245	1,758,650,600		

Note: The above events are compiled after a thorough search of company announcements relating to cybercrime and a thorough media investigation using the Nexis Lexis database. The number of clients records exposed is reported based on the estimates released in company statements after the cybercrime events. The average CAR is calculated based on the ten day period following the denoted cybercrime.

Another type of cybercrime is that of misplaced or stolen portable devices. The main reason why misplaced devices are not included under accidental disclosure in Table 3, is that there are numerous cases of an ongoing investigation into the associated breaches. Whereas some companies have identified the case as misplaced, it appears as if the act of theft has not been unanimously ruled out. In total, 1.7 billion individual records were lost during 245 events between

2005 and 2015. There has however been a sharp decline in the number of annual events relating to publicly traded companies, with 68 been identified in 2006, yet only two declared in 2014.¹⁰

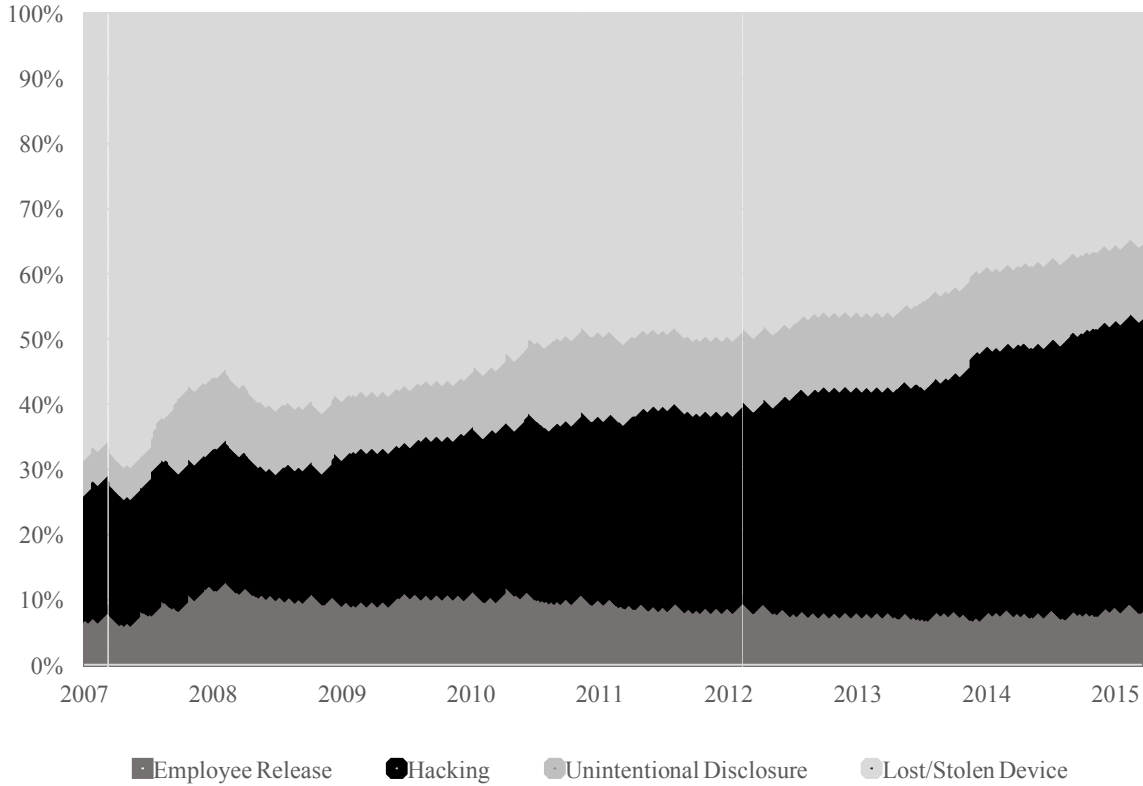


Figure 3: Causes of cybercrime (2007-2015).

Note: The above figure is generated by segregating the proportionate cause of the 819 investigated cybercrime events into their respective categories.

The choice of dummy variables for such events also generated some concern. We have attempted to choose such dummy variables on the date in which the denoted cybercrime occurred, but for 62 of the 245 events relating to portable devices, the dummy variable in fact refers to the date in which the company accepted responsibility for the data breach as the data surfaced in the public domain, although the portable device may have been lost some time before. This is found to be acceptable

¹⁰ It must be noted that the loss of a portable device is assured to be more prevalent than the estimates in Table 4 suggest, but we have only included events where the data lost on such portable devices were found to have resurfaced in illicit markets.

as knowledge of the lost device would not have been available to the market under these circumstances, but it is within the regulatory scope of the company to ensure that the public is made aware of such events. Although the number of annual events appears to have declined, there is, however, evidence that the average CAR peaked during the 2009 to 2014 period with the average CAR for 2011 more than 5.5%.

The CARs analysed throughout are indexed to thirty days before the cybercrime. In the case of hacking in Figure 2, within four trading weeks of the event, the average CAR has fallen nearly 1.4% based on the stock market response to the news. The share price is then found to increase in value in the period after that. This stock market behaviour presents evidence that stock markets efficiently price the specific risk associated with such hacks, representing the perceived reputational, legal and regulatory costs associated with a breach in regulatory platforms. This result agrees with the findings earlier in Table 3, where we identified an increasingly negative sentiment pertained in the CARs associated with hacking events over time, with the trend peaking at over 10% in 2014 and 2015.

Summary statistics for all events present evidence that the stock market is widely aware of the numerous types of cybercrimes that a company can potentially face and that the stock market is incorporating the information into stock valuation. As a proportion of total cybercrime, hacking is the most dominant form, but this is closely followed by the loss or theft of portable devices. Both account for over half of all cases of cybercrime between 2005 and 2015. As we can see in Figure 3, hacking has grown substantially throughout the same period with employee release (whether accidental or intentional) remaining constant. The ease of sale of stolen data appears to be incentivising hackers to further the scale and sophistication of their attacks, particularly with

lucrative profits correlated to the number of individual records that can be obtained (Ablon et al. 2014, Townsend, 2014, Young, Zhang and Prybutok, 2007, and Boes and Leukfeldt, 2016).¹¹

5. RESULTS

The evidence for stock price volatility and contagion for all companies above \$1 billion market capitalisation is reported in Tables 5 through 9, presenting the results of the individual EGARCH regressions based on the differing cybercrime types. Almost every company's stock price has a statistically significant and positive systematic co-movement with the global stock markets throughout the sample, evidenced by $b_1 \neq 0$, indicating exposure to global systematic risk. Exposure to the global systematic risk factor changed significantly for all companies investigated as $b_2 \neq 0$ as reported. In addition to responding to global conditions, the majority of markets also experienced spillovers from the international financial crisis as indicated by a flight to safety to the oil and gold markets. All investigated companies experienced idiosyncratic shocks from these flights to safety, evidenced by $b_3 \neq 0$. $b_3 < 0$, it indicates the potential for portfolio diversification benefits relative to commodity investment (which is incorporated through the inclusion of oil and gold in our EGARCH specification), which is the case for numerous stocks in this sample.

Table 5 shows all data breaches caused by employee release which is denoted as an insider or purposeful release. In a total of 13 occurrences, the null of no contagion in any form – systematic, idiosyncratic or volatility given by the joint test¹² for $b_2 = b_4 = \pi_2 = 0$, is rejected in 9 of the stock returns for the companies who experienced this type of cybercrime. The largest cases in

¹¹ The extent of markets development for transactions in illicit data is exemplified by the fact that today, data obtained from cybercrime activities represent a de facto self-sustained industry supported by back office and supply chain services, as described, for example in Levchenko et al. (2011) for the case of spam activities.

¹² We also consider potential joint tests incorporating b_5 , such as $b_2 = b_4 = b_5 = \pi_2 = 0$; $b_2 = b_4 = b_5 = 0$. The results are similar as b_5 is mostly accompanied by some other contagion estimates (b_2, b_4 or π_2).

terms of total records lost appear to be representative of the companies who transfer returns contagion effects to their domestic stock exchange. No companies are found to transfer volatility or systematic contagion to their domestic exchanges. Of the 4 contagion defined cases in this sample, 2 incidents generated idiosyncratic shocks to their own domestic exchange in the immediate aftermath of the cybercrime incident. The remaining 2 incidents in 2014 and 2015 where the null hypothesis of joint tests (bivariate and multivariate) is rejected indicating a combination of systematic, idiosyncratic and volatility contagion drivers.

