Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54
Publication Date: 05-10-2023 ISSN: 2706-6495

An Analysis of Impact Extent of Cybersecurity on Confidence in Securities Market

By: Sumayah Saed S. Alsahafi

PhD Candidate at the University of Manchester, Saudi Arabia

Email: sumayah.sahafi@gmail.com

Abstract

Risk and opportunity more often can be seen as two sides of the same coin, for which modern technology is a fantastic illustration. This dichotomy generates prospective market disruptions and a variety of future opportunities. The history of cyberattacks is thought to have started during the cold war. This dissertation investigates cybersecurity control to maintain investors' trust in the securities market. A primary cause for the loss or decline in value of multiple financial markets was the lack of cyber-regulation in the financial sector.

Does regulation offer the best means of preserving investors' faith in securities? Is there a plan to replace it? The data demonstrates that the dangers associated with cybersecurity cause investors to lose faith in markets, resulting in considerable financial consequences. The study suggests that understanding the interrelationships with cybersecurity is crucial to maintaining the efficiency of the financial markets and keeping pace with their continuous and rapid evolution.

The dissertation also highlights claims that regulations, particularly the disclosure approach, are evaluated to determine their effectiveness in the market. Although the national regime can be successful within its region, financial markets are known to be interconnected internationally and impact each other.

Keywords: Cybersecurity, Cold War, Technology, Cyberattacks, Investors, Securities Market, Financial Markets, Regulation, Confidence, Risk, Protection, Disclosure.

1. Introduction

1.1. Research background

Demonstrating how cybersecurity and the financial markets first came together is useful to set the scene and underline its importance for this study. Therefore, we first consider the history of cybersecurity in the financial markets and then review the concepts of cybersecurity as it applies to financial markets and their importance in boosting public trust in the sector.

1.1.1. The history of cybersecurity in financial markets

The Cold War's race in science and technology led to the development of the Internet. After World War II, tensions between the United States and the Soviet Union soon increased. The 1957 launch of the Sputnik spacecraft by the Soviet Union alarmed Americans. This launch altered how the world saw the United States as a technological superpower, making the American people feel vulnerable, and raised the Soviet Union's symbolic stature. As a result, the United States government changed its approach to focus more on technology and research in response to its perceived deficit as the prospect of nuclear war hung over the nation.[1]

As far as it has been known, the notion of the Internet as a self-governing cyberspace, Goldsmith and Wu argue, is now largely uprooted.[2] The unstoppable juggernaut that will overrun the old and outdated determinants of human governance and displace the role of territorial government has not materialised.[3] Instead, something akin to a technological version of the 'cold war'' is now in danger of emerging. The dream of a self-governed global network now looks more like a collection of nation-state networks struggling with the threat of the unchecked evils of anarchy. Users must now look forward to life in the 'bordered' Internet.[4]

The crucial point is that "people may hardly expect to be absolved of conformity with the law of those countries".[5] This is especially true if they seek to conduct business in, travel to live in, or use the infrastructure of other countries. In essence, the Internet does not maintain global cyber laws wherever it is used. On the other hand, financial markets must abide by the local regulations of

[1] Michael Gervais, 'Cyber Attacks and The Laws Of War' (2012) Journal of Law & Cyber Warfare 1.
[2] Jack Goldsmith, 'Who Controls The Internet? Illusions Of A Borderless World' (2007) 23 Strategic Direction.
[3] Goldsmith (n 2).
[4] Ibid.
[5] Ibid.

where they conduct business. This suggests that local rules may be utilised to control the effects of international Internet activity.[6]

The extent of business-government cooperation has significantly increased since 1998, despite its gradual and fragmentary progress. The financial sector was the first core infrastructure area to establish such a foundation for partnerships with governments. Integrating new information technology led to efficiency improvements, which slowed the process as worries about increased vulnerability were overtaken by an interest in efficiency gains.[7]

Following these worries, financial infrastructures have become a notable target of cyber threats that have increased in sophistication and intensity. Example events included a significant North Korean offensive against the financial transaction messaging network and an impactful Iranian distributed denial-of-service (DDoS) assault.[8] These attacks may have occurred because (i) many of the products in this sector are now digital rather than based on paper money or physical objects, and (ii) the financial industry is very integrated, and numerous businesses rely on the same technologies to perform crucial tasks, such as payments clearing and settlements.[9]

According to previous studies, breached markets experience reduced customer satisfaction and increased negative word of mouth. Although increasing shareholder value is a top priority for markets, a dearth of research exists on the impact of consumer data breaches on corporate valuations. According to Kashmiri et al., disclosing a significant investors' data breach in one US market is likely to raise investors' expectations of subsequent data breaches in other markets, leading to an interindustry contagion effect.[10] However, results are inconsistent, despite a solid theoretical foundation for hypothesising a negative market response to the news of viral assaults and security breaches.[11]

[6] Ibid.
[7] Sean Atkins and Chappell Lawson, 'Cooperation Amidst Competition: Cybersecurity Partnership In The US Financial Services Sector' (2021) 7 Journal of Cybersecurity.
[8] Lawrence A. Gordon and others, 'Increasing Cybersecurity Investments In Private Sector Firms' (2015) Journal of Cybersecurity.
[9] Gordon and others (n 8).
[10] Saim Kashmiri, Cameron Duncan Nicol and Liwu Hsu, 'Birds Of A Feather: Intra-Industry Spillover Of The Target Customer Data Breach And The Shielding Role Of IT, Marketing, And CSR' (2016) 45 Journal of the Academy of Marketing Science.
[11] Ali Alper Yayla and Qing Hu, 'The Impact Of Information Security Events On The Stock Value Of Firms: The Effect Of Contingency Factors' (2011) 26 Journal of Information Technology.

Moreover, industry assessments indicate that markets have minimally focused on cybersecurity investments during the previous ten years. The difficulty in demonstrating the value of securities infrastructure investments appears to be the more significant barrier to obtaining adequate funding for cybersecurity needs.[12] To make effective information security investment decisions, develop an effective security management strategy, and create related policies,[13] determining the actual cost of potential security incidents, such as virus attacks and security breaches from internal and external sources, is necessary.[14]

However, the cost analyses of these incidents are frequently disregarded by many markets. For example, 32% of respondents to the 2004 e-Crime Watch Survey reported not keeping track of financial losses caused by electronic or related crimes.[15] A possible cause of this lack of reporting is how difficult it is to measure the cost-benefit ratios of cybersecurity efforts. Contributors to this issue include the scarcity of precise measures and efficient tools for economic and financial analysis.[16]

Although numerous media and trade publications exist regarding the estimated physical cost of computer virus assaults and security breaches, most of the statistics presented are rarely empirically tested for accuracy and dependability. In addition, data collection faces considerable obstacles in cybersecurity research. First, data is required to detect a security event, and it is estimated that only one-tenth of computer attacks are discovered.[17] Second, challenges exist in reporting the discovered attacks. For example, of the respondents to the Crime Scene Investigation and Federal Bureau of Investigation (CSI/FBI) Computer Crime and Security Survey conducted in 2004, 48% acknowledged they did not disclose all instances of computer intrusion incidents, with only 20% reporting to law enforcement organisations, and 16% to internal corporate legal

