CHAPTER 13

An Incentives-Based Mechanism for Corporate Cyber Governance Enforcement and Regulation

Shaen Corbet and Constantin Gurdgiev

Introduction

Asymmetric information in international financial markets is defined as the environment in which one party in the transaction has superior, private information relevant to the transaction relative to other parties. One such example of asymmetric information importance to the financial services links technological innovation with the need for protecting consumer

JEL classifications: G15, G32, G38
We wish to extend our gratitude to Erwin L. Alberty and Asmita Jain of Middlebury Institute of International Studies at Monterey, CA, USA for their helpful comments on this paper.

S. Corbet • C. Gurdgiev (✉)
DCU Business School, Dublin City University, Dublin, Ireland

Trinity Business School, Trinity College, Dublin, Ireland
e-mail: shaen.corbet@dcu.ie; gurdgic@tcd.ie

T. Walker et al. (eds.), *Ecological, Societal, and Technological Risks and the Financial Sector*, Palgrave Studies in Sustainable Business In Association with Future Earth, https://doi.org/10.1007/978-3-030-38858-4_13

data. It is a relationship mostly based on trust between consumers and the service provider, backed by reputational signals concerning the provider's trustworthiness. Corporate reputational damage risks and potential breach-related legal judgements and awards, thus, can be seen as key deterrent against cybersecurity strategies and practices that can lead to a breach. Unfortunately, as shown in Corbet and Gurdgiev (2017a, 2019), as well as in the regulatory literature surveyed below, these strategies may not be enough as the rate of cybersecurity attacks, their adverse impact, and complexity continue to grow.

In this chapter, we first summarize the current state of evidence for the unexpected transmission of cybercrime shocks via equity markets valuations during the period of 2005–2015. We show that these transmissions are beyond those which would occur through the known spill-over channels between stock prices of companies subjected to cybercrime in a variety of jurisdictions. In fact, equity trading and portfolio links as well as institutional structures such as international subsidiaries and intermediaries all help propagate risk contagion effects, creating systemic cybersecurity risk spill-over channels. The systemic risk contagion channel transmits cybersecurity risk from one company's share price to other sectoral and market-related companies.

As we show, on the regulatory side of the financial markets, the Committee on Payments and Market Infrastructures (CPMI) of the International Organization of Securities Commissions (IOSCO) warns financial and monetary institutions (FMIs) about the potential for cybersecurity to become systemic through contagion effects. As the result, the IOSCO and other regulatory agencies have been calling for pre-emptive testing of FMI systems as 'an integral component of any cyber resilience framework', stating that 'all elements of a cyber-resilience framework should be rigorously tested to determine their overall effectiveness before being deployed within an FMI, and regularly thereafter' (CPMI-IOSCO 2016, p. 18). Similarly, Dahlgren (2015) warns that cyber threats pose a potentially 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 in this literature is a failure to include other potential channels for systemic risk transmissions, including exchanges and over-the-counter markets. Another omission is the fact that none of the aforementioned sources provide empirical evidence to support the hypothesis of systemic nature of cybersecurity risks. Corbet and Gurdgiev's (2019) study corrected for both omissions.

Beyond the systemic nature of the threat, the magnitude of costs and disruptions imposed onto 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 cyber-attacks cause annual losses of 260 billion euros ($288 billion) to 340 billion euros'. And despite the common perception that cybersecurity vulnerabilities apply primarily to private sector companies, evidence is mounting that central banks and regulators themselves are not immune to cybercrime.

As the best practice for cybersecurity implementation, CPMI-IOSCO (2016, p. 18) suggests the need for penetration testing of FMI systems:

> FMIs should carry out penetration tests to identify vulnerabilities that may affect their systems, networks, people or processes. To provide an in-depth evaluation of the security of FMIs' systems, those tests should simulate actual attacks on the systems. Penetration tests on internet-facing systems should be conducted regularly and whenever systems are updated or deployed. Where applicable, the tests could include other internal and external stakeholders, … as well as third parties.

To carry out such testing, it is proposed that FMIs need to 'challenge their own organisations and ecosystems through the use of so-called red teams to introduce an adversary perspective in a controlled setting'. Furthermore, CPMI-IOSCO also suggests that 'a red team may consist of an FMI's own employees and/or outside experts, who are in either case independent of the function being tested' (CPMI-IOSCO 2016, p. 19). In more common parlance, such 'red teams' are known in the industry as 'white knights' or 'white hats', representing teams of experts in cybersecurity hired by companies on a fee-for-service basis to provide audits and test the company's own cybersecurity systems.

On foot of these regulatory discussions and the empirical findings presented in Corbet and Gurdgiev (2019), this chapter proposes a novel regulatory mechanism for identification, prevention, and mitigation of cybersecurity risks in financial markets. We build on the idea of active deployment of the white knights teams, while aiming to expand the potential technical capabilities of such teams and the scope of incentives for these teams to aggressively pursue their test targets. We further propose putting these teams outside direct reporting to the companies tested to reduce potential conflicts of interest and agency problems that may arise from close proximity between the white knights and their target companies. Our proposal is to deploy the power and the capabilities of the hacktivists to provide regulatory and enforcement supports. The idea of drawing on hacking community resources to combat cybercrime may initially appear counter-intuitive, but it is anchored in the already evolving markets for hacktivist services in detecting and preventing potential weaknesses in corporate cybersecurity infrastructure. It is also linked to the existent and successfully growing systems of using whistle-blowers and independent reporters to detect and punish corporate financial/accounting irregularities and crimes.[1]

The ethical dilemma implied by this proposal is addressed throughout this chapter. In our opinion, hacktivists (or hackers that are at least marginally committed to illicit hacking), if appropriately remunerated and monitored, could provide the necessary skill set and offer benefits to regulatory agencies and companies in the form of identifying structural cybersecurity weaknesses.[2] Such a skill set is currently lacking in the regulatory and enforcement community for a variety of reasons, including the lack of aligned incentives for hacktivists to join regulatory and enforcement institutions. Our proposal counters this problem by creating a functional set of incentives and rewards, aligned with key performance indicators, for hacktivists' participation in legal and supervised tests of the firms' security systems.

Of course, the data breaches, when supervised, must not lead to the resultant or potential future damage to consumers. Our proposal addresses these potential problems by offering a staggered system of reimbursement for hacktivists, linked to the success of the cybersecurity tests conducted by them over time.

[1] Evidence for the potential efficacy of such a mechanism may be presented in the attempted start-up of a hedge fund 'TRO LLC'. This hedge fund idea was developed by Mr. Andrew Auernheimer (a hacker also known as 'WEEV'). The main issue with this hedge fund idea is that at its core is the promotion of hacking or identity theft for financial gain. As a result, Mr. Auernheimer has proposed that the fund will not be directly for hack companies but will 'probe the public surface of a company' and 'actually watch hackers' (CNBC interview, 28 April 2014).