Table 5: Data breaches caused by an employee release (2005-2015)

Date	Records Lost	Specification 1					Specification 2			
		b_1	b_2	b_4	b_5	π_2	$b_2 = b_4 = 0$	$b_2 = \pi_2 = 0$	$b_4 = \pi_2 = 0$	$b_2 = b_4 = \pi_2 = 0$
28/04/2005	13.69	-0.022***	-0.014	0.004	-0.091***	-0.016	4.46	0.09	0.25	0.09
28/04/2005	14.40	-0.012***	-0.076***	0.005	-0.026*	-0.064***	0.09	0.41	0.98	0.10
03/07/2007	15.96	0.004	0.003	0.014	0.091***	-0.034*	7.03***	0.91	6.94***	6.97***
04/09/2007	10.43	-0.007***	0.01	0.003	-0.181***	-0.023	0.98	0.65	0.88	1.49
30/11/2007	10.69	-0.038***	-0.040***	0.121***	-0.399***	0.025	1.95	2.01	2.11	2.27
30/12/2007	15.97	-0.001	0.027	0.238***	-1.075***	0.050***	2.27	1.49	0.36	1.86
08/07/2009	7.65	0.016***	-0.009	0.008	-0.185***	-0.014*	0.45	0.30	0.42	0.48
25/05/2010	6.93	-0.014***	-0.044***	0.011	-0.147***	-0.011***	2.56	1.94	3.95*	2.92
12/09/2013	14.51	-0.016***	0.035*	0.155***	-0.267***	-0.040***	18.70***	37.88***	6.25**	45.65***
06/02/2014	10.31	-0.012***	-0.081***	-0.030***	0.063**	0.010***	0.03	1.14	3.16	1.47
06/10/2014	17.38	0.009***	-0.041	0.007	-0.176***	0.029***	25.22***	6.28***	48.75***	44.90***
05/01/2015	12.77	-0.019***	0.003	0.084***	0.342***	0.040***	1.55	1.71	3.12*	3.19
08/04/2015	14.54	0.007***	-0.015	0.006	-0.195***	0.014***	7.56**	0.82	8.62***	9.31***

Note: Specification 1 refers to the EGARCH(1,1) spillover methodology whereas Specification 2 relates to the multivariate testing procedures denoting the contagion type to each domestic stock exchange stemming from the cybercrime events. Record lost represents the log of the recorded estimated size of the data breach as measured by the number of customers affected. ***, ** and * indicate statistical significance at the 1%, 5% and 10% levels respectively.

Tables 6 and 7 refer to external data breaches and hacking events. These results are of paramount interest to the hypotheses central to this paper, namely the contagion effects stemming from the increased frequency and sophistication of hacking. Of the different types of cybercrime included, hacks are by far the most frequent while these attacks appear to be targeted at high-value companies (in this case over \$1 billion in market capitalisation). This may indicate that some of these companies may have superior physical security systems in place to mitigate physical theft

and insider release, but the increased sophistication of hacking appears to be capable of targeting both large and small companies just as effectively.

Table 6: Data breaches caused by an external data breach or hack (2005-2011)

Date	Records Lost	Specification 1					Specification 2			
		b_1	b_2	b_3	b_4	π_2	$b_3 = b_4 = 0$	$b_3 = \pi_2 = 0$	$b_4 = \pi_2 = 0$	$b_3 = b_4 = \pi_2 = 0$
15/04/2005	13.15	-0.013***	0.071***	0.193***	-0.303***	-0.014**	3.91***	3.98***	3.29***	6.78***
20/12/2005	8.24	0.135***	0.029	-0.142***	0.009	-0.163***	2.61	2.82*	1.77	4.63
31/01/2006	9.85	-0.001	-0.001	0.076***	0.165***	-0.01	10.88***	35.93***	0.35	36.06***
06/02/2006	6.91	-0.038***	-0.040***	0.121***	-0.399***	-0.021***	3.87***	16.22***	5.01**	16.47***
09/02/2006	12.21	-0.066***	0.082***	0.129***	-0.017***	0.073***	5.94***	26.38***	12.35***	37.79***
29/08/2006	9.85	0.009***	-0.018	0.007	-0.195***	0.006	8.96**	3.05*	9.03***	12.17***
12/01/2007	11.28	0.086***	0.066***	-0.186***	0.000***	-0.001	0.91	2.65	0.28	2.89
17/01/2007	18.42	-0.003	-0.002	-0.087***	0.003**	-0.046***	19.36***	0.47	15.38***	15.78***
07/07/2007	10.40	0.040*	0.091*	-0.029***	-0.006***	-0.006*	6.02***	5.58**	6.11***	6.17***
17/07/2007	9.90	0.079***	-0.025*	-0.185***	-0.011*	0.011**	13.07***	5.28**	8.00***	13.42***
14/09/2007	15.66	-0.001	0.070***	0.127***	-0.346***	0.039***	15.15***	0.34	14.59***	14.79***
25/01/2008	7.15	-0.010***	-0.008	0.064***	0.166***	0.027	5.69***	1.69	4.56***	6.13***
12/08/2008	8.52	-0.014***	-0.044***	0.011	-0.147***	0.043***	4.43**	0.99	2.69***	3.71***
26/11/2008	10.99	-0.001	-0.001	0.076***	0.165***	-0.01	4.13***	1.83	4.26**	4.39***
20/01/2009	18.68	0.019***	0.057**	-0.121***	0.031***	0.178***	6.48***	4.10**	7.33***	7.81***
16/02/2009	9.95	0.061***	0.018*	-0.137***	0.046	0.017	0.69	0.47	0.78	0.77
05/09/2009	10.86	0.003	0.044***	0.179***	-0.991***	0.035*	4.24	0.06	2.85	2.91
01/01/2010	18.42	0.060***	0.016	-0.158***	-0.006*	0.041***	24.11***	45.95***	18.37***	20.83***
28/02/2010	13.12	0.036***	0.038*	-0.136***	0.011	0.031*	22.41***	2.45	23.95***	24.98***
04/06/2010	12.21	0.007	0.012*	0.051**	0.007	-0.032***	19.56***	8.28***	15.42***	9.63***
09/06/2010	11.73	-0.022***	0.004	-0.090***	0.004	-0.443***	22.95***	14.57**	9.76***	23.14***
09/06/2010	11.21	0.009***	-0.018	0.007	-0.195***	-0.014	50.26***	44.62***	41.14***	88.25***
14/09/2010	14.77	-0.004*	-0.023*	0.068***	0.233***	-0.015	0.92	0.01	3.74	3.75
27/12/2010	15.45	-0.018***	0.113***	0.137***	-0.294***	0.014	17.12***	34.98***	5.96**	39.76***
09/03/2011	8.19	0.013***	0.061***	0.611***	-0.920***	-0.023**	0.32	1.25	0.87	2.05
02/04/2011	19.34	0.015***	0.015***	-0.002	0.084	-0.07	2.56	0.84	0.98	1.82
27/04/2011	18.44	-0.008**	0.102***	0.109***	0.051*	0.006	63.54***	183.07***	0.47	183.35***
06/06/2011	13.82	-0.018**	0.132***	0.105***	0.073	-0.061**	5.30*	0.18	1.11	0.02
09/06/2011	12.79	-0.010***	-0.008	0.064***	0.166***	0.045***	5.46***	1.28	5.86***	6.03***

Note: Specification 1 refers to the EGARCH(1,1) spillover methodology whereas Specification 2 relates to the multivariate testing procedures denoting the contagion type to each domestic stock exchange stemming from the cybercrime events. Record lost represents the log of the recorded estimated size of the data breach as measured by the number of customers affected. ***, ** and * indicate statistical significance at the 1%, 5% and 10% levels respectively.