[12] Hasan Cavusoglu, Huseyin Cavusoglu and Srinivasan Raghunathan, 'Economics of IT Security Management: Four Improvements To Current Security Practices' (2004) 14 Communications of the Association for Information Systems.
[13] Anat Hovav and John D'Arcy, 'The Impact of Denial-Of-Service Attack Announcements on the Market Value Of Firms' (2003) 6 Risk Management and Insurance Review.
[14] Yayla and Hu (n 11).
[15] Josh McNutt, 'Analysis of the US-CERT DAC' (2004) Carnegie-Mellon University Pittsburgh Pa Software Engineering Inst.
[16] Yayla and Hu (n 11).
[17] Seymour Bosworth and Michel E. Kabay (eds) *'Computer security handbook'* (John Wiley & Sons, 2002).

councils.[18] This low reporting rate exacerbates the estimate that only 10% to 20% of all cyber-related attack occurrences are discovered.[19] A primary justification for not disclosing is the concern that unfavourable publicity may significantly affect the organisation's stock price.[20]

After an attack, many compromised organisations spent millions of dollars bolstering security measures and tightening security controls. However, more than 20% of the compromised markets still experienced significant losses in income, clientele, and business opportunities. As a result of the potential impact on business value and operations, cybersecurity is swiftly increasing as a priority by corporate governance and executive leadership. For instance, 88% of CEOs in the United States are concerned that cyberattacks could obstruct the growth of their businesses. Similarly, investors are now asking for more information on data breaches, cyber-security concerns, and how markets manage these risks.[21]

Responding to these increased concerns, in May 2011 the Securities and Exchange Commission (SEC) hosted a roundtable meeting to explore the cybersecurity landscape and disclosure problems to address the growing cyber risks. Following this, the SEC's Division of Corporation Finance released disclosure recommendations on cybersecurity in October 2011[22] to help businesses decide when to disclose cybersecurity risks.

In response to multiple accounting disasters at companies like Enron and WorldCom, the Sarbanes-Oxley Act (SOX) of 2002 was passed. Stockholders of these companies lost their jobs and a significant portion of their asset value, including entire retirement savings for many. The SOX Act is not a deterrent to financial and accounting crimes but supports maintaining investors' faith in the stock market, although it is not flawless.[23]

[18] Yayla and Hu (n 11).
[19] Bosworth and Kabay (n 17).
[20] Sotirios Pirounias, Dimitrios Mermigas and Constantinos Patsakis, 'the Relation between Information Security Events and Firm Market Value, Empirical Evidence on Recent Disclosures: An Extension of the GLZ Study' (2014) 19 Journal of Information Security and Applications.
[21] He Li, Won Gyun No and Tawei Wang, 'SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors' (2018) 30 International Journal of Accounting Information Systems.
[22] Ibid.
[23] Dave Chatterjee, 'Should Executives Go To Jail Over Cybersecurity Breaches?' (2019) 29 Journal of Organizational Computing and Electronic Commerce.

National efforts are emerging to organise cybersecurity within the financial markets.[24] However, the global, interrelated structure of financial markets makes it challenging for governments to agree on international legislation or specific strategies to prevent attacks that could distribute impact between them.

1.1.2. The concept of cybersecurity

According to the SEC, cybersecurity is "the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorised access".[25] However, the SEC does not define a cyberattack. The American Department of Defense makes three distinctions between various computer network operations: (i) The term computer network defence (CND) refers to measures taken "to protect, monitor, analyse, detect and respond to unauthorised activity within Department of Defense information systems and computer networks", (ii) computer network attacks (CNA) are defined as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves", and (iii) computer network exploitations (CNE) are defined as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks".[26] Legal studies typically ignore military views of CND or CNE in favour of concentrating on CNA, commonly referred to as cyberattacks.[27]

To carry out a successful cyberattack, the attacker must have access to the target's computer or network, either remotely (through the Internet) or locally (through a thumb drive, for example). This access is necessary to exploit a vulnerability, such as modified software or hardware, and deliver a 'payload', which is typically software that, once installed on the target computer, performs a variety of nefarious tasks, such as "reproducing and retransmitting itself, destroying files on the system, or altering files". People within a targeted organisation remain the weakest

[24] Ibid.
[25] Matthew F. Ferraro, 'Groundbreaking' Or Broken?: An Analysis Of SEC Cyber-Security Disclosure Guidance, Its Effectiveness, And Implications' (2013) SSRN Electronic Journal.
[26] Ferraro (n 25).
[27] Ibid.

point in computer network security as unsuspecting computer users who download harmful software, misplace hardware, or carelessly publish confidential information online.[28]

However, modern definitions of cyberattacks exclude or ignore that they can have severe economic consequences just as their kinetic counterparts, as illustrated in the following example. A fighter jet from state A flies into the airspace of state B and launches a bombardment on a farm and its crop field, utterly and irreparably destroying both. The physical damage is evident, as can be seen by the farm's devastation and crops burned. The financial loss is quantifiable, such as in this example, as having a replacement cost of $500,000. Here, it is clear that a kinetic weapon (i.e., the fighter jet's attached bombs) had kinetic consequences (physical destruction of a farm and crops). Now, consider a second hypothetical non-kinetic attack. An export credit agency (ECA) intrudes into the computer networks of state B's central stock exchange and manipulates and deletes information worth $500,000. Because no kinetic weapons were employed in this scenario, the ECAs may not be taken as seriously as the aircraft strike.[29]

From an impact perspective, damage worth $500k was caused in the first and second scenarios. According to some experts, such meddling with a state's economic health is "equivalent to an armed attack" from this impact-based perspective.[30] The second situation is likely to be considered less severe than the use of physical force. However, the first scenario would be categorised as using force, which is forbidden under international law. The different circumstance surrounding the act of the attack, for example, the use of military weapons following an intrusion into the sovereign airspace of state B, is what matters when classifying these events instead of the effects of the impact of the event, which appears to be the key consideration under international law regarding the use of force. In the age of cyber warfare, such difference may no longer be necessary, especially given the immense economic damage that a cyberattack can inflict.[31]

1.1.3. The value of cybersecurity to support confidence

As mentioned above, executives of organisations are gradually elevating cybersecurity to a key priority because no market is immune to cybersecurity risks. Following legislative developments,

[28] Ibid.
[29] Ido Kilovaty, 'Rethinking the prohibition on the use of force in the light of economic cyber warfare: towards a broader scope of Article 2 (4) of the UN Charter', (2014) JL & Cyber Warfare 4: 210.
[30] Kilovaty (n 29).
[31] Ibid.