[2] This view is broadly consistent with the existent literature and practices on the use of whistle-blowers (internal and external to the company) in detecting other potential breaches and violations, as discussed in Dahlgren (2015) and referenced by the RICO system, discussed below.

Overall, the identification of the weakness can provide a deterrent based on a threat of reputational damage to the company through regulatory disclosure in cases where structural data security weaknesses have been identified, and if the mitigation of discovered breaches is lagging. Public disclosure in this scenario may in fact be more beneficial as a punishment alongside regulatory fines, as shown by the evidence on the abnormal negative returns resulting from voluntary and involuntary disclosures, presented in Corbet and Gurdgiev (2019) and summarized in Fig. 13.1.

The evidence concerning an increasing frequency and severity of cybersecurity breaches over time leads to another view of problems addressed by the proposed mechanism, where regulatory authorities can maintain their current technological capabilities as the hackers' skill sets and tools develop in real time. Direct engagement with hacktivists can provide invaluable access to the skills and tools that regulatory authorities often lack. Hackers and hacktivists learn by doing. In traditional sequencing of events, hackers first breach a company's or an organization's data systems and cause financial and reputational damage to it, thereby imposing severe costs on consumers and other companies (through the systemic contagion

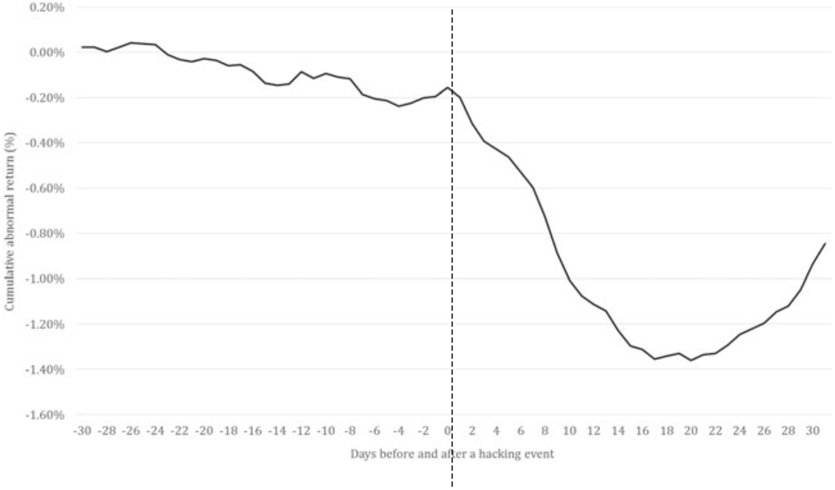

Fig. 13.1 Cumulative abnormal returns associated with investigated hacking events. Source: Authors own data extraction from the LexisNexis database, see Corbet and Gurdgiev (2019)

channels). Subsequent to this, regulatory authorities spend time and resources identifying who has caused the breach, mitigating the breach costs, and pursuing prosecution of those responsible. In this process, authorities and companies also discover and address the causes of the vulnerability exposed by the hackers. Our proposal establishes a transmission channel for skills from the hackers to the regulators who supervise actual live hacks ex ante illegal breaches occurring.

Put in simpler terms, in the current environment, regulators chase hackers after the damage is done, while companies remedy the cost of breaches through insurance and by ex post systems upgrades.[3] In our proposed preventative channel, hacktivists and regulatory authorities can work together under a model of effective monitoring and remuneration, instead of opposing each other. Currently, U.S. Government agencies (outside security institutions, for which data is not available[4]) operate on the basis of hiring former hackers and hacktivists, and employing contractors who use former hackers in formal employment. Larger U.S. corporations do the same. This employment situation presents a set of problems associated with broader 'agency issues'. Firstly, hacktivists available for hire are self-selected to be older, a more mature generation of hackers who are moving to become white knights. Their skill sets can be outdated relative to the younger generations of hackers still operating in the grey or black markets. Secondly, once in employment, white knights can be subject to contractual and career pressures to act in the interest of the employers and managers, as opposed to the interest of the firm owners. Thirdly, white knights are usually hired on the basis of exploiting a known vulnerability, as opposed to proactively testing all systems.

[3] Data on the frequency of cybercrime on publicly traded companies covering the period from 2005 through early 2015 shows that one specific form of cybercrime becoming ever more prevalent is a breach of the company's firewall to steal client data which can be used for a host of illegal activities.

[4] While U.S. Security Agencies are reported to have engaged white knights and current hacktivists, these engagements are structured on selecting known hacktivists and using them as agents working for the agency. This is distinct from the mechanism we propose in a fundamental way. Our proposal involves voluntary self-selection of hacktivists to participate in a reward-for-breach testing 'tournament', as opposed to cooption of a selected hacktivist for cooperation with an agency. As a result, our mechanism is designed to address the core issue of economic agency problems that arise from direct or indirect employment of hacktivists by the contracting entity.

In an environment where the size and technical complexity of data breaches are becoming more advanced and sophisticated, more pressure must be placed on corporate mechanisms to protect consumers' data across all sectors.[5,6]

We propose a fine-sharing model for rewarding hacktivists who successfully breach tested companies' cybersecurity under regulatory and enforcement bodies' supervision. Such a system would price hacktivists' efforts based on imposing a regulatory cost of cyber risk discovery onto companies directly responsible for maintaining cybersecurity in the first place. In economic policy terms, this mechanism qualifies as satisfying 'user-payer' principle of efficiency in enforcement, as such fines would directly target those corporate counterparties and markets participant that are most directly responsible for potential failures of cybersecurity.

In general, the reputational damage from the disclosure of a successful cybercrime event should be reflected through the influence of the efficient market hypothesis into stock prices.[7] Partially, as our discussion below indicates, this reflection is true. Examples of negative reputational costs to companies due to cybersecurity attacks abound and include the world's largest shipping company, AP Moller-Maersk, which suffered a loss of US$300 million in a 2017 cyber-attack, leading to a reputationally costly profit guidance revision and share price loss of 7 percent (Novet 2017).

[5] Notably, in a range of sectors, although not yet widely in finance, the use of 'white hat' or 'white knight' hackers is growing in both frequency and scope. Some industry-level examples are discussed in Kelly (2013). The lack of similar approaches in financial regulation was recently discussed in McKendry and Macheel (2015). Our proposal builds on this momentum and extends the system of cooperative engagement between regulators, companies, and white knight hacktivists to a mechanism that would create functional incentives for hacktivists' participation in the regulatory prevention of the cybersecurity risks. Such a mechanism is currently lacking in the industry.