Of the 29 reported hacks that occurred between 2005 and 2011, eight events had no contagion effects on the domestic exchange in which the stock trades. Two events instigated systematic contagion effects, whereas seven generated idiosyncratic contagion. The remaining 12 events generated contagion through a combination of all drivers. In Table 7, we find the contagion effects of hacks taking place between 2012 and 2015 inclusive of 34 separate events. This is a notable finding that in large companies, there were significantly more occurrences in the most recent three years than the seven years preceding. Nine hacks resulted in no contagion, and only one event led

to systematic contagion. Five hacks led to idiosyncratic contagion whereas the remaining 19 events were as a consequence of a combination of the contagion channels.

Table 7: Data breaches caused by an external data breach or hack (2012-2015)

Date	Records Lost	Specification 1					Specification 2			
		b_1	b_2	b_4	b_5	π_2	$b_2 = b_4 = 0$	$b_2 = \pi_2 = 0$	$b_4 = \pi_2 = 0$	$b_2 = b_4 = \pi_2 = 0$
30/03/2012	15.76	-0.005	0.024	-0.015	0.001	-0.048***	9.73***	8.61***	10.47***	18.92***
25/05/2012	11.72	0.061***	0.067***	0.209***	0.000***	-0.049**	29.57***	78.71***	23.73***	66.82***
06/06/2012	15.68	0.085***	0.026***	-0.154***	-0.001***	-0.052*	9.92***	0.80	10.40***	11.04***
11/07/2012	15.98	-0.010**	0.081***	0.171***	-0.446***	-0.022*	15.84***	19.96***	17.38***	40.55***
12/07/2012	13.02	-0.068***	-0.013	0.037**	0.006***	0.018	5.17**	1.44	4.91***	5.85**
13/07/2012	12.97	-0.026***	0.023	0.047*	0.196***	-0.027***	0.34	0.04	0.22	0.23
04/09/2012	13.82	-0.022***	0.001	-0.098***	0.001	0.452	17.66***	0.01	16.91***	16.97***
13/05/2013	11.98	-0.029***	-0.062***	0.142***	0.005*	0.005*	0.31	0.05	0.20	0.24
17/05/2013	16.91	-0.079***	-0.018	0.036	0.002***	-0.037**	5.12**	5.21***	4.49**	9.61***
05/07/2013	12.39	-0.018*	-0.002	0.206***	-1.161***	0.059***	7.63***	0.50	7.43***	7.90***
08/08/2013	8.95	0.072***	0.016	-0.185***	-0.001*	-0.200***	4.65*	7.90***	3.37**	10.78***
04/10/2013	14.88	-0.025***	-0.068***	0.113***	0.015	0.029	8.59***	9.73***	2.96*	12.15***
07/11/2013	18.84	-0.023***	-0.066***	0.124***	0.017	0.021**	3.46	2.03	2.42	4.34
04/12/2013	14.12	-0.007***	-0.038***	0.015	-0.162***	-0.014	15.64***	14.20***	14.05***	14.67***
04/12/2013	14.51	-0.001	-0.080***	0.006	0.091*	0.092***	16.79***	4.23**	10.83***	15.41***
04/12/2013	14.98	0.007	-0.115***	-0.001	0.093	0.064***	13.54***	7.41***	13.00***	13.53***
04/12/2013	13.65	0.085***	0.026***	-0.154***	-0.001***	-0.037*	6.79***	6.43**	6.83***	9.15***
04/12/2013	13.79	-0.020***	-0.056***	0.092***	-0.080*	-0.025**	15.38***	19.63***	14.79***	25.59***
04/12/2013	14.74	-0.064***	-0.015	0.047**	0.050**	-0.002**	4.18	1.14	4.01	4.15
05/12/2013	13.05	-0.007**	-0.029*	0.068***	0.233***	-0.014	14.76***	8.60***	5.33**	14.14***
13/12/2013	17.53	-0.002*	-0.077***	-0.023*	-0.061**	0.006*	10.72***	11.99***	3.21	8.80**
07/04/2014	11.29	0.069***	0.029***	-0.180***	-0.001***	-0.033*	6.74***	0.52	6.45***	6.93***
28/04/2014	16.99	-0.073***	-0.01	0.004*	0.094	-0.021***	14.79***	0.91	13.02***	16.30***
21/05/2014	18.79	-0.032***	-0.028	0.065***	-0.126***	-0.019***	10.09***	9.11***	10.64***	19.99***
18/08/2014	15.32	-0.021***	0.035	0.081***	-0.595***	-0.009	0.34	0.42	0.22	0.63
20/08/2014	15.26	0.009***	0.016***	0.005***	0.047***	-0.127**	22.03***	29.21***	18.97***	48.79***
28/08/2014	18.15	-0.004*	-0.023*	0.068***	0.283***	0.033**	8.29***	9.82***	8.69***	10.95***
02/09/2014	17.84	-0.012***	-0.081***	-0.030**	0.000*	-0.018	1.63	0.20	1.54	1.80
20/10/2014	14.31	-0.012*	-0.095***	0.001	0.115***	0.034***	4.55	0.35	1.82	2.22
10/11/2014	13.59	0.009***	0.016***	0.005***	0.047***	0.041*	26.57***	13.63***	31.16***	45.08***
24/11/2014	10.76	-0.008**	0.102***	0.146***	0.056*	0.025*	15.04**	18.95***	15.25***	19.52***
05/02/2015	18.29	0.074***	0.017***	-0.214***	0.000***	-0.028	16.20***	17.14***	16.49***	15.69***
29/03/2015	13.12	-0.003**	-0.021	0.043**	0.079***	-0.012***	3.21	0.93	0.30	1.23
03/04/2015	9.41	0.010***	0.075	0.002	-0.141*	0.043***	2.64	0.41	0.90	1.33

Note: Specification 1 refers to the EGARCH(1,1) spillover methodology whereas Specification 2 relates to the multivariate testing procedures denoting the contagion type to each domestic stock exchange stemming from the cybercrime events. Record lost represents the log of the recorded estimated size of the data breach as measured by the number of customers affected. ***, ** and * indicate statistical significance at the 1%, 5% and 10% levels respectively.

Table 8 presents the results for contagion effects stemming from data breaches caused by a lost, stolen or discarded data device. There are forty-eight recorded cases between 2005 and 2015. It is fascinating to note that only one instance could be identified between late-2011 and 2015 indicating that companies have either stopped reporting or admitting to such events or indeed, there has been increased scope of punishment on staff who were to lose data in this manner, which may have worked as a mitigating strategy. Thirty-four of the cases identified are found to result in no contagion channels to the domestic stock exchange. Only one instance in 2005 led to systematic

contagion, whereas five cases led to idiosyncratic contagion. Twenty-eight cases reported no contagion channels which indicates that the stock market does not appear to allocate significant weight to this form of cybercrime, even though we can see that a considerable number of individual private records are lost in this manner.

Table 8: Data breaches caused by a lost, stolen or discarded internal data device (2005-2007)