cybersecurity is essential across all industries and even more important in the financial sector to increase protection for investors. Cybercrimes will continue to raise the risk of hacker attacks as digital data in the financial sector expands.[32]

This cybersecurity challenge is a primary concern for regulators and is gaining more attention from global organisations, such as the Financial Stability Board (FSB), Basel Committee and SEC. Cybersecurity is considered one of the largest concerns facing the financial sector, especially as process centralisation and digitisation develop along with financial institutions' internal concentration on the risks. Similarly, for new financial start-ups, these data-intensive markets frequently have a limited understanding or perception of security needs because they operate within a digital environment with a wealth of data. As a result, cybersecurity should be a top priority for these markets.[33]

Without the currently enabled technology, the financial markets of today are worthless. A market plan can benefit more from technology. Data can be stored, retrieved, analysed, reported, and redistributed without difficulty. Projecting annual growth and long-term goals are frequent practises among financial institutions. Technology serves as a tool to enhance operations and visibility for achieving these goals.[34] However, cybersecurity technologies exist to prevent all attacks and to consolidate the confidence and protection for the investors.

1.2. Aims of the research

The assessment above highlights the value of cybersecurity for financial securities and the effects cyberattacks have on financial markets, as well as how crucial strong cyber laws and investment policies are to the security and stability of financial markets.

This research evaluates how successfully investor trust has been safeguarded by regulatory reforms connected to cybersecurity. Examined are the most recent revisions to general frameworks for financial cybersecurity and cyber threats that harm the securities markets. Also, this study demonstrates if someone or some organisation is willing to take responsibility for an accused

[32] Jennifer Callen-Naviglia and Jason James, 'FinTech, RegTech and the Importance of Cybersecurity' (2018) Issues In Information Systems.
[33] Douglas W. Arner, Janos Barberis, and Ross P. Buckey, 'FinTech, RegTech, and the reconceptualization of financial regulation', (2016) Nw. J. Int'l L. & Bus.37 : 371.
[34] Gurdip Kaur, Ziba Habibi Lashkari and Arash Habibi Lashkari, *Understanding Cybersecurity Management In Fintech*, (Cham: Springer, 2021).

attack and stand up for the rights of the investors. Furthermore, the sector's exposure to these cyber-related risks can increase our understanding of the problem. Alternative strategies and regulation as a single financial sector response to cyber gaps are also discussed.

To protect investors, this dissertation demonstrates how disclosure alters the way financial markets operate. Also, an assessment of these disclosures is made to determine if the current framework varies in its application basis. The effects of disclosure are illustrated through specific cases that help identify the accountable party when disclosures are made incorrectly. These results suggest discloser benefits as an acceptable strategy to safeguard investors and markets.

The findings provide the basis for a study on cybersecurity disclosure in financial securities. With respect to cyberspace, this study evaluates how well regulation curbs risk-taking in financial institutions and suggests that regulations should consider these issues to ensure the effective expansion of cybersecurity operations. Evaluating if regulation is the best strategy to preserve the trust of investors in securities is a foundational aspect of this investigation, and these results can influence the field of financial policy and regulation.

1.3. Methodology

This dissertation uses a doctrinal approach to demonstrate how cybersecurity and financial securities can be combined to gain increased trust and protection of investors through an exposition of the rules governing cybersecurity in financial markets, analyses of the regulations, an explanation of problematic regions, and a potential prediction of future developments. A careful review of primary and secondary legal resources enables an in-depth investigation of the connections between certain variables and cybersecurity legal loopholes in the financial sector. Using this doctrinal perspective supports an enhanced understanding of the implications of this issue for financial markets.

Failure of cybersecurity in financial markets can create financial system disruptions at national and international levels and result in significant losses for investors because they are the most at-risk group. A study of expanding cybersecurity in the financial sector offers crucial information for maintaining the financial system's stability. A lack of international consensus that prevents all nations from reaching an agreement on cybersecurity challenges also motivates this study, which considers if the best approach to preventing attacks is to increase broad investment in cybersecurity so these incidents can be handled at an international scale.

1.4. Dissertation structure

Chapter 2 examines the cybersecurity concerns brought on by assaults on financial securities. This study considers some cases that significantly impacted financial markets because it is primarily concerned with analysing regulatory trends. This chapter also demonstrates if there is someone to blame for these attacks to address the protection of investors' rights. Next, this chapter considers how these dangers affect financial markets and argues how regulation can be the sole solution for these impacts. To assess the advantages and disadvantages of the pertinent legislation, the characteristics of these interactions are reviewed.

Chapter 3 evaluates disclosure regulation as the primary regulatory tactic leveraged by many rules to report the state of cybersecurity within the financial sector. The background of disclosure facilitates comprehension of the approach's beginning and significance. Due to this, the conclusions from other studies offer a useful tool for evaluating these strategies. Also, various viewpoints are asserted as presenting a more accurate picture of disclosure. The SEC-recommended disclosure process is demonstrated as being followed. The example scenario is presented where disclosure violates Rule 10b-5, resulting in the identification of the accuser, which is pertinent to the context of this study. Chapter 3 concludes the argument by the avails of disclosure to protect investors and markets.

Chapter 4 concludes with a summary of the thesis objectives and research question and emphasises the significance and applicability of the study. Also, a summary of the debate of how the research leads to some advances is discussed, followed by an outline of the significance of the findings for financial market cybersecurity efforts. Finally, this chapter highlights areas that could benefit from additional study to advance knowledge of cyber processes in financial markets and the regulatory consequences.

2. Analysis of the confidence state in financial securities

Highlighting the importance of cybersecurity, as discussed in the previous chapter, requires an illustration of the risks in the financial sector, which facilitates an understanding of the ways in which to gain investors' confidence. Demonstrating the risks as we will do, provides a basis for determining who is responsible for risk-taking. This chapter further examines a wide range of influences of those risks on investors' confidence. The chapter concludes with an outline of the flaws of the strategy of regulation as the sole solution to preventing risk-taking behaviours.