[6] Those hackers or hacktivists possessing the best technological talent are more likely to be swayed by the financial returns of private practice. In simple terms, there is an argument in favour of a learning-by-doing second order effect of such a system of enforcement based on repeated interactions with leading experts in cybersecurity who represent the front end of the knowledge curve, as opposed to the past 'dark hat' hackers who may or may not be leaders in their field at the moment of their engagement by the firms and regulators as 'red teams' or white knights.

[7] Corbet and Gurdgiev (2019) document the evidence on the negative abnormal returns experienced by the companies following cybersecurity breaches. This evidence is summarized below and in Fig. 13.1. Some examples of reputational damages sustained by companies following the attacks is discussed and summarized in Alva Group (2016), Tiedemann-Nkabinde and Davydoff (2019), and Spam Titan (2019), amongst others.

The Moller-Maersk hack was part of a much wider ranging NotPetya DNS (Domain Name System) attack that impacted thousands of businesses and public agencies around the world. As per Security Magazine (2019): ‘No sector was spared, leaving organizations open to a range of advanced effects from compromised brand reputation to losing business. … The top impacts of DNS attacks—damaged reputation, business continuity and finances’ with reported 26 percent of businesses experiencing ‘lost brand equity due to DNS attacks’. Another example of reputational damages arising from cybersecurity breaches is the case of the Equifax data breach of 2017 which exposed sensitive data of more than 145 million people worldwide. In the wake of the public disclosure of the attack, Equifax shares dropped 13 percent in one day, and the company is currently dealing with numerous lawsuits resulting from the breach. Shell (2017) reported, in the wake of the Equifax breach disclosure, that the company sustained significant brand damages as the result of the hack. According to Shell (2017), the second-worst breach-related impact ‘was a drop of 10 points suffered by eBay in the 10 days after its May 2014 hack. Other high-profile breaches, such as one at Anthem Blue Cross in February 2015 and Home Depot in September 2014, did not cause as big a hit to those brands’. Furthermore, as Shell (2017) notes, ‘Equifax’s initial hit to its reputation is bigger than the 23-point decline in Chipotle Mexican Grill’s Buzz score decline in October 2015 after its E. coli crisis began’. Notably, Ponemon (2018b) shows that in 2017–2018, the direct costs of data breaches were smaller than the indirect costs, which include reputational losses in every country and region covered in their study. Overall, The Council of Economic Advisers (2018, p. 6) shows that reputational damages from cyberattacks rank 6th in magnitude of associated costs after losses of intellectual property, increases in cost of financial capital, losses of strategic information, data and equipment, and court settlement costs. This rank puts reputational damages and costs ahead, in magnitude, of losses of revenues, costs of breach notifications, costs of cybersecurity improvements and consumer protection improvements, and regulatory fines and penalties. The latter rank the lowest in terms of their cost impact to companies experiencing a cybersecurity breach, providing further evidence of the ineffectiveness of current regulatory and enforcement regimes in providing preventative deterrence.

Given the continuous growth in cybersecurity threats and the success rates with which cyber criminals can penetrate corporate security systems, this reputational cost is not sufficient to create functional incentives for the firms to take corrective actions to prevent hacking threat from materializing. Under our proposed mechanism, this reputational cost would be augmented by the threat of more effective fines and would provide financial support for hacktivists' engagement with the authorities. The onus of corporate responsibility would therefore shift back to the target company, forcing the company to proactively improve its internal infrastructure, or face a repeat attack and regulatory disclosure of potential risks to the public and the markets. In time, the constant threat of data breaches could be reduced from the technological advancements of both the company and the regulatory/supervisory authorities, making consumer data more protected and the companies operating within a regulated regime more trustworthy.

The remainder of the chapter is organized as follows. Section "Cybercrime and Financial Markets" discusses the related, previous literature on the influence of cybercrime on financial markets and the systemic nature of the risks presented by such attacks to the international financial markets. Section "White Knights and Proactive Risk Mitigation" proposes a brief outline of the regulatory/supervisory mechanism that uses white knight hackers and hacktivists as regulatory and enforcement agents. Section "Concluding Remarks" concludes.

Cybercrime and Financial Markets

To date, the only study that focuses specifically on the interlinkages between the differing types of cybercrime and financial market volatility or systemic stability risks within the financial markets is provided by Corbet and Gurdgiev (2019) (see McKendry and Macheel 2015).

In this section, we first summarize the existent research on cybercrime impact in the financial markets and the economy in general, followed by a review of the classification of the cybercrime events. We conclude this section by summarizing the findings from Corbet and Gurdgiev (2017a, b, 2019) that establish the systemic nature of the cybersecurity risks in financial industry.

Cybercrime and Financial Risks: The State of [Regulatory] Play

In the early literature, Rollins and Wilson (2007) found that although the U.S. and international community have taken some steps to coordinate laws to prevent cybercrime, computer attacks will continue to become more numerous, faster, and more sophisticated, leading to the situation where the U.S. Government agencies may not, in the future, be able to respond effectively to such attacks. Rollins and Wilson's (2007) view is confirmed by UN (2011) and DHS (2018), amongst others.

Amplifying the predictions of Rollins and Wilson (2007) concerning the evolution of the cyber threats, Ionescu et al. (2011) find that the Global Financial Crisis led to an exponential growth in cybercrime in the period 2007 to 2011. This growth has been only partially matched by improvements in the knowledge and technological abilities of computer specialists who are acting to prevent or restrict cybercrime expansion. Ionescu et al. (2011) argue that the rate of growth in cyber threats is unlikely to fall, a sentiment also echoed by Ponemon's (2018a, b) reports.

An added threat, subject to the even greater potential costs, risks, systemic uncertainty and enforcement problems, is the evolution of the Artificial Intelligence (AI) (Yampolskiy 2016), where 'the potential that a super-intelligence may be capable of inventing dangers we are not capable of predicting'. Quite naturally, in an environment of malicious AI deployment, the robustness of cybersecurity systems will have to be tested live, in real time, and not ex post as today's best practices imply.[8] This view of evolutionary dynamics in cybersecurity threats within the financial sector is mirrored in the findings concerning the general trend toward an ever-increasing degree of automation/computerization and the pursuit of speed of information processing in financial services. For example, MacKenzie (2018) clearly states that today, financial markets are already operating at speeds as fast as within 50 microseconds of the speed of light. This increase in speed of data transmission and processing, associated with the rise in algorithmic trading, puts ever more pressure on existent regulatory and enforcement structures designed to prevent, mitigate, and punish cybercrime as it relates to the financial markets. An additional and related dimension is the evolution of quantum computing, which brings higher degrees of uncertainty and complexity to the analysis of the future evolution of cyber threats (Keplinger 2018).