Date	Records Lost	Specification 1					Specification 2			
		b_1	b_2	b_4	b_5	π_2	$b_2 = b_4 = 0$	$b_2 = \pi_2 = 0$	$b_4 = \pi_2 = 0$	$b_2 = b_4 = \pi_2 = 0$
16/12/2005	14.51	0.074***	0.017***	-0.214***	0.008***	-0.006**	10.58***	3.01*	10.49***	16.85***
25/02/2005	14.00	-0.027***	-0.013	0.009	-0.091***	-0.016*	8.58***	1.10	8.22***	9.80***
19/04/2005	11.97	-0.017***	-0.198***	0.129***	0.164***	0.054***	3.04	3.10	3.58	4.11
20/04/2005	12.21	-0.001	0.070***	0.127***	-0.346***	0.016**	0.55	0.02	0.61	0.67
02/05/2005	13.30	-0.020***	-0.056***	0.092***	-0.080**	-0.025**	0.80	0.34	0.79	0.82
06/06/2005	15.18	-0.010***	-0.008	0.064***	0.166***	0.009	7.15***	6.04***	7.53***	13.29***
06/06/2005	14.39	0.009***	0.016*	0.005	0.042	0.005	1.74	2.21	1.82	3.99
29/06/2005	9.84	-0.022***	-0.014	0.004	-0.099***	-0.028***	13.73***	13.98***	9.13***	24.52***
19/11/2005	11.99	-0.008	-0.016	0.043***	0.0789***	-0.037***	0.90	0.37	0.92	1.33
16/12/2005	14.51	0.108**	-0.259***	0.060***	0.059***	-0.149***	0.22	0.34	0.02	0.37
22/12/2005	11.16	0.017	-0.059***	-0.026***	0.018**	-0.004	1.05	0.46	1.01	1.45
25/12/2005	12.33	0.001	0.032**	-0.034***	0.008*	-0.054***	5.04***	4.58***	0.31	4.97***
28/12/2005	12.24	-0.022***	-0.017***	0.065***	0.042***	-0.009	1.61	2.02	1.62	1.84
21/04/2006	8.19	-0.003	-0.021	0.042***	0.079***	-0.021***	0.31	0.73	0.32	0.37
11/05/2006	9.26	-0.070**	0.013***	-0.029**	-0.006	-0.028**	1.21	1.21	1.17	1.36
14/06/2006	13.74	-0.085***	0.012	0.019***	0.138*	-0.009	0.18	1.56	0.09	1.60
18/06/2006	9.47	0.081***	-0.005	0.036***	0.087*	-0.012**	17.71***	23.54***	17.61***	17.22***
18/07/2006	13.49	0.013	-0.038**	-0.017***	0.043	0.001*	0.02	0.17	0.01	0.17
18/07/2006	10.74	0.032***	0.019*	0.009	0.047**	0.465***	4.94*	4.07***	4.79***	5.88**
25/07/2006	9.53	-0.009***	-0.034*	0.058***	0.013*	-0.019***	2.68	3.15	0.41	3.46
25/09/2006	10.82	-0.008***	-0.046***	0.068***	0.004*	0.069***	4.62*	4.31	4.47	4.86*
14/10/2006	10.67	0.005	-0.100***	-0.008***	0.018*	-0.025	1.09	0.18	1.07	1.08
02/11/2006	11.00	-0.022***	-0.035*	-0.017	-0.053*	-0.048***	1.89	1.12	0.01	1.14
06/11/2006	7.32	-0.011***	0.035**	0.073***	0.180***	-0.014**	0.80	2.05	0.90	2.90
13/12/2006	12.86	-0.003	-0.029	0.046***	0.087***	0.022***	1.81	0.17	0.47	0.60
30/04/2007	8.62	-0.014***	-0.086***	-0.035**	0.019***	0.026***	1.06	0.18	1.05	1.24
01/05/2007	10.76	-0.004***	-0.023	0.068***	0.233	-0.032***	11.38***	1.79	4.68**	6.43**
15/05/2007	7.71	0.027***	-0.028**	0.068***	0.057	-0.029	1.08	2.25	0.56	2.75
28/09/2007	13.59	-0.017***	-0.018	-0.074***	0.029	-0.007*	4.79***	1.12	3.43***	4.73***
16/10/2007	9.21	-0.012***	-0.081***	-0.030**	0.015***	0.010**	4.74***	4.57***	3.43**	8.12***
26/03/2008	16.34	-0.012***	-0.035**	0.053***	0.160***	-0.038**	1.48	0.04	1.30	1.34
04/04/2008	11.00	-0.038***	-0.064***	0.018	0.057	-0.003	2.66	0.03	2.65	2.67
12/05/2008	9.47	-0.007**	0.01	0.003	-0.181***	0.012	1.76	1.02	1.69	1.70
22/05/2008	11.64	0.009***	-0.018	0.007	-0.195***	0.015	13.41***	1.12	11.50***	13.44***
29/05/2008	10.73	-0.024***	-0.033**	0.024	0.134***	0.087***	0.66	0.01	0.65	0.65
19/06/2008	10.95	-0.046***	-0.026*	0.041	0.096*	0.034***	7.38***	6.88***	9.70***	17.80***
17/07/2008	10.65	-0.020***	-0.009	0.067***	-0.406***	-0.006**	1.22	2.61	1.07	1.35
10/09/2008	16.34	-0.012***	-0.035**	0.053***	0.160***	0.084***	0.74	3.48	0.24	3.72
24/11/2008	11.48	-0.029***	-0.038**	-0.017	-0.053*	-0.041**	2.78	0.50	2.08	2.50
06/08/2010	9.70	-0.037***	0.024	0.044**	-0.583	-0.030*	0.09	0.07	0.05	0.12
18/08/2010	7.88	-0.022***	-0.009	-0.016	-0.290***	-0.019***	0.33	0.01	0.11	0.10
15/03/2011	13.46	-0.028***	-0.001	0.018	-0.420***	-0.037***	2.12	0.69	1.84	2.59
15/03/2011	14.12	0.021***	-0.035**	0.038***	0.059	-0.122***	2.31	3.61	2.29	2.70
29/03/2011	9.47	-0.016***	0.175***	0.149***	-0.408***	-0.026*	13.10***	0.30	12.90***	13.11***
07/07/2011	10.43	-0.019***	0.003	0.084***	0.342***	0.040**	8.29***	6.58***	3.41**	8.93***
19/09/2011	11.32	0.072***	0.054***	-0.198***	-0.001***	0.025*	0.93	0.87	0.58	1.46
12/10/2011	8.94	-0.036***	0.027	0.046*	-0.546	-0.006	0.30	0.17	0.04	0.20
23/05/2014	7.99	-0.022***	-0.009	-0.016*	-0.290***	-0.039**	0.27	0.22	0.12	0.33

Note: Specification 1 refers to the EGARCH(1,1) spillover methodology whereas Specification 2 relates to the multivariate testing procedures denoting the contagion type to each domestic stock exchange stemming from the cybercrime events. Record lost represents the log of the recorded estimated size of the data breach as measured by the number of customers affected. ***, ** and * indicate statistical significance at the 1%, 5% and 10% levels respectively.

The final variety of cybercrime is denoted as accidental disclosure. Sixteen events were identified, with causes denoted as accidental email releases, emails sent to the wrong target and security

accidentally opened on secure websites or servers among others. Of the denoted events, twelve resulted in no contagion effects, two events generated idiosyncratic contagion to the wider domestic exchange, and two events led to contagion channels directed by a combination of the denoted drivers.

Table 9: Data breaches caused by unintentional disclosure

Date	Specification 1						Specification 2			
	b_1	b_2	b_4	b_5	π_2	$b_2 = b_4 = 0$	$b_2 = \pi_2 = 0$	$b_4 = \pi_2 = 0$	$b_2 = b_4 = \pi_2 = 0$	
21/09/2007	8.56	0.074***	0.017***	-0.214***	0.008***	0.013	0.51	0.07	0.45	0.52
04/02/2006	7.00	0.009***	-0.034**	0.058***	-0.003**	-0.001***	0.95	1.07	0.35	1.45
06/08/2006	16.81	0.063***	-0.011***	-0.045	0.013*	0.041***	2.04	0.70	2.31	3.01
23/07/2007	14.22	0.008***	0.046***	0.149***	0.076***	-0.017	3.34***	1.32	3.54***	3.72***
21/09/2007	8.56	0.010***	-0.003	0.065***	0.162***	0.029	0.57	0.12	0.56	0.67
10/10/2007	7.50	0.007**	0.018	0.003	-0.181***	0.003	2.08	0.29	2.31	2.57
24/02/2010	13.30	0.019***	-0.008	0.064***	0.135***	0.033***	4.94***	0.01	4.66***	4.98***
25/05/2010	7.16	0.068***	0.125***	0.016***	0.037**	0.006**	1.71	3.44*	1.03	1.67
21/07/2010	10.20	0.061***	0.121**	0.022***	0.033***	0.007	1.37	1.01	2.81	1.29
27/07/2010	11.68	0.021***	-0.004	0.072**	0.166***	-0.022*	0.36	1.79	0.31	0.59
30/08/2010	10.00	0.046***	-0.026*	0.041**	0.096***	-0.031***	0.73	0.25	0.77	0.76
03/09/2012	16.33	0.022***	0.001	-0.090***	0.001**	-0.443*	25.20***	12.73***	10.65***	22.45***
21/06/2013	15.61	0.052*	-0.080***	-0.023***	0.025	0.021***	9.38***	12.16***	0.07	12.16***
17/07/2013	11.89	0.015***	-0.015	0.063***	0.168***	-0.015***	3.61	0.06	3.19	3.57
30/07/2013	10.60	0.072***	0.016	-0.185***	-0.001*	0.207***	1.17	0.87	1.05	1.16
22/05/2014	10.46	0.002*	-0.099***	0.002	0.111***	-0.025***	0.10	0.03	0.01	0.04

Note: Specification 1 refers to the EGARCH(1,1) spillover methodology whereas Specification 2 relates to the multivariate testing procedures denoting the contagion type to each domestic stock exchange stemming from the cybercrime events. Record lost represents the log of the recorded estimated size of the data breach as measured by the number of customers affected. ***, ** and * indicate statistical significance at the 1%, 5% and 10% levels respectively.