2.1. Exposing the harmful risks in financial securities

Technology today is a great example of how risk and opportunity are progressively becoming two sides of the same coin. Technology is the source of many opportunities, as well as potential disruptions.[35] Risk is, in general, the likelihood that anything may go wrong. It concerns the uncertainty in different spheres of a person's daily life. For instance, a businessperson may view declining pricing as a risk to their company's revenue if they are uncertain whether the pricing will recover. Even more so than with trends such as that in the example, the risk of incurring the negative effects of a single or sequence of accidents most greatly affects investors' confidence.[36]

Financial institutions are primary targets of cyberattacks today because they largely run online. Sixty per cent of financial organisations employ cloud services, the majority of which are private clouds. In that context, there is an urgent need for the threat landscape to be explored, given how sophisticated cyber threats are becoming and the increased diversity and intensity of attacks. Cyber dangers take the form of security incidents that jeopardise the confidentiality, integrity or accessibility of data.[37]

To explore risks in this field, most studies use data on cyberattacks obtained directly from the market. However, managers can be strongly motivated to keep knowledge about cyberattacks a secret, particularly if the attack's occurrence and the extent of the harm it caused were unforeseen. Managers have been found to only reveal information about less damaging attacks, while keeping investors in the dark about any that were worse. In particular, if investors are unsure whether a company has information security issues, the management will withhold negative information unless it falls below a certain threshold.[38] Such behaviour can be counterproductive though since, often, while the market's response to disclosures of attacks is modest, the leakage of information on attacks previously covered up provokes an adverse and considerable response.[39]

Accordingly, there is evidence that businesses, in general, are paying closer attention to cyberattacks. As of 29 June 2014, 1517 companies listed on the New York Stock Exchange

[35] Maricela Ramírez and others, 'The Disclosures of Information on Cybersecurity in Listed Companies in Latin America: Proposal for a Cybersecurity Disclosure Index' (2022) 14 Sustainability.
[36] Kaur, Lashkari and Lashkari (n 34).
[37] Kaur, Lashkari and Lashkari (n 34).
[38] Ibid.
[39] Eli Amir, Shai Levi and Tsafrir Livne, 'Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets' (2018) 23 Review of Accounting Studies.

(NYSE) or National Association of Securities Dealers Automated Quotations (NASDAQ) included cybersecurity, hacking, cyberattacks or data breaches as potential business risks in their securities filings.[40] This followed a trend of increase compared to the previous two years (2013, 1288; 2012, 879). Against the background of heightened risk, the boards of publicly traded companies have adopted different strategies for their cybersecurity monitoring, with some utilising the whole board, others the audit committee and others a technology committee, while some are yet to produce active monitoring plans. SEC Commissioner Luis Aguilar noted a discrepancy between the degree of risk of security breaches and the measures boards have taken to manage that risk.[41] As a result, the implication is that many markets are still ill-equipped to handle cyber threats.[42]

Threat actors come in many forms, including professional cybercriminals, amateur hackers and rival nation-state security services. Foreign governments with the means and motivation to undermine or abuse the financial system are the most worrisome actors from a systemic standpoint. Some, such as North Korea, wish to take advantage of the system without thinking about the long-term effects. Others, such as Iran, wish to undermine the financial services in an effort to compete with the United States and its allies on a geostrategic level, while others still, such as Russia, aim to put systems at risk to act as a deterrent.[43]

The costs of these attacks may be high. To provide examples, a data breach of Target Corporation in 2013 with an estimated cost of at least $162 million affected almost 40 million consumers.[44] Verizon Communications, meanwhile, when attempting to acquire Yahoo!, reduced its offer price by $350 million after Yahoo! disclosed it had fallen victim to a 2014 cyberattack.[45] More recently, private financial data of roughly 143 million Americans was leaked in a breach at Equifax. Over 240 class action lawsuits are being defended by the company as a result, and $87.5 million has

[40] Danny Yadron, 'Boards Race to Fortify Cybersecurity' (2014) The Wall Street Journal.
[41] Yadron (n 40).
[42] Julia L. Higgs and others, 'The Relationship between Board-Level Technology Committees and Reported Security Breaches' (2016) 30 Journal of Information Systems.
[43] Atkins and Lawson (n 7).
[44] Brian Prince, 'Shifting Priorities: How Enterprises are Safeguarding against Cybersecurity Threats' (2015) 196 Forbes 119–124.
[45] Henk Berkman and others, 'Cybersecurity Awareness and Market Valuations' (2018) 37 Journal of Accounting and Public Policy.

already been spent on legal fees.[46] Cyberattacks such as these have compromised incredibly sensitive information, intellectual property and personal financial information, among others. Global economic losses from cybercrime are estimated to exceed $450 billion.[47] Considering this, it is clear to see how breaches have a detrimental effect on market valuations and investor protection.[48]

2.2. Who should be accused of failing to protect against risks?

An organisation should ideally be committed to protecting sensitive data, and accordingly, take every reasonable precaution and measure. The organisational representative can then, and only then, effectively address the concern that stakeholders are likely to have following a successful attack: "What did this institution do to prepare?" Such a representative should not be punished for the cyberattack if every attempt was made to prevent data breaches.[49]

Looking higher up the chain of command, it can be challenging to hold directors accountable for institution losses, as highlighted by the renowned decision made by the Delaware Court of Chancery in the Caremark International Inc. Derivative Litigation. In cases when a director's choice results in a loss, culpability is often assessed according to the director-protective business judgement rule, providing the decision was the result of a process that was either consciously evaluated in good faith or was otherwise sensible. Rather than subjecting directors to judges' or jurors' second-guessing, which may harm investors' interests, to allow for an impartial assessment of the choice then an investigation into the decision-making process is advisable. As such, the business judgement rule is process-oriented and underpinned by a great respect for all choices made by the board in good faith.[50]

When employees at Caremark caused losses by breaking federal laws, the court determined that "plaintiffs would have to show either (i) that the directors knew or (ii) should have known that

[46] Char Sample and others 'Culture + Cyber: Exploring the Relationship' In *Advances in Human Factors in Cybersecurity* (2017), 185–196.
[47] Higgs and others (n 42).
[48] Lawrence A. Gordon, Martin P. Loeb and Tashfeen Sohail, 'Market Value of Voluntary Disclosures Concerning Information Security' (2010) 34 MIS Quarterly; Sangmi Chai, Minkyun Kim and H. Raghav Rao, 'Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior' (2011) 50 Decision Support Systems.
[49] Chatterjee (n 23).
[50] Edward A. Morse, Vasant Raval and John R. Wingender Jr. 'SEC Cybersecurity Guidelines: Insights into the Utility of Risk Factor Disclosures for Investors' (2017) 73 The Business Lawyer 1–34.

violations of the law were occurring and, in either event, (iii) that the directors did not take any steps in a good faith effort to prevent or remedy that situation, and (iv) that such failure proximally resulted in the losses complained of". The court stated that this standard would be difficult to satisfy because it would effectively call for a lack of good faith in the performance of supervisory obligations.[51]

Accordingly, board decisions to use staff or technology to address cybersecurity concerns are likely to be shielded from liability claims in shareholder derivative lawsuits. Even if the market's cybersecurity precautions prove unsuccessful, the process-oriented business judgement rule seems to offer substantial protection for real board decisions. In the same way, allegations that directors failed to keep an eye on or exercise oversight over cybersecurity concerns are unlikely to prevail if the directors can show that they acted in good faith.[52]

In other cases, authorised personnel can pose serious cyber threats by misusing their authority and privileges. In further cases still, employees can cause potential damage unintentionally. For example, an employee can be a victim of a phishing attack if they click a malicious link that covertly downloads malware on their workstation/computer to create a backdoor.[53]

A high-performance security culture that encompasses the three core characteristics of dedication, preparation and discipline must have the support of the top management if it is to succeed.[54] The senior leadership is crucial for establishing security mechanisms that provide confidence, for requiring security audits and drills, demanding sufficient resources, rallying organisation-wide support, monitoring the performance constantly, enforcing security policies and so on.[55] They must take a hands-on approach, with great attention and effort if they are to comprehend the organisational weaknesses and what it will take to overcome the obstacles.[56]

It is bad practice to assign responsibility for cybersecurity to a group of security experts and then hold them accountable for failure.