[8] These tests will have to involve not only the best human hacktivist talent, but also preventative AI. Reactionary responses to cybersecurity breaches in the age of AI will be too little, too late to mitigate extensive damages that can be inflicted by information systems moving closer to the speeds of light, as opposed to human-led attacks by modern day hacktivists.

One startling observation throughout numerous research papers identifies the ease with which stolen data can be purchased and sold through a network of illicit, secretive, and publicly available mechanisms. Holt and Lampke (2010) examine the nature of the market for stolen data based on the analysis of six web forums run by data thieves. All manner of personal and financial data can be obtained at a fraction of their true value, with inefficient regulation and numerous legal issues enhancing the ease at which these hackers can operate. In 2016, cybersecurity firm Kaspersky Labs uncovered an online marketplace for trading illegally obtained data and sales of access to more than 70,000 hacked corporate and government servers for as little as US$6 each, according to Khrennikov (2016). The evolutionary development of illicit markets for trading in stolen data is also highlighted in Beckert and Dewey (2017).

Kraemer-Mbula et al. (2013) examine the effects of globalization on growth in sophistication of financial cybercrime. One of the key findings of the paper is the need to further develop policy makers', law enforcement's, and security firms' capacity to identify trends and concentrate preventative resources, as well as to increase knowledge of how cybercrime operates.

If proactive testing of corporate systems by hackers can be deployed to increase the publicly visible probability of detecting cybersecurity systems flaws, such tests can act not only as an enforcement mechanism, but also as a regulatory deterrence. Kremer (2014) asks how the perceptions of security and threats in cyberspace play an important role in justifying the means and measures employed by different security agencies. Security mind-sets in this sense are differentiated between a national security mind-set, concerned with military and strategic considerations of national security, and a liberal mind-set which perceives security together with individual rights. Summers (2015) states that one of the biggest challenges that remains for the regulation of information and communication technology is that the global information space does not respect national boundaries and that any regulatory approach can call for some degree of cooperation between countries. Eric S. Rosengren from the Federal Reserve Bank of Boston echoes Summers' conclusions in his April 2016 speech (Rosengren 2016, p. 2), stating that 'Cyber criminals are looking for the targets of opportunity without regard to geographic location, and the existence of a global population of potential attackers looking for softer targets means increased risks'.[9]

[9] Another example of the lagging nature of legal and enforcement frameworks relating to cybercrime is presented by the relatively frequent hacking events involving cryptocurrencies exchanges. According to Chen and Yuji Nakamura (2016), lack of legal frameworks operat-

In a forward step in terms of international coordination of cybersecurity enforcement, the European Union approved the first set of joint rules aimed at preventing cyber-attacks, including rules requiring companies to improve defensive systems and to disclose such attacks. As reported by Stearns (2016), the EU legislation '…will impose security and reporting obligations on service operators in industries such as banking, energy, transport and health and on digital operators like search engines and online marketplaces. The law … also requires EU national governments to cooperate among themselves in the field of network security'. Unfortunately, the European Union initiatives in this area continue to rely on the company's and regulators' internal resources and systems to detect threat vulnerabilities and address cyber risks. Once again, as with the U.S. regulators' approach, the European regulatory bodies continue to use response-based systems for managing cybersecurity, instead of adopting a proactive preventative approach. As noted by numerous reports, an added dimension to this approach is posited by the predominance of the 'insure and forget' model of corporate responses to cyber threats (Egan 2014 and PWC 2014).

Meanwhile, the impact of data security breaches on financial bottom line is growing. The Ponemon (2015, 2018a, b) studies find that the total cost of data breaches across corporate sectors rose 23 percent year-on-year in 2014, with cyberattacks now accounting for 47 percent of all data-breach cases in 2015, up from 37 percent in 2013. In 2018, the comparable figure was 56 percent. In 2016, Russian hackers stole the account data of some 76 million clients from a global banking institution. As claimed by the FBI, nearly 519 million financial records have been stolen from U.S. companies by hackers within the period of 12 months prior to October 2014. In one incident, Russian hackers allegedly acquired more than 150,000 press releases from Wall Street publications in August 2015 and used them to gain a trade advantage, worth US$100 million (Riley et al. 2015). As revealed in an indictment unsealed in 2016, a group of Iranian-sponsored hackers launched attacks against 46 Wall Street institutions in 2011, including the New York Stock Exchange and NASDAQ (Larson et al. 2016). The presence of big data-based FinTech services providers and other non-banks offering e-banking-related products complicates the picture, as recently noted by Packin and Aretz (2016). As

ing in the relation to cybersecurity is illustrated by the August 2016 attack on Hong Kong-based bitcoin exchange Bitfinex.

stated by Robert Anderson, executive assistant director of the FBI's Criminal, Cyber, Response, and Services Branch, 'We're in a day when a person can commit about 15,000 bank robberies sitting in their basement' (Anderson et al. 2013).

As argued in Corbet and Gurdgiev (2017b), despite the executives' rhetoric about the urgency of preparing traditional banks and MFIs for cybersecurity challenges, banking institutions continue to treat cybersecurity as a non-strategic matter. Three major cybersecurity exercises carried out in recent years in the U.S., U.K., and Canada, such as SFIMA-organized Quantum Dawn, CBEST, and IIROC (Investment Industry Regulatory Organization of Canada), through which scenarios testing exposed significant areas of concern when it comes to the financial sector's ability to counter systemic risks associated with cybercrime. More ominously, the results also indicate that at the organizational level, major banks and MFIs continue to treat cybersecurity as a technical challenge, to be handled by the IT departments, rather than a strategic threat to be prioritized across the entire organizational structure through fully integrated enterprise risk management systems.

Cybercrime Events and Their Impact

Both Egan (2014) and PWC (2014) suggest that the prevalent view in the business and regulatory community is that cybersecurity breaches can pose a systemic threat to the financial sector as a whole or to the financial markets at large. However, empirically mainstream literature on the subject still lacks evidence to prove such a hypothesis.

Corbet and Gurdgiev (2019) look at 819 cybercrime events with sufficient disclosure identified between January 1, 2005, and April 30, 2015, which are divided into the following categories: data breaches caused by an employee release, data breaches caused by an external data breach or hack, data breaches caused by a lost, stolen, or discarded internal data device, and data breaches caused by unintentional disclosure. The data is taken from the systemic analysis of the LexisNexis database, using methodologies described in Corbet and Gurdgiev (2019). Our analysis and data collection cover the publicly listed companies regulated by the U.S. Securities and Exchange Commission, which represents a wide range of multinational, globally trading companies, as well as all foreign-registered companies trading on the U.S. exchanges. As a result, our data represents the entire population of all publicly disclosed breaches involving U.S. regulated companies.