We can identify from the above analysis that hacking is the most prevalent source of contagion onto the domestic stock exchange in which the company's stock trades. This should be widely observed by international regulators, as the increased sophistication and frequency of such events will generate further, more frequent and severe stock market shocks, which have the potential to impact the wider market.

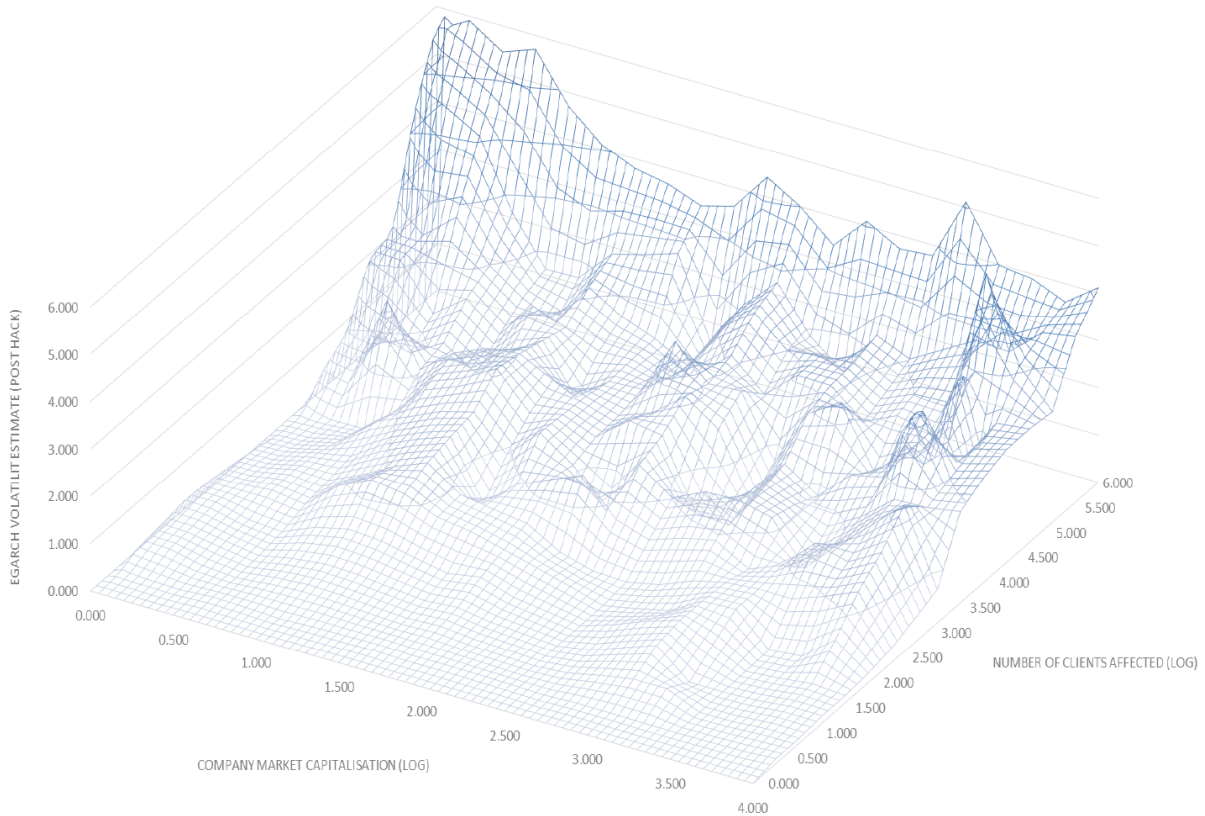


Figure 4: Volatility spillovers due to data breaches compared to the company market capitalisation and number of clients records affected.

Note: Records lost represents the log of the recorded estimated size of the data breach as measured by the number of customers affected.

It is important to analyse some of the key characteristics attached to this contagion transmission as measured by π_2 in the EGARCH models. In Figure 4, 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. It is very clear that there is a significant correlation between the volatility impact and the cybercrime and the number of clients' records exposed, that is, the larger the scale of the event, the larger the contagion transmission. It is also notable that smaller companies (in terms of market capitalisation on the date of cybercrime event) appear to be more susceptible to the cybercrime, with higher values of

π_2 indicative of the significant stock market pressures. There is evidence of a threshold of volatility for these smaller companies as evidenced by the sharp incline in EGARCH volatility, whereas there is a gradual incline as companies with larger market capitalisations experiencing significant volatility effects that increase in proportion to the size of the number of records released during the cybercrime. Figure 4 presents evidence that stock markets appear to effectively punish companies in proportion to the size of the cybercrime, that investors view these events as significantly detrimental to company valuation when incorporating the potential legal costs, regulatory and fraud investigations, operational stoppages and reputational damage associated.

Segregating the differing types of contagion stemming from cybercrime over time presents interesting observations based on stock market behaviour. In Figure 5, we can see that the vast majority of the stock market contagion stemming from the information release of a cybercrime event was based on idiosyncratic contagion. Multiple drivers account for a combination of idiosyncratic and systematic contagion which has remained constant throughout the investigated period between 2005 and 2015. Whereas, the number of events with no contagion effects has increased as a proportion of the total sample. This would indicate that the cybercrime event has been identified as unique to the company rather than the wider stock market. The share of idiosyncratic contagion has continued to fall throughout the period, which can be identified as a side-effect of the growth of non-contagion and multiple drivers in the sample. The most interesting observation is based on the rise of systematic contagion since early 2014.