[51] Morse, Raval and Wingender (n 50).
[52] Ibid.
[53] Kaur, Lashkari and Lashkari (n 34).
[54] P. K. Chatterjee, 'City Hosts a Highly-Heralded Cyber Security Event' (2018) Free Press Journal.
[55] Salah Kabanda, Maureen Tanner and Cameron Kent, 'Exploring SME Cybersecurity Practices in Developing Countries' (2018) 28 Journal of Organizational Computing and Electronic Commerce.
[56] Chatterjee (n 23).

This is a symbolic check-the-box strategy that is unlikely to yield real outcomes. Every organisational member must take joint ownership, duty and accountability for the security preparation, which must be led by top leaders to protect investors.[57]

2.3. Growing influences on risk-taking or risk-averse behaviours

A cyberattack often provokes reactions from investors, with a number of studies having demonstrated a correlation between negative cybersecurity events (e.g. when software vulnerability notifications are made,[58] announcements of IT products having viruses[59] or reports of cybersecurity breaches[60]) and low stock prices.

Looking in further detail, according to Campbell et al. in their 2003 study, there is a considerable negative market reaction to breaches involving violations of confidentiality but no discernible market response to other breaches. The authors concluded that as cybersecurity safeguards a variety of market assets, the economic repercussions of a security breach depend on the type and worth of the underlying assets affected.[61]

It has been demonstrated that breaches concerning major e-businesses in charge of sensitive data, such as Amazon, eBay, Yahoo, First Data Corporation and JP Morgan Chase, are likely to be perceived as having major economic consequences. Due to the massive volumes of sensitive data that these companies collect, keep and transport, any news of a cybercrime involving them is likely to cause a big, negative, anomalous return on their stock prices.[62]

In addition, the nature of the event determines how a cybersecurity incident or breach provokes a market reaction.[63] Wang et al. demonstrated that the market's reaction to a security breach may

[57] Ibid.
[58] Rahul Telang and Sunil Wattal, 'An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Prices' (2007) 33 IEEE Transactions on Software Engineering.
[59] Anat Hovav and John D'Arcy, 'Capital Market Reaction to Defective IT Products: The Case of Computer Viruses' (2005) 24 Computers & Security.
[60] Henk Berkman and others, 'Cybersecurity Risk Mitigation, Private Information Leakage and Earnings Announcements' (SSRN Electronic Journal, 1st December 2018) < https://www.researchgate.net/profile/Jonathan-Jona/publication/325752038_Cybersecurity_Awareness_and_the_Cost_of_Liquidity/links/5d726f0b92851cacdb23ff46/Cybersecurity-Awareness-and-the-Cost-of-Liquidity.pdf > accessed; Amir, Levi and Livne (n 39).
[61] Edward A. Morse, Vasant Raval and John R. Wingender, 'Market Price Effects of Data Security Breaches' (2011) 20 Information Security Journal: A Global Perspective.
[62] Ibid.
[63] Yayla and Hu (n 11).

depend on the specificity of the information provided—when the breach report contains highly specific details regarding the breach, the market reacts more negatively.[64]

Through case study investigations, Andoh-Baidoo, Amoako-Gyampah and Osei-Bryson examined the changes to the market values of companies whose systems had been compromised, to gauge the impact of different Internet security breaches.[65] An announcement regarding a company's Internet security vulnerability in a significant American newspaper was their definition of an event. The three-day event window they used for their analysis comprised the day before the event to the day after the event. Their sample of 110 incidents, which was ultimately reduced to 41 events, was sourced from reportage in the Wall Street Journal, New York Times, Financial Times, Washington Post and USA Today, concerning breaches between 1997 and 2003. On average, the companies in their survey saw a 3.18 per cent decline in market value. Of the 41 firms, all reported abnormally low returns; for 27 firms, the returns were negative, while 14 reported zero or positive returns during that time.[66]

From another perspective, Martin et al. considered the impact of a data breach on peer organisations as dependent on the breach's severity. While low-severity data breaches have a detrimental impact on competing firms' performance, higher-severity data breaches can be beneficial for them as clients of the breached company are then inclined to switch to a rival company due to the circumstances. According to Kashmiri et al., a peer firm's ability to prevent a similar data breach through its IT, its commitment to corporate social responsibility and its marketing acumen in the wake of the breach of the unlucky firm all have a moderating effect on the impacts of the breach on that peer firm.[67] Cyberattacks and security breaches may hurt peer companies, but at the same time, they will increase the market value of information security service providers such as those offering Internet security software and services and IT consulting firms.[68]

An organisation can be impacted by a cyberattack in a variety of ways, and these effects will change based on the type and gravity of the attack: (i) Above the surface as tangible costs: technical

[64] Berkman and others (n 60).
[65] Francis Kofi Andoh-Baidoo, Kwasi Amoako-Gyampah and Kweku-Muata Osei-Bryson, 'How Internet Security Breaches Harm Market Value' (2010) 8 IEEE Security & Privacy Magazine.
[66] Morse, Raval and Wingender (n 61).
[67] Berkman and others (n 60).
[68] Michael L. Ettredge and Vernon J. Richardson, 'Information Transfer Among Internet Firms: The Case of Hacker Attacks' (2003) 17 Journal of Information Systems.

investigation, customer breach notification, post-breach customer protection, regulatory compliance, public relations and cybersecurity improvements. The intangible costs might have a long-term impact on the firm's anticipated future cash flows, whereas the majority of tangible expenses are immediate or short-term; (ii) Beneath the surface as hidden or intangible costs: insurance premium increases, increased cost to raise debt, lost value of customer relationships, value of lost contract revenue, attorney fees and litigation, devaluation of trade name and loss of intellectual property. The Washington Post claims that there was an increase in cybersecurity breaches of over 50% between 2007 and 2008. Despite the fact that these violations affect a wide range of institutions, there is general agreement that they may be quite costly for markets: "lost current and future revenues brought on by the deterioration of a company's relationships with both its clients and its business partners; potential legal repercussions related to violations".[69]

Some recent studies point to a decrease in the average cost of cybersecurity breaches in recent years. That is, there appears to be a movement in investors' perspectives toward considering cybersecurity breaches as a corporate 'nuisance' or simply another regular operating cost, as opposed to posing a potentially major financial danger to the existence of markets.[70]