Figure 13.1 shows the evidence for Cumulative Abnormal Returns (CAR) relating to hacking events.[10] The data clearly indicates that financial markets are becoming more aware of the negative sentiment contained within these events and are punishing the companies involved. This analysis was confirmed by an investigation of company media coverage in the days following the identified cybercrime events.

In Table 13.1 we display the annual summary statistics relating to announced hacking events on publicly 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

Table 13.1 Annual summary statistics of the included cybercrime events (2005–2015)

Year	*Total number of events*	*Clients records exposed*	*Average of CAR*	*Total number of hacking events*	*Clients records exposed in hacking events*	*Average of CAR to a hacking event*
2005	30	677,314,000	−1.59	4	36,480,000	−1.34
2006	108	498,330,900	−2.46	15	27,402,500	−3.25
2007	85	408,197,900	−1.51	19	18,690,700	−2.68
2008	45	326,522,000	−1.76	8	128,056,800	−0.87
2009	44	238,973,800	−2.67	13	54,655,000	−4.97
2010	134	573,785,700	−3.29	29	242,697,200	−5.12
2011	126	1,008,086,300	−2.63	34	409,421,900	−6.20
2012	104	264,776,600	−4.36	33	217,769,000	−8.40
2013	62	430,011,700	−4.78	20	190,794,800	−6.39
2014	56	644,055,000	−6.48	37	559,620,000	−10.56
2015[a]	*25*	*120,671,600*	−6.19	*18*	*57,186,600*	−10.15

Source: Authors' own data extraction from the LexisNexis database, see Corbet and Gurdgiev (2019)

Note: The above events are compiled after a thorough search of company announcements relating to cybercrime and a thorough media investigation using the LexisNexis 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

[a] 2015 data covered in the study implies annualized, seasonally adjusted rate of 93 total cybercrime events, and 48 hacking events implying a reversal in the 2013–2014 dynamics

[10] CAR methodology for assessing financial markets penalty for cybersecurity breach is consistent with that used in The Council of Economic Advisers (2018).

companies involved. The frequency of these events is of primary concern. On one hand, numerous hacks may indeed be kept as private as possible due to the reputational damage and other associated concerns attached. On the other hand, the proliferation of social and media fora creates an environment where such concealment is harder to execute. More disturbingly, there has been a dramatic rise in the number of hackers and hacking organizations that 'take responsibility' for their actions, further fuelling the debate about the lack of legal scope and punishment against such actions.

Hacking has become more prevalent and more costly to targeted firms since 2010. CAR analysis presents evidence that the average stock market reaction in the ten days following the hacking event has become increasingly negative as one would expect. Whereas, between 2005 and 2008, the average CAR fell by 3 percent, the same abnormal returns have fallen over 5 percent since 2010, with 2014 and 2015 presenting the largest average falls of over 10 percent associated with hacks. In fact, since 2010, the minimum of the ten-day post-CAR, reflective of the worst-case scenario for the investigated companies, indicates that post-hack share price falls in excess of 45 percent.[11] This share price behaviour presents evidence that stock markets attempt to 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 in Table 13.1, where we identify an increasingly negative sentiment pertained in the CARs associated with hacking events over time, with the trend peaking at over 10 percent in 2014 and 2015.

Analysing the summary statistics for all events presents evidence that, as a proportion of total cybercrime, hacking is now the most dominant form and has grown substantially throughout the period. This result validates the scope of this chapter that hacking is a concern that is simply not disappearing and requires a proactive, pre-emptive, and preventative approach to enforcement.

The ease of sale of stolen data appears to be incentivizing hackers to further the scale and sophistication of their attacks, particularly with lucrative profits correlated to the number of individual records that can be

[11] Data on other cyber-risk events, including accidental disclosure of data, and theft of data and devices is available in Corbet and Gurdgiev (2019).

obtained (Ablon et al. 2014; Townsend 2014; Boes and Leukfeldt 2016).[12] This phenomenon increases the scope of issues for companies and regulators alike.[13]

The above evidence is in line with the findings reported in more current studies. For example, Ponemon (2018b) shows significant increases in the cost of cybersecurity breaches in 2017–2018. According to the author, the average total cost of a data breach rose 6.4 percent in 2018 to reach US$3.86 million per company impacted by the breach. In contrast, in 2014, the average total cost of data breaches was US$3.5 million. The severity of the breaches rose as well: the average cost for each lost record rose to US$148, an increase of 4.8 percent. Meanwhile, the average size of the data breach is up 2.2 percent. Per Ponemon (2018b, p. 3), 'the average global probability of a material breach in the next 24 months is 27.9 percent, an increase over last year's 27.7 percent'. In 2014, the first year covered by the annual Ponemon reports, the same probability was 22.2 percent. Confirming our findings above, Ponemon (2018b) also shows that malicious or criminal cyberattacks took longer to identify and detect in 2018 than in 2017. Overall, The Council of Economic Advisers (2018, p. 1) estimates that 'malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016'. Finally, Accenture (2019, p. 14) reports estimates of the value of economic activity at risk from cybersecurity events:

> globally, we found that the total value at risk from cybercrime is US$5.2 trillion over the next five years. … [and] the size of opportunity varies by industry, with High tech subject to the greatest value at risk—US$753 billion—over the next five years, followed by US$642 billion for Life Sciences and US$505 billion for the Automotive industry.

This statement supports our assertion that cybercrime impacts are widely distributed across the globe and economic sectors.

[12] 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.

[13] A substantive discussion of legal and enforcement challenges relating to development and implementation of cybercrime combatting legal frameworks and operational enforcement systems is discussed in Kramer et al. (2009) and Wilson (2014).

Systemic Risk Spill-Overs from Hacking Events

Corbet and Gurdgiev (2019) present the evidence for stock price volatility and contagion for all companies above US$1 billion market capitalization based on the results of the individual EGARCH analysis of hacking events between 2005 and the end of April 2015 across the differing cybercrime types, defined in Sect. "Cybercrime Events and Their Impact" above. Almost every company's stock price in the sample has a statistically significant and positive systematic co-movement with the global stock markets, indicating exposure to global systematic risk.