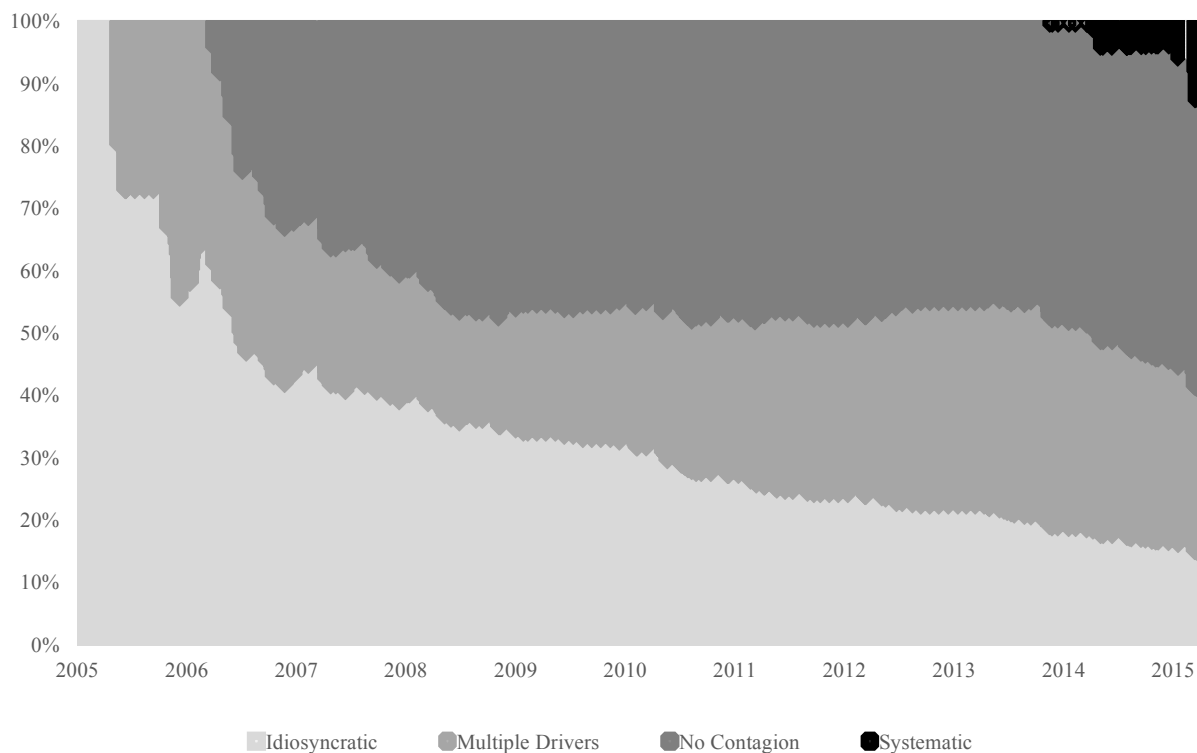


Figure 5: EGARCH calculated contagion type stemming from cybercrime event (2005-2015).

In late 2014 over 12% of cybercrime events resulted in systematic contagion to the wider national stock exchange in which the company is traded. This key finding can be explained through the increased sophistication of such cyber-attacks which has been shown to have caused increased abnormal cumulative losses to the targeted company and a significant increase in the number of client's records that have been illegally exposed. One explanation for such a shift in contagion dynamics is the rise of the Darknet/web, which acts as an international market platform in which this data can be readily sold. The marked increase in hacking events and their associated negative CARs in 2014 and 2015 (over 10%) appear to be directly responsible for the rise in systematic contagion. There also seems to be widespread recognition by investors that the successful targeting of one company, may, in fact, represent a wider threat to the technological structures of domestic publicly traded companies, therefore resulting in such systematic contagion. The results provided

in this research continue to present evidence of continuing advancements in contagion arising from a variety of cybercrime, but none more so than hacking. We must ask what actions can be taken to mitigate the effects of such events, particularly in an environment that is continuing to develop and damage at such increased speed.

6. CONCLUDING REMARKS

This paper implements an EGARCH based modelling framework that encapsulates several channels of contagion and relates them to 819 observed incidents of cybercrime between 2005 and 2015. We determine that hacking is the most prevalent source of cybercrime, with incidents becoming more frequent, more severe in their impact on equity valuations and volatility, and sophisticated since 2012. This has resulted in wider transmission of systematic and idiosyncratic contagion to the domestic stock exchange in which the company's stock trades. The contagion effects of hacking are far more pronounced than cybercrime relating to employee releases, whether accidental or with more questionable motives, and the physical theft of data. Data that has been lost or stolen through portable devices presents strong evidence of contagion effects, but there have been quite a few occurrences since 2012 indicating that companies may be allocating more resources while attempting to stop this type of cybercrime at the source.

Two findings may be of significant interest to regulatory authorities. Stock market volatility is found to be strongly positively correlated with both the size of the company and the number of client's records that have been obtained through the cybercrime incident. It appears that investors are proportionately punishing companies who are responsible for the loss of their client's private data. The second significant finding is based on the changing nature of contagion in recent years.

Between 2005 and 2012, almost 50% of all contagion could be denoted as either idiosyncratic or a combination of idiosyncratic and systematic contagion. Since early 2006, there has been an ever growing proportion of cybercrime generating no contagion effects to the domestic stock exchange, which indicates that investors were becoming more accepting of the added cyber risks that were becoming ever more prevalent. Since 2014, systematic contagion has grown rapidly and as of late 2015, to the extent that over 10% of such contagion to the wider stock exchange originates from cybercrime events.

These results support the added importance of immediate regulatory intervention to mitigate the potentially disastrous effects of cybercrime. The timeliness of such intervention is ever more important given the growth of cybercrime in recent years; the complexity of; its use for commercial and political purposes; and indeed the development of AI. Cybercriminals currently appear to be more advanced in a host of key areas than those whose role it is to monitor and regulate, therefore it is of vital importance that urgent action is taken. Some alternative regulatory strategies that are left beyond the scope of this paper include the role of ‘white knights’ and proactive risk mitigation. The regulatory authorities interested in developing preventative approaches to cyber security should strive to introduce a more structured relationship with ‘white knight’ hackers to disincentivise ‘black knight’ cyber security attackers and to reduce the flows of talent toward illicit hacking activities.

REFERENCES

- Acemoglu, D., Malekian, A., Ozdaglar, A. (2013). Network security and contagion. Working Paper 19174, National Bureau of Economic Research. June 2013. <http://www.nber.org/papers/w19174>
- Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. Paper presented at the Proceedings of the 27th International Conference on Information Systems
- Ablon L, Libicki, MC, Golay, AA (2014) Markets for cybercrime tools and stolen data. Rand National Security Division, Santa Monica, California, June.
- Alkaabi, A., Mohay, G., McCullagh, A., Chantler, N., 2010. Dealing with the problem of cybercrime, Digital Forensics and Cyber Crime, Second International ICST Conference, ICDF2C-2010, Abu Dhabi, United Arab Emirates, pp. 1-18.
- Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eaton, M.J.G., Levi, M., Moore, T., Savage, S., 2013. Measuring the Cost of Cybercrime, *The Economics of Information Security and Privacy*, 1(4), pp. 265-300.
- Baldwin, Adrian, Gheyas, Iffat, Ioannidis, Christos, Pym, David, and Williams, Julian (2016). Contagion in cyber security attacks, *Journal of the Operational Research Society* · July 2016, DOI: 10.1057/jors.2016.37, <https://www.researchgate.net/publication/265275014> Contagion in cyber security attacks
- Be'ery, Tal (2014). How Can Cyber Defenders Regain the Advantage?, *Security Week*, June 2014. Accessed: <http://www.securityweek.com/how-can-cyber-defenders-regain-advantage>
- Boes, S. and Leukfeldt, E.R. "Fighting Cybercrime: A Joint Effort", Chapter 9 in "Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level" Eds: Clark, Robert M., Hakim, Simon, Springer 2016, ISBN 978-3-319-32824-9.
- Brenner, S.W., Clarke, L.L., 2009. Combatting cybercrime through distributed security, *International Journal of Intercultural Information Management*, 1(3), pp. 259-271.
- Brown, C. (2015) "White or Black Hat? An Economic Analysis of Computer Hacking", September 9, 2015, Working Paper, Economics Department, Georgetown University.
- Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, 11(3), 431.
- Cannataci, J.A., Pia Mifsud Bonnici, J., 2003. Can self-regulation satisfy the transnational requisite of successful internet regulation? *International Review of Law, Computers and Technology*, 17(1), pp.51-61.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9(1), 69-104.

CGI and Oxford Economics (2017). “The Cyber Value-Connection”, April 2017. <https://www.cgi-group.co.uk/white-paper/the-cyber-value-connection>

Chalfin, Aaron and Mcrory, Justin (2014) *Criminal Deterrence: A Review of the Literature*, Berkeley Econometric Project, working paper, May 9, 2014.

Chen, L. Y. and Yuji Nakamura, Y., (2016) “Hacked Bitcoin Exchange Says Users May Share \$68 Million Loss”, Bloomberg, August 5, 2016: <https://www.bloomberg.com/news/articles/2016-08-05/hacked-bitcoin-exchange-says-it-will-spread-losses-among-users>

Ciner, C, Gurdgiev, C and B Lucey (2013) “Hedges and Safe Havens: An Examination of Stocks, Bonds, Gold, Oil and Exchange Rates” *International Review of Financial Analysis* 29, pp. 202-211.

CPMI-IOSCO (2016). “Guidance on cyber resilience for financial market infrastructures”, June 2016, Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions Guidance on cyber resilience for financial market infrastructures, ISBN 978-92-9197-288-3.