Other potential explanations for the waning effects of security breaches, according to Gordon et al., include successful recovery plans or clients who are more steadfastly willing to continue doing business with the afflicted organisations. Given the cumulative frequency of these instances over the past few years, customers now perceive security breaches as less serious than in the past. Hence, customers might now be more inclined to deal with enterprises that have experienced a breach due to the relatively routine occurrences of such breaches, in contrast to the beginning of the Internet age, when hacker assaults constituted a new and frightening phenomenon.[71]

A serious issue has been created lately by an apparent shift in investors' perspectives on data security incidents. Corporate executives have taken cues from investors to keep their firms' information security investments at the current level, or at least not raise them significantly, with modern investors viewing security breaches as more like a nuisance than as a potentially serious

[69] Lawrence A. Gordon, Martin P. Loeb and Lei Zhou, 'The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?' (2011) 19 Journal of Computer Security.
[70] Ibid.
[71] Oliver Hinz and others, 'The Influence of Data Theft on the Share Prices and Systematic Risk of Consumer Electronics Companies' (2015) 52 Information & Management.

economic threat to the survival of firms. Yet, this opens up the risk that a big unanticipated breach, or the famous "black swan", has the potential to endanger a company's viability.[72]

Hovav and D'Arcy investigated how security breaches such as viruses, worms and denial-of-service. Yet, the researchers concluded that the relative impact of each type of breach versus the others was uncertain.[73] Telang and Wattel, meanwhile, in a study specifically on software vendors' disclosures of vulnerabilities, discovered that each time a vulnerability was exposed, businesses experienced a market value loss of about 0.6 per cent, or roughly $0.86 billion, for each market.[74]

Some security breach research has documented how the stock market reacts negatively and significantly when there has been a security breach. Garg et al., for instance, charted "cybersecurity incidents" that occurred between 1996 and 2002. The occurrences include denial-of-service attacks, computer viruses and the theft of confidential information, in addition to situations where customer data were exposed. They discovered that for the enterprises concerned, the typical abnormal return was 5.3% over the three days that followed the occurrence.[75] Similar results were found by Cavusoglu et al., who discovered anomalous returns over a two-day timeframe of 2.1 per cent for 66 incidents between 1996 and 2001, where the markets reacted to "malicious attempts to interfere with a company's activity and its information". Both assaults on proprietary data and its integrity, and compromises of personal information, were included in the researchers' classification.[76]

Elsewhere in the literature, Ko and Dorantes compared the one-year financial performance of companies that faced cybersecurity breaches between 1997 and 2003 to similar companies without breaches using a matched-firm analysis. They investigated 19 businesses whose data were accessed improperly. Ko and Dorantes showed that while the performance of the security-breached enterprises was not significantly affected the following year, they tended to lag behind those that had not experienced a breach.

[72] Gordon, Loeb and Zhou (n 69).
[73] Hovav and D'Arcy (n 59).
[74] Sanjay Goel and Hany A. Shawky, 'Estimating the Market Impact of Security Breach Announcements on Firm Values' (2009) 46 Information & Management.
[75] Ashish Garg, Jeffrey Curtis and Hilary Halper, 'The Financial Impact of IT Security Breaches: What Do Investors Think?' (2003) 12 Information Systems Security.
[76] Kevin M. Gatzlaff and Kathleen A. McCullough, 'The Effect of Data Breaches on Shareholder Wealth' (2010) 13 Risk Management and Insurance Review.

The results offered "partial support" to their hypothesis that organisations that experience security breaches will go on to perform worse than their counterparts.[77]

The factors most likely to affect the size and direction of the stock price response to news of a security event are subject to debate among researchers. Occasionally, a company's characteristics and its performance on the stock market can be linked.[78] Hovav and D'Arcy's 2003 investigation found that a denial-of-service assault had significant negative effects for a subset of Internet-only businesses, but their overall sample showed no evident stock market reaction.[79] Similar to this, Cavusoglu et al. discovered that security breaches of online enterprises were more strongly connected to a negative stock price response than breaches of traditional firms. They also discovered that the attacks size had a moderating impact on the stock price response.[80]

Some researchers have explored events' characteristics in an effort to explain the sizes and patterns of stock price reactions to news of security problems, finding that the type of breach may influence how the stock market reacts.[81] Similar to this, the main finding by Campbell et al. was that the type of breach might influence the stock market reaction, with illegal data access, in particular, strongly related to an adverse stock market response.[82] In contrast to those findings, however, Cavusoglu et al. discovered that cases of unauthorised access to data in their sample were not punished more severely than other instances of security breaches. Accordingly, they concluded that the kind of breach did not affect how the stock market reacted to the incident.[83]

There are likely to be two potential securities market reactions to a leak of sensitive consumer data. Perhaps, as demonstrated by Cavusoglu et al. and Garg et al., the market may respond negatively to news of a breach, showing an awareness of the potential consequences of breaches.

[77] Myung Ko and Carlos Dorantes, 'The Impact of Information Security Breaches on Financial Performance of the Breached Firms: An Empirical Investigation' (2006) 17 Journal of Information Technology Management 13–22.
[78] Gatzlaff and McCullough (n 76).
[79] Hovav and D'Arcy (n 59).
[80] Huseyin Cavusoglu, Birendra Mishra and Srinivasan Raghunathan, 'The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers' (2004) 9 International Journal of Electronic Commerce.
[81] Gatzlaff and McCullough (n 76).
[82] Katherine Campbell and others, 'The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market' (2003) 11 Journal of Computer Security.
[83] Cavusoglu, Mishra and Raghunathan (n 80).

Alternatively, as observed by Hovav and D'Arcy and Campbell et al., there may be no significant securities market response to news of a data breach. The latter case could indicate that these occurrences have become so routine that they no longer provoke a major market reaction.[84]

Strangely, not every victim of a data breach encounters the same effects on their market price. Investors in the financial services sector are keenly aware of the consequences of data security because this is where the majority of sensitive data is stored and often exchanged. Financial services is the largest industry in terms of transaction volume and frequency, implying higher risk exposures and hence bigger potential losses. Furthermore, market capitalisation losses significantly impact financial services firms.[85]

Investors, who perceive breaches of employee or customer data unfavourably, especially in markets with great potential for growth, should be aware of these. A high decline in shareholder value is also often linked to a refusal by the firm affected to disclose specifics about the breach, a scenario firms should thus be wary of creating. In addition, since firms operating in larger markets are mostly shielded from a negative market-wide reaction to news of a data breach, firms operating in smaller markets appear to have most reason to fear the consequences of a breach occurring.[86]

It is difficult to assess the costs incurred by catastrophic breaches. For instance, a researcher at Mizuho Investor Securities first estimated the cost of the 2014 Sony hack to have been $1.25 billion. However, in such cases, the figures given by the firms targeted are substantially lower. Sony estimated that in the year following the incident, the cost of the investigation and corrective actions was $35 million. Another point worth mentioning is that most enterprises in major markets have insurance to cover a portion of their cyber risk; then, the enterprise, its insurance firm and the taxpayer will all bear a roughly equal share of the operational expenses of a cyber-breach.[87]