We note the presence of heteroscedasticity and volatility persistence in our returns data. When testing for contagion and volatility spill-overs, methods which do not correct for heteroscedasticity are found to be biased. Such tests overstate any increases in market volatility and the magnitude of cross-market relationships. As such, non-heteroskedastic adjusting tests may incorrectly suggest that volatility spill-overs have occurred. To account for this, we implement a variation of the generalized autoregressive conditional heteroscedasticity (GARCH) based approach. Specifically, we use the exponential generalized autoregressive conditional heteroscedasticity (EGARCH) model, as it allows for asymmetric effects between positive and negative returns. After completing the standard robustness tests, the EGARCH (1,1) methodology, for the most part, was selected as the appropriate model to test for changes in volatility. We also considered the use of GARCH, Threshold GARCH (TGARCH), and GJR-GARCH, but EGARCH was found to outperform each methodology. An intercept and a deterministic trend were included in the Augmented Dickey Fuller (ADF) and Phillips Perron (PP) models. The trend was included to capture the reduction in average volatility that took place during the period under investigation. The ADF model tests, whether the equity series, contain 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 test down by sequentially removing the last lag until a significant lag is reached. This gives the order of augmentation for the ADF test that minimized the Akaike information criterion. The results rejected the null-unit root hypotheses at a minimum of the 5 percent level. Models that incorporate volatility asymmetries, or negative correlations between returns and volatility innovations, generally outperform models that do not. Further, the EGARCH methodology exploits information contained in realized measures of volatility while providing a flexible leverage function that accounts for return-volatility dependence and remaining in a GARCH-like modelling framework and estimation convenience. The model allows independent return and volatility shock, and this dual shock nature leaves a room for the establishment of a variance risk premium.

Focusing on hacking events, Corbet and Gurdgiev (2019) note that hacking events are predominantly targeted at higher value publicly listed companies (in this case: over US$1 billion in market capitalization). This finding indicates that some of these companies may have superior physical security systems in place to mitigate other cybercrime events, such as physical theft and insider release, but the increased sophistication of hacking appears to affect larger companies just as effectively as the smaller ones.

Of the 29 reported large 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. Hacking events taking place between 2012 and 2015 included 34 large-scale events. Of these, nine hacks resulted in no contagion and only one event resulted in systematic contagion, five hacks resulted in idiosyncratic contagion, whereas the remaining 19 events were a result of a combination of the contagion channels.

Segregating the differing types of contagion stemming from cybercrime over time presents interesting observations based on stock market behaviour. Figure 13.2 documents the rise of systematic contagion since early 2014.

In 2014 over 12 percent of cybercrime events resulted in systematic contagion to the wider national stock exchange. 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 rise 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. Investors also appear to recognize that the successful targeting of one company may in fact represent a wider

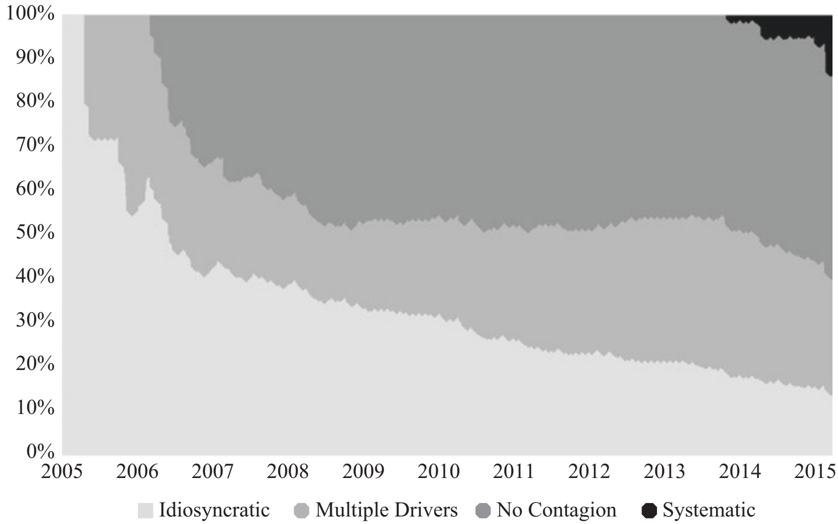

Fig. 13.2 EGARCH calculated contagion type stemming from cybercrime event (2005–2015). Source: Corbet and Gurdgiev (2019)

threat to the technological structures of domestic publicly traded companies, therefore resulting in such systematic contagion. The results provided in Corbet and Gurdgiev (2019) continue to present evidence of continuing advancements in contagion resulting 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.

White Knights and Proactive Risk Mitigation

The increasingly systemic nature of risks involved in cybersecurity attacks requires more than an amplification of the currently prevalent means for preventing and mitigating the damages inflicted onto companies, exchanges, and economic systems by such adverse events. In line with the empirical findings in Corbet and Gurdgiev (2019), we propose that the regulatory authorities interested in developing preventative approaches to cybersecurity introduce a more structured relationship with hacktivists and the ‘white knights’ in order to dis-incentivize ‘black knight’ cyber attackers and to reduce the flows of talent toward illicit hacking activities.

This objective can be achieved via formally establishing a link between white knight hackers success in penetrating the company security systems based on a fully supervised hack and the financial rewards that can be generated by such a success.

We propose that the regulatory authorities create an open pool for white knight hackers that can be accessed by any fully vetted and registered hacktivist. The authorities can either algorithmically (including randomly) or systemically (e.g. based on pre-set micro- or macro-prudential risk criteria) identify target companies for security systems testing.[14] In the event that a white knight hacker succeeds in hacking the systems of the selected company, a fine proportional to the potential scale of damages can be imposed by the regulatory authorities. This fine can be subsequently co-shared with white knight hacktivists instrumental to detecting the vulnerability.

To reduce incentives to ‘double dip’—an activity whereby a white knight hacktivist first penetrates the company cybersecurity systems for the purpose of gaining the regulatory reward, and then subsequently uses/resells access software to collect information illicitly, the pay-outs from the winners’ pool should be staggered over time (e.g. 3–5 years), conditional on no repeat security breaches of the tested company. As a second order effect, such time lock-in can also nudge greater degree of commitment by the hacktivists to assisting regulators and enforcement agencies over time, following their first successful contest.

The key regulatory and enforcement objective of the white knight contest would be to identify the unexposed liabilities of a company and deploy regulatory enforcement based on such a discovery. A mechanism for this cooperative interaction can be glimpsed from the Federal statutes and practices relating to the Racketeer Influenced and Corrupt Organizations Act, RICO,[15] and the Dodd-Frank Act[16] recovery approaches, in which a percentage of fines secured against the corporate misbehaviour is allocated

[14] This mixed approach is consistent with the selection mechanisms currently used by the tax authorities in identifying target companies and individuals for conduct of audits.