Dahlgren, S. (2016.a) “The New Era of Supervision: Progress to Date and the Road Ahead” October 29, 2014, Remarks at the New York Bankers Association's Annual Meeting, New York City.

Dahlgren, S. (2016.b) “The Importance of Addressing Cybersecurity Risks in the Financial Sector” March 24, 2015, Remarks at the OpRisk North America Annual Conference, New York City.

Drinkwater, Doug (2016). Does a data breach really affect your firm’s reputation? CSOnline, January 7, 2017: <http://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html>

DTCC (2014). CYBER RISK – A GLOBAL SYSTEMIC THREAT A White Paper to the Industry on Systemic Risk, October 2014. http://dtcc.com/~media/Files/Downloads/issues/risk/Systemic_Risk_Summary_Report.ashx

Egan, Matt (2014) “Companies Turn to Cyber Insurance as Hacker Threats Mount”, March 20, 2014, <http://www.foxbusiness.com/features/2014/03/20/companies-turn-to-cyber-insurance-as-hacker-threat-mounts.html>

Engle, R., 2004. Risk and volatility: econometric models and financial practice, *American Economic Review*, 94(3), pp. 405-420.

Farrell, Scott (2016). Big Hack Attack: Protecting Corporate Reputation and Brand Value in the Wake of a Data Breach, *The Public Relations Strategist*, Summer 2016,

http://apps.prsa.org/Intelligence/TheStrategist/Articles/view/11571/1129/Big_Hack_Attack_Protecting_Corporate_Reputation_an#.WSR22BPYv_8

Finkle, J. and Spicer, J. 2016. "U.S. warns banks on cyber threat after Bangladesh heist" Reuters, Tue Jun 7, 2016. <http://www.reuters.com/article/us-cyber-heist-regulator-idUSKCN0YT25H>

FSOC (2016) Update on Review of Asset Management Products and Activities, Washington: Financial Stability Oversight Council (FSOC), April 18, 2016b. www.treasury.gov/initiatives/fsoc/news/Documents/FSOC%20Update%20on%20Review%20of%20Asset%20Management%20Products%20and%20Activities.pdf

Fultz N., Grossklags J. (2009). Blue versus Red: Towards a Model of Distributed Security Attacks. In: Dingledine R., Golle P. (eds) Financial Cryptography and Data Security. FC 2009. Lecture Notes in Computer Science, Vol 5628. Springer, Berlin, Heidelberg, https://link.springer.com/chapter/10.1007%2F978-3-642-03549-4_10.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. Information Management & Computer Security, 11(2), 74.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. Risk Management & Insurance Review, 13(1), 61-83.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. Information & Management, 46(7), 404-410. doi:10.1016/j.im.2009.06.005.

Gordon, Lawrence A., Loeb, Martin P., and Zhou, L. (2011). "The impact of information security breaches: Has there been a downward shift in costs?" Journal of Computer Security, vol. 19, no. 1, pp. 33-56, 2011. <http://content.iospress.com/articles/journal-of-computer-security/jcs398>

Gottschalk, P., 2010. Categories of financial crime, Journal of Financial Crime, 17(4), pp. 441-458.

Greenfield, David (2014). Social Media in Financial Markets: The Coming of Age..., GNIP White Paper, <http://stocktwits.com/research/social-media-and-markets-the-coming-of-age.pdf>

Gurdgiev, C., 2016. Is the rise of financial digital disruptors knocking traditional banks off the track? International Banker, June 2016. Available at SSRN: <http://ssrn.com/abstract=2795113>

Gulino, Denny (2016). US Office of Fin Research Focuses on Global Risks, Contagion, MarketNews MNI, December 13, 2016, <https://www.marketnews.com/content/us-office-fin-research-focuses-global-risks-contagion>

Haines, J., Johnstone, P., 1997. Global cybercrime: New toys for the money launderers, Journal of Money Laundering Control, 2(4), pp. 317-325.

Heal, G., Kunreuther, H. (2004). Interdependent security: a general model, Working Paper 10706, National Bureau of Economic Research (2004). <http://www.nber.org/papers/w10706>

Heal, G., Kunreuther, H. (2007). Modeling interdependent risks. *Risk Anal.* 27(3), 621–634 (2007). <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2007.00904.x/abstract>.

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management & Insurance Review*, 6(2), 97-121. doi:10.1046/J.1098-1616.2003.026.x.

Holt, T.J., 2003. Examining the forces shaping cybercrime markets online, *Social Science Computer Review*, 31(2), pp. 165-177.

Holt, T.J., Lampke, E., 2010. Exploring stolen data markets online: products and market forces, *Criminal Justice Studies: A Critical Journal of Crime, Law and Society*, 23(1), pp. 33-50.

Ionescu, L., Mirea, V., Blăjan, A., 2011. Fraud, corruption and cybercrime in a global digital network, *Economics, Management and Financial Markets*, 6(2), pp. 373-380. Kelly, Meghan (2013) “From dark days to white knights: 5 bad hackers gone good” *Venture Beat*, November 8, 2013; <http://venturebeat.com/2013/11/08/black-to-white-hat/>.

Jang-Jaccard, Julian, and Nepal, Surya (2014) “A survey of emerging threats in cybersecurity”, *Journal of Computer and System Sciences* Volume 80, Issue 5, August 2014, Pages 973–993, <http://www.sciencedirect.com/science/article/pii/S0022000014000178>

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce*, 12(1), 69-91. doi:10.2753/JEC1086-4415120103.

Kaplan, James, Sharma, Shantnu, and Weinberg, Allen (2011) “Meeting the cybersecurity challenge”, *McKinsey Quarterly*, June 2011, <http://cpalemmens.com/mylibrary/McKinsey%20and%20company%20-%20Meeting%20the%20cybersecurity%20challenge.pdf>

Kholekile L. Gwebu, Jing Wang, and Wenjuan Xie (2014). “Understanding the cost associated with data security breaches”, January 2014, PACIS, <http://www.pacis-net.org/file/2014/1946.pdf>

Khrennikov, I. 2016. “Hackers Found Selling Access to 70,000 Company Computer Systems”, *Bloomberg*, June 15, 2016: <https://www.bloomberg.com/news/articles/2016-06-15/your-company-s-servers-now-on-sale-for-just-6>

Klop, Marloes (2016). “Cybercrime and Corporate Reputation: Business, Government, and Public Perspectives”, *IPSOS MORI*, October 2016, https://www.ipsos.com/sites/default/files/2016-11/Perceptions_of_Cybercrime_18.10.2016.pdf

Ko, M., & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management*, 14, 13-22.

Kraemer-Mbula, E., Tang, P., Rush, H., 2013. The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, 80(3), pp. 541-555.

Kremer, J., 2014. Policing cybercrime or militarizing cybersecurity? Security mind-sets and the regulation of threats from cyberspace, *Information and Communications Technology Law*, Special Issue: Cyber-Privacy or Cyber-Surveillance? Legal responses to fear in Cyberspace, 23(3), pp. 220-237.

Kuypers, Marshall A., Maillart, Thomas, and Paté-Cornell, Elisabeth (2016). "An Empirical Analysis of Cyber Security Incidents at a Large Organization", Stanford University, https://fsi.stanford.edu/sites/default/files/kuypersweis_v7.pdf

Laszka A., Schwartz G. (2016) Becoming Cybercriminals: Incentives in Networks with Interdependent Security. In: Zhu Q., Alpcan T., Panaousis E., Tambe M., Casey W. (eds) *Decision and Game Theory for Security. GameSec 2016*. Lecture Notes in Computer Science, Vol. 9996. Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-319-47413-7_20

Levchenko, K., Pitsillidis A, Chachra, N., Enright, B., Felegyheazi, M., Grier, C., Halvorson, T., Kanich, C., Kreibich, C., Liu, H., McCoy, D. Weaver, N., Paxson, V., Voelker, G.M., and Savage, S. (2011, May). "Click trajectories: End-to-end analysis of the spam value chain". In *Security and Privacy (SP), 2011 IEEE Symposium on* (pp. 431-446). <http://www.ieee-security.org/TC/SP2011/PAPERS/2011/paper027.pdf>

Mawad, Marie and Valentini, Fabio Benedetti (2017). Cybercrime Outbreak Targets French Banking Customers, *Bloomberg*, May 11, 2017. <https://www.bloomberg.com/news/articles/2017-05-11/cybercrime-outbreak-targets-french-banking-customers>

McKendry, Ian and Macheel, Tanaya (2015) "Regulators to Step Up Cybersecurity Activity: Lawsky", *American Banker*, July 28, 2015, <http://www.americanbanker.com/news/bank-technology/regulators-to-step-up-cybersecurity-activity-lawsky-1075715-1.html>.