In summarising the findings from the literature presented here, the conflicting results on how cybersecurity breaches affect publicly traded companies' stock market returns are concerning for at least two reasons. First, the results of multiple surveys and anecdotal evidence repeatedly demonstrate that the costs associated with cybersecurity breaches are high, both generally and with

[84] Gatzlaff and McCullough (n 76).
[85] Morse, Raval and Wingender (n 61).
[86] Gatzlaff and McCullough (n 76).
[87] Gilles Hilary, Benjamin Segal and May H. Zhang, 'Cyber-Risk Disclosure: Who Cares?' (2016) SSRN Electronic Journal.

respect to particular types of breaches. Therefore, it appears, at least on the surface, that the contradictory findings about the effect of security breaches on stock market returns occur. Second, though this is so far missing from the literature, the costs and benefits of breaches should be compared to determine how much an organisation should spend on cybersecurity activities, such as preventing, detecting and resolving security breaches. Making judgments about investments in cybersecurity activities requires a thorough understanding of the true impacts of security breaches on the securities market returns of organisations, encompassing both the implicit and explicit costs of breaches.[88]

2.4. Regulation as the sole solution for mitigating influences

At present, there are three clear barriers to regulating cybersecurity in the financial sector. First, the field of cybersecurity seems resistive to codifying the relevant laws in a thorough multilateral binding convention. Second, governments have demonstrated a strong unwillingness to contribute to the creation of international customary laws related to the cybersphere. They have been hesitant to provide explicit expressions of opinion juris on issues linked to cybersecurity, and state conduct in this field is inherently cloaked in secrecy.[89]

While the first two relate to states' unwillingness to act in ways that are meaningful for the formation of new regulations, the third issue is states' actual behaviour in respect to cyber governance. To say that states have completely abandoned standard-setting would be untrue as there are mandatory or non-mandatory national cyber regulations to protect financial markets,[90] such as the General Data Protection Regulation (GDPR), Cybersecurity Disclosure Guidance by the SEC, the National Institute of Standards and Technology (NIST), the SOX, the Gramm–Leach–Bliley Act (GLBA) and the Office of the Superintendent of Financial Institutions (OSFI).

When the rise in cyber events, relating to the risks detailed in Section 2.1, caught the attention of both the state and federal governments, regulations were put in place by the State of New York in 2017 that mandate financial service businesses to create cybersecurity procedures and submit yearly certifications attesting their compliance.[91] According to Fischer, in 2014, there were 56

[88] Gordon, Loeb and Zhou (n 69).
[89] Kubo Mačák, 'Is the International Law of Cyber Security in Crisis?' (2016) 8th International Conference on Cyber Conflict (CyCon), IEEE 127–139.
[90] Ibid.
[91] New York 23 NYCRR 500 2017.

federal laws in the United States that dealt with cybersecurity,[92] and that figure will now only have increased. In May 2018, the first cybersecurity law in the European Union (EU) came into force, requiring a wide range of businesses to report any breaches they encounter. Following on from this, in the EU, further cybersecurity legislation is now in the works.[93]

When national governments' understanding of the risks of cyberattacks is promoted, their willingness to submit to internationally binding rules tends to improve. With reference to key developments in the past that were at first not well-understood, despite the dominant spacefaring governments' initial strong resistance, the domain of outer space eventually became subject to a binding legal regime. Moreover, the first worldwide nuclear safety rules were not implemented for almost three decades after the launch of the world's first nuclear power station in 1954 in Obninsk, Soviet Union (now Russia). In the interim, non-binding safety standards and criteria, the majority of which were produced by the International Atomic Energy Agency, served as guidance for governments (IAEA). Later, nuclear safety treaties unified this developing corpus of non-binding standards and made many of the pertinent requirements obligatory for all member states.[94]

A number of factors have delayed the expansion of cyber financial regulation. For instance, cybersecurity capabilities are heavily influenced by the market's size and segmentation. Smaller companies have historically trailed behind large corporations. In that context, the financial sector has not yet discovered an efficient method for achieving cyber financial regulation that will not place an unfair burden on smaller markets. In addition, sustaining the progress that giant corporations have made across the system remains a key problem.[95]

Moreover, though key players in different markets believe information exchange on risks and vulnerabilities to be highly beneficial, they are also compelled to work against government and industry cooperation in this area. Since market operations and reputations are tightly linked to the cyber infrastructure, knowledge of these systems and security lapses is linked to organisations' competitive advantage. Although the strength of this motivation to shirk cooperation has diminished over time as businesses have discovered that it is generally not in their best interests to

[92] Eric A. Fischer, 'Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation' (2014).
[93] Berkman and others (n 60).
[94] Mačák (n 89).
[95] Atkins and Lawson (n 7).

compete on cybersecurity, it does return and become especially intense after learning of a cyberattack.[96]

Furthermore, since the industry is extensively regulated, enterprises are hesitant to share information with the government regarding threats and vulnerabilities out of concern that it will result in audits or expose them to further liability. They are also anxious about how the information they contribute will actually be used in the context of an investigation, regulatory action or significant lawsuit.[97]

The need for a more adaptive regulatory model (i.e. a strategy designed to facilitate routine learning, self-correction and adaptability to changing conditions over time) is indicated by the cyberspace's constant change. Yet, most regulatory approaches design solutions that are only re-examined when failure results in large enough costs to warrant high-level attention. It might be challenging to regulate a landscape of adaptative change over time because regulation frequently results in stagnant checklists.[98]

Furthermore, even though CEOs are becoming more aware of the dangers of cyberattacks, many still see cybersecurity as primarily an IT issue, and only a small number of boards of directors believe that strategic investments in cybersecurity may produce business value and a competitive advantage.[99] For those who hold that belief, security spending encourages businesses to increase their investment because it gives them confidence they are safe from their rivals.[100] As a result, enterprises that invest in this way seem to be more competitive in the long run, because even if competitors eventually catch them up, the time lag is far greater than it would have been if they had not taken the measures to protect themselves.[101]

[96] Atkins and Lawson (n 7).
[97] Ibid.
[98] Ibid.
[99] Dejan Kosutic and Federico Pigni, 'Cybersecurity: Investing for Competitive Outcomes' (2020) 43 Journal of Business Strategy.
[100] Armando R. Gomes and others, 'Analyst Coverage Networks and Corporate Financial Policies' (2017) available at SSRN 2708935.
[101] Benn Lawson and Danny Samson, 'Developing Innovation Capability in Organisations: A Dynamic Capabilities Approach' (2001) 5 International Journal of Innovation Management; Donald Mitchell and Carol Coles, 'The Ultimate Competitive Advantage of Continuing Business Model Innovation' (2003) 24 Journal of Business Strategy.