[15] See https://www.justice.gov/sites/default/files/usao/legacy/2012/10/31/usab6006.pdf for some details on RICO cases rewards.

[16] See http://www.kmblegal.com/practice-areas/whistleblower-law/dodd-frank-act-whistleblower-incentives for some details on Dodd-Frank Act and associated whistleblower rewards system.

to the entities (including for-profit organizations) and/or individuals (especially, whistle-blowers) that help to proactively expose corporate malfeasance.[17]

Beyond the above mechanism, owing to the highly uncertain nature of the size and the likelihood of the payoff for individual hacktivists, we propose that the regulatory authorities provide a notional reward to the top five or even the top ten of the white knight hacktivists who take part in the hacking contest.

This payment, alongside the staggered payout, are two crucial modalities to our proposal because they ensure that hacking contests would remain active and well-resourced, even in the event where a small group of hackers comes to dominate the market in any period of time, capturing the top rewards repeatedly. Recently, Brown (2015) modelled the decision of a profit-motivated hacker to choose the life of a malicious hacker, a 'black hat', or to provide cybersecurity services as a 'white hat' hacktivist. Brown (2015, p. 1) notes that 'a key component of the model is the contest between white and black hats for some part of firm output that is vulnerable to attack. White and black hat earnings are increasing, nonlinear functions of the proportion of black hats'. In the context of our structuring of approved white knight contests, the regulatory and supervisory authorities need to include in the white knight enforcement system design an explicit incentive for non-winning hackers to remain in the white knights pool. As per Brown (2015, p. 3), 'assuming that hackers prefer to work in the industry with the highest returns, when white hat wages fall below the amount that could be made working as a black hat, hackers will switch to black hat work.

Fortunately, although displaying a general lack of consensus within the profession itself, many individual regulators and regulatory analysts are increasingly converging on the view that in relation to cybersecurity risks, threat intelligence is the key to more proactive management of the cybersecurity (Dahlgren 2015; Rosengren 2016; DHS 2018). Our proposal is in line with this evolving approach to structuring preventative systems for enhancing cybersecurity.

[17] Dahlgren (2015) argument can be seen as supportive of the idea that regulatory and supervisory fines should apply more broadly to the cases of cybersecurity breaches. She states: 'I fear that until we can assign financial consequences to cyber risks, and ensure staff are taking that into account when making decisions, we will not get the commitment needed from every level of the organization to adequately address the problem. As long as decisions are made and actions are taken without this type of assessment, we are going to see more and more of these weaknesses exposed.'

Concluding Remarks

To understand the nature and extent of cybersecurity risks contagion across the financial markets, Corbet and Gurdgiev (2019) have implemented an EGARCH-based modelling framework that encapsulates several channels of contagion and relates them to 819 observed incidents of cybercrime between 2005 and 2015. The authors find that hacking was the most prevalent source of cybercrime, with incidents becoming more frequent and sophisticated since 2012. This increase has resulted in wider transmission of systematic and idiosyncratic contagion to the domestic stock exchange in which the companies' stock trades. Two key findings from Corbet and Gurdgiev (2019) are of significant interest to regulatory authorities in shaping the future institutional structures for addressing rapidly evolving cybersecurity risks. Firstly, stock market volatility was found to be strongly positively correlated to both the size of the company and the number of client's records that have been obtained through the cybercrime incident. Secondly, the changing nature of contagion from cybersecurity events to the broader financial markets: between 2005 and 2012, almost 50 percent of all contagion could be denoted as either idiosyncratic or a combination of idiosyncratic and systematic contagion. Since 2014, systematic contagion has grown rapidly, to the extent that over 10 percent of such contagion to the wider stock exchange originates from cybercrime events.

In response to these findings, the present chapter stresses the need for an immediate and robust regulatory intervention to mitigate the potential disastrous effects of cybercrime. The timeliness of such intervention is ever more important given the growth of cybercrime in recent years, their complexity, their use for commercial and political purposes, and the development of AI. Cybercriminals currently appear to be more advanced in a host of key areas than those whose role is to monitor and regulate. Therefore, it is of vital importance that urgent action is taken. A novel alternative and regulatory strategy for combatting cybercrime, as discussed in this paper, includes formally integrating 'white knights' hacktivists into regulatory institutions of risk prevention, mitigation, and regulatory enforcement. We propose that the regulatory authorities interested in developing preventative approaches to cybersecurity introduce a more structured relationship with white knight hackers. These structured relationships should aim to dis-incentivize black knight cybersecurity attackers and to reduce the flows of talent toward illicit hacking activities, while simultaneously increasing the rate and the robustness of cybersecurity risk tests imposed onto publicly listed companies.

References

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for cybercrime tools and stolen data. *Rand National Security Division*. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

Accenture. (2019). The cost of cybercrime. Retrieved from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf.

Alva Group. (2016, November 10). What is the long-term impact of a cybersecurity breach on corporate reputation? *Alva*. Retrieved from https://www.alva-group.com/case-studies/what-is-the-long-term-impact-of-a-cybersecurity-breach-on-corporate-reputation/.

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), 265–300.

Beckert, J., & Dewey, M. (2017). The architecture of illegal markets: Towards an economic sociology of illegality in the economy. *Oxford Scholarship Online*: August 2017. https://doi.org/10.1093/oso/9780198794974.001.0001.

Boes, S., & Leukfeldt, E. R. (2016). Fighting cybercrime: A joint effort. In R. M. Clark & S. Hakim (Eds.), *Cyber-physical security: Protecting critical infrastructure at the state and local level*. Springer.

Brown, C. (2015). *White or black hat? An economic analysis of computer hacking* (working paper). Retrieved from the Economics Department of Georgetown University.

Chen, L. Y., & Yuji Nakamura, Y. (2016, August 5). Hacked bitcoin exchange says users may share $68 million loss, *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2016-08-05/hacked-bitcoin-exchange-says-it-will-spread-losses-among-users.

Corbet, S., & Gurdgiev, C. (2017a). Hacking the market: Systemic contagion from cybersecurity breaches, LSE Business Review, Retrieved November, 2017, from http://eprints.lse.ac.uk/86064/.

Corbet, S., & Gurdgiev, C. (2017b). Financial disrupters: Is the rise of financial disruptors knocking traditional banks off their track? *Journal of Terrorism and Cyber Insurance, 1*(2), 58–62.

Corbet, S., & Gurdgiev, C. (2019). What the hack: Systematic risk contagion from cyber event. *International Review of Financial Analysis, 65*, 101386.

CPMI-IOSCO. (2016). *Guidance on cyber resilience for financial market infrastructures*. Retrieved from BIS: https://www.bis.org/cpmi/publ/d146.pdf.