Moore, Tyler (2010). *Introducing the Economics of Cybersecurity: Principles and Policy Options*. Proceedings of a Workshop on Detering CyberAttacks: Informing Strategies and Developing Options for U.S. Policy <http://www.nap.edu/catalog/12997.html> source: <https://www.nap.edu/read/12997/chapter/1> accessed <http://static.cs.brown.edu/courses/csci1800/sources/lec27/Moore.pdf>

NCI (2016). How does a data breach affect your business' reputation?, National Cybersecurity Institute, Excelsior College, February 16, 2016 <http://www.nationalcybersecurityinstitute.org/general-public-interests/how-does-a-data-breach-affect-your-business-reputation/>

Nelson, D.B., 1991. Conditional heteroscedasticity in asset returns: A new approach, *Econometrica*, 59(2), pp. 347-370.

Norton Rose Fulbright (2016). Cyber risk and directors' liabilities: an international perspective, December 2016, <http://www.nortonrosefulbright.com/knowledge/publications/145122/cyber-risk-and-directors-liabilities-an-international-perspective>

OFR (2016). 2016 Financial Stability Report. Office of Financial Research, the U.S Department of Treasury.

Overvest, B. and Straathof, B. (2015) “What drives cybercrime? Empirical evidence from DDoS attacks” April 24, 2015, CPB Netherlands Bureau for Economic Policy Analysis, CPB Discussion Paper 306.

PWC (2014) “Managing cyber risks with insurance: Key factors to consider when evaluating how cyber insurance can enhance your security program”, June 2014, <https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-managing-cyber-risks-with-insurance.pdf>

PWC (2016) The Global State of Information Security Survey 2016. Online Content, London: PricewaterhouseCoopers, 2016. <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/data-explorer.html>

Reuters (2016) “US hit by 77,000 cyberattacks in 2015 – A 10 per cent jump”, REUTERS, 3/21/16: <http://www.newsweek.com/government-cyber-attacks-increase-2015-439206>

Rollins, J., Wilson, C., 2007. Terrorist capabilities for cyberattack: Overview and policy issues, Focus on Terrorism, Nova Science Publishers, New York, Volume 9, ISBN: 978-1-60021-709-8, pp. 43-63.

Rosengren, E.S. (2016) “Perspectives on Risks – Both Economic and Cyber”, Remarks at the Federal Reserve Bank of Boston’s 2016 Cybersecurity Conference, Boston, Massachusetts. April 4, 2016

Schwartz, G.A., Sastry, S.S.: Cyber-insurance framework for large scale interdependent networks. In: Proceedings of the 3rd International Conference on High Confidence Networked Systems (HiCoNS), pp. 145–154. ACM (2014). <http://robotics.eecs.berkeley.edu/~sastry/pubs/Pdfs%20of%202014/SchwartzCyber2014.pdf>

Smith, A.D., Rupp, W.T., 2002. Issues in cybersecurity; understanding the potential risks associated with hackers/crackers, *Information Management and Computer Security*, 10(4), pp. 178-183.

Stearns, J., 2016. European Union’s First Cybersecurity Law Gets Green Light, July 6, 2016, Bloomberg. <https://www.bloomberg.com/news/articles/2016-07-06/european-union-s-first-cybersecurity-law-gets-green-light>

Stiroh, K. (2016) “The Theory and Practice of Supervision”, Federal Reserve Bank of New York, Remarks at the SIFMA Internal Auditors Society Education Luncheon, Harvard Club, New York City As prepared for delivery, April 11, 2016

Summer, S., 2015. EU criminal law and the regulation of information and communication technology, *Bergen Journal of Criminal Law and Criminal Justice*, 3(1), pp. 48-60.

Tabarrok, Alex (2015) What Was Gary Becker’s Biggest Mistake? *Marginal Revolution*, September 16, 2015. <http://marginalrevolution.com/marginalrevolution/2015/09/what-was-gary-beckers-biggest-mistake.html>, The Economist.

Telang, R., Wattel, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering*, 33(8), 544-557.

Tendulkar, Rohini (2013). Cyber-crime, securities markets and systemic risk, OICU-IOSCO and the World Federation of Exchanges, Staff Working Paper SWP1/2013. 16 July, 2013 http://www.csrc.gov.cn/pub/csrc_En/affairs/AffairsIOSCO/201307/W020130719521960468495.pdf

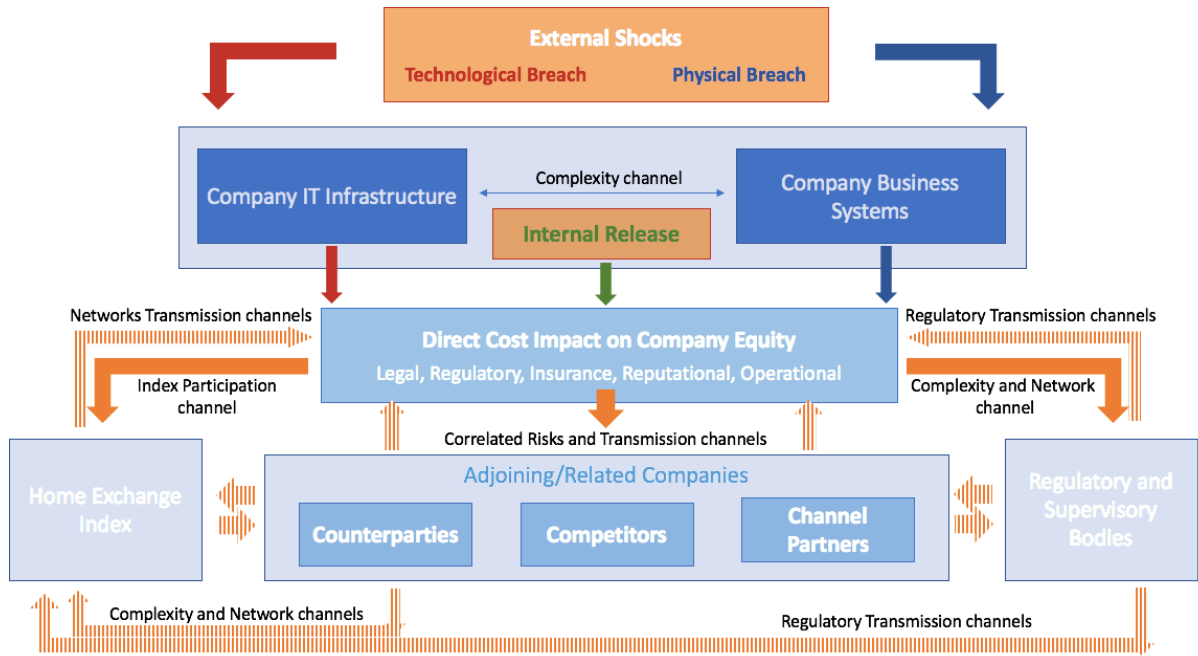
Townsend, K., 2014. Cybercrime and Punishment, *InfoSecurity*, September 2014, <http://www.infosecurity-magazine.com/magazine-features/cybercrime-and-punishment/>

U.S. Department of Justice (2014) National Institute for Justice: Five Things About Deterrence, July 2014, <https://www.ncjrs.gov/pdffiles1/nij/247350.pdf>

Yampolskiy R. V., 2016. “Fighting malevolent AI: artificial intelligence, meet cybersecurity” *The Conversation*, June 13, 2016.

Young, R., Zhang, L., Prybutok, V.R., 2007. Hacking into the mind of hackers, *Information Systems Management*, 24(4), pp. 281-287.

APPENDIX: CYBERSECURITY EVENT IMPACT MAP



Legend