Dahlgren, S. (2015, March 24). The importance of addressing cybersecurity risks in the financial sector. *Federal Reserve Bank of New York*. Retrieved from https://www.newyorkfed.org/newsevents/speeches/2015/dah150324.

DHS. (2018). *Cybersecurity strategy*. Department of Homeland Security. Retrieved from https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

Egan, M. (2014, March 20). Companies turn to cyber insurance as hacker threats mount. *Fox Business*. Retrieved from http://www.foxbusiness.com/features/2014/03/20/companies-turn-to-cyber-insurance-as-hacker-threat-mounts.html.

Finkle, J., & Spicer, J. (2016, June 7). U.S. warns banks on cyber threat after Bangladesh heist. *Reuters*. Retrieved from http://www.reuters.com/article/us-cyber-heist-regulator-idUSKCN0YT25H.

Greenfield, D. (2014). Social media in financial markets: The coming of age…, [GNIP White Paper]. Retrieved from https://s3.amazonaws.com/st-research/social-media-and-markets-the-coming-of-age.pdf.

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), 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), 373–380.

Kelly, M. (2013, November 8). From dark days to white knights: 5 bad hackers gone good. *Venture Beat*. Retrieved from http://venturebeat.com/2013/11/08/black-to-white-hat/.

Keplinger, K. (2018). Is quantum computing becoming relevant to cyber-security? *Network Security, 2018*(9), 16–19.

Khrennikov, I. (2016, June 15). Hackers found selling access to 70,000 company computer systems. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2016-06-15/your-company-s-servers-now-on-sale-for-just-6.

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

Kramer, F. D., Starr, S. H., & Wentz, L. K. (2009, April). *Cyberpower and national security*. Center for Technology and National Security Policy, National Defense University, Washington DC. Retrieved from http://ctnsp.dodlive.mil/2009/04/01/cyberpower-and-national-security/.

Kremer, J. (2014). Policing cybercrime or militarizing cybersecurity? Security mind-sets and the regulation of threats from cyberspace. *Information and Communications Technology Law, 23*(3), 220–237.

Larson, E., Hurtado, P., & Strohm, C. (2016, March 24). Iranians hacked from Wall Street to New York dam, US says. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2016-03-24/u-s-charges-iranian-hackers-in-wall-street-cyberattacks-im6b43tt.

Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., Felegyheazi, M., Grier, C., … Savage, S. (2011). Click trajectories: End-to-end analysis of the spam value chain. *2011 IEEE Symposium on Security and Privacy*, pp. 431–446. Retrieved from http://www.ieee-security.org/TC/SP2011/PAPERS/2011/paper027.pdf.

MacKenzie, D. (2018). Material signals: A historical sociology of high-frequency trading. *American Journal of Sociology, 123*(6), 1635–1683.

McKendry, I., & Macheel, T. (2015, July 28). Regulators to step up cybersecurity activity: Lawsky. *American Banker*. Retieved from http://www.americanbanker.com/news/bank-technology/regulators-to-step-up-cybersecurity-activity-lawsky-1075715-1.html.

Novet, J. (2017, August 16). Shipping company Maersk says June cyberattack could cost it up to $300 million. *CNBC*. Retrieved from https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html.

Packin, N. G., & Aretz, Y. L. (2016). Big data and social netbanks: Are you ready to replace your bank? *Houston Law Review, 53*(5), May 11, 2016.

Ponemon Institute. (2015). 2015 Cost of data breach study: Global. Retrieved from http://ibm.co/1FStqBu.

Ponemon Institute. (2018a). DNS cybersecurity & protection. Retrieved from https://www.onserve.ca/ponemon-institute-2018-cybersecurity-report-information/

Ponemon Institute. (2018b). 2018 Cost of data breach study: Global. Retrieved from https://www.ibm.com/downloads/cas/861MNWN2.

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

Riley, M., Robertson, J., & Geiger, K. (2015, October 17). Russian hackers of Dow Jones said to have sought trading tips. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2015-10-16/russian-hackers-of-dow-jones-said-to-have-sought-trading-tips.

Rollins, J., & Wilson, C. (2007). *Terrorist capabilities for cyberattack: Overview and policy issues* (Congressional Research Service (CRS) Report for Congress, Order Code RL33123), The Library of Congress, updated January 22, 2007, 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. *Federal Reserve Bank of Boston*. Retrieved from https://www.bostonfed.org/news-and-events/speeches/2016/perspectives-on-risks-both-economic-and-cyber.aspx.

Security Magazine. (2019, June 20). Domain name system attack cost rises 49 percent to $1,070,000. Retrieved from https://www.securitymagazine.com/articles/90400-domain-name-system-attack-cost-rises-49-percent-to-1070000.

Shell, A. (2017, September 17). Equifax image is battered by data breach as consumers feel violated. *USA Today*. Retrieved from https://www.usatoday.com/story/money/2017/09/18/equifax-image-battered-data-breach-consumers-feel-violated/677908001/.

Spam Titan. (2019, January 25). New research reveals extent of reputation loss after a cyberattack. Retrieved from https://www.spamtitan.com/web-filtering/new-research-reveals-extent-of-reputation-loss-after-a-cyberattack/

Stearns, J. (2016, July 6). European Union's first cybersecurity law gets green light. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2016-07-06/european-union-s-first-cybersecurity-law-gets-green-light.

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

The Council of Economic Advisers. (2018). The cost of malicious cyber activity to the U.S. economy. *The Council of Economic Advisers*. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

Tiedemann-Nkabinde, R., & Davydoff, D. (2019, March 4). Why reputational risk is a security risk and what to do about it. *Security Magazine*. Retrieved from https://www.securitymagazine.com/articles/89908-why-reputational-risk-is-a-security-risk-and-what-to-do-about-it.

Townsend, K. (2014, September). Cybercrime and punishment. *InfoSecurity*. Retrieved from http://www.infosecurity-magazine.com/magazine-features/cybercrime-and-punishment/.

UN. (2011). Cybersecurity: A global issue demanding a global approach. Retrieved from http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html.

Wilson, C. (2014). Cyber Crime. In F. D., Kramer, S. H., Starr, & L. K. Wentz (Eds.), *Cyberpower and national security* (Chapter 18). Center for Technology and National Security Policy, National Defense University, Washington DC, April 2009. Chapter 18 updated version from March 2014. Retrieved from http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-18.pdf.

Yampolskiy, R. V. (2016, June 13). Fighting malevolent AI: Artificial intelligence, meet cybersecurity. *The Conversation*. Retrieved from https://theconversation.com/fighting-malevolent-ai-artificial-intelligence-meet-cybersecurity-60361.