Yeh and Chang recently claimed that the scope of the countermeasures many businesses adopt does not correspond to the seriousness of the perceived threats. To remedy this, they proposed that organisations should assess the possible loss of value brought on by a security breach using estimations, allowing them to invest in information security measures that are proportionate to the anticipated loss.[102]

If the goal is to try to avert every conceivable incident, then budgets will never be sufficient. While it may be necessary to invest more money, it is probably more important for businesses to invest with a focus on risk mitigation. Efforts should be made to identify the organisation's key assets and areas at risk and to model plausible attack scenarios. This supports appropriate decision-making on reasonable investments in the business's various divisions.[103]

Some believe that increased development of cybersecurity calls for expanded and deeper (more operation-level) public-private cooperation, enabling businesses to make use of a wider and more useful array of government resources and instruments. In the long term, it is proposed that successful cybersecurity will depend more on consistent improvement than it will on following a set of rules.[104]

3. Evaluating disclosure as a strategy to protect investors

The impacts of disclosure and its general desirability are rather equivocal in the academic literature. It is commonly known that disclosures can advance some of businesses' significant objectives, including lowering the cost of capital for businesses, raising market liquidity and efficiency and levelling the playing field in the financial markets. Destroying risk-sharing opportunities, encouraging the destabilising of beauty-contest incentives and crowding out private information generation are just a few of the further unintended effects of disclosure that have been extensively discussed in the literature. Recently, researchers have been delving deeper into the subject, to comprehend the benefits and drawbacks and provide answers to investors' important questions[105], including: what are the benefits of disclosure? How can the disclosures be effective? What is the best way to disclose information?

[102] Goel and Shawky (n 74).
[103] Emily Mossburg, John Gelinne and Hector Calzada, 'Beneath the Surface of a Cyberattack: A Deeper Look at Business Impacts' (2016).
[104] Atkins and Lawson (n 7).
[105] Itay Goldstein and Liyan Yang, 'Information Disclosure in Financial Markets' (2017) 9 Annual Review of Financial Economics.

This chapter will outline the background to the topic of disclosures, for a comprehensive understanding of the beginnings of disclosures and how they concern investors. The focus will be on the ways disclosures can be made and the associated processes, which affect the various impacts disclosures may have. Chapter 2 noted the responsibility investors have to mitigate losses, and this chapter will present insights from the person who is responsible if a disclosure goes wrong. Finally, the chapter will present the advantages of disclosures that boost investors' confidence, painting a comprehensive picture of the approaches to making such a disclosure and the negative effects that could result. Overall, this chapter supports the reader to build a nuanced, realistic picture of disclosures and the scenarios in which they are made.

3.1. Background to disclosures

The primary focus of regulatory efforts to support the stability and quality of the financial markets is on information disclosure. Since the adoption of the Securities Act of 1933 and the Securities Exchange Act of 1934, the United States federal government has aggressively regulated US equities markets, according to Greenstone, Oyer and Vissing-Jorgensen.[106] Its requirement placed on the disclosure of financial information is the focal point of these efforts. The SOX Act of 2002 and the Dodd-Frank Act of 2010 both strongly emphasised various areas of increased disclosure, standing as recent, visible markers of the efforts made to improve related regulation in recent years. The earlier of the two, the SOX Act, was created to 'protect investors by increasing the accuracy and dependability of corporate disclosures made pursuant to the securities laws, and for other objectives'.[107]

Following its enactment, a different branch of the federal government sought to advance security in the digital sphere in October 2011. The Division of Corporation Finance of the SEC released a staff document titled "Disclosure Guidance Topic No. 2—Cybersecurity", which set forth the SEC staff's views on public companies' obligations to disclose cybersecurity risks and cyberattacks, in response to pressure from the Senate Commerce Committee and a wave of widely publicised attacks on public companies. Companies registered with the SEC were already expected to disclose important information for the benefit of investors in their registration statements and periodic reports according to the Securities Acts of 1933 and 1934. Yet, for the first time, the Disclosure

[106] M. Greenstone, P. Oyer and A. Vissing-Jorgensen, 'Mandated Disclosure, Stock Returns, and the 1964 Securities Acts Amendments' (2006) 121 The Quarterly Journal of Economics.
[107] Goldstein and Yang (n 105).

Guidance established that the SEC regarded cybersecurity-related information as 'material' necessitating disclosure.[108]

Policymakers expressed a strong desire to evaluate the guideline soon after it was released, over two years ago. Sen. John D. (Jay) Rockefeller IV asked SEC Chairwoman Mary Jo White in a letter written in April 2013 to "elevate Disclosure Guidance and issue it at the Commission level", to "send a strong signal to the market that companies need to take their cybersecurity efforts seriously". He also expressed his gratitude for the effectiveness of the Disclosure Guidance. As discussed infra, Senator Rockefeller played a significant role in advocating for cyber disclosure guidance. Chairwoman White responded by stating that she would assess "existing disclosure processes and overall compliance with the guidance and recommendations... for additional action in this area".[109]

Despite objecting in writing to the SEC's interpretation of the relevant law or claiming that the information was not 'material' and not required to be disclosed, the registrants were forced to begin complying with the SEC's demands and now disclose more information about cyberattacks than they wish. Failure to comply with the Disclosure Guidance involves considerable risks because the SEC may take enforcement action against a corporation for failing to disclose material information, and shareholders may pursue a lawsuit for similar reasons.[110]

The SEC's guidelines have played a major role in the rise of cybersecurity disclosures on the global stock market landscape. A second SEC guideline on disclosing cybersecurity risks was released in 2018. After three years, in June and August 2021, the US Securities Commission issued firms the first penalties for lax disclosure controls and processes connected to cybersecurity risks.[111]

Disclosure in financial markets has three core objectives: (i) it protects investors, and thud, by enhancing their confidence in the market, preserves the good functioning (if not the very existence) of the (securities) market, thereby supporting its growth; (ii) it addresses the problems of agency concerning large corporations, providing transparency around how they are organised, financed and operating; (iii) it ensures that prices fully reflect all value-relevant information, to help

[108] Ferraro (n 25).
[109] Ferraro (n 25).
[110] Ibid.
[111] Ramírez and others (n 35).

financial markets in their fundamental function of efficiently allocating scarce financial resources across the economy.[112]

The fairness rationale has been almost universally discarded. Today, nobody seriously argues that protecting investors via disclosure is a proper policy simply because doing so is... just. Many, instead, and especially policymakers, contend that protecting investors is instrumental to the good functioning—if not the very existence—of the markets, warranting an efficiency justification. Providing investors with adequate protection increases their confidence in the markets. Alternatively, without a strong and widespread belief in market integrity, the investing public would withdraw its savings, with disastrous consequences for the entire economic system.[113]

Disclosure protects investors in three main ways: first, by providing them with all information reasonably needed to decide how to invest their savings, considering a security's risk and expected returns, the issuing entity, the attached rights and so forth. Thus, disclosure helps investors find the kind of investment that best matches their preferences, thereby minimising the risk of making poor investment decisions due to insufficient information regarding the securities purchased or sold.[114]

Second, disclosure may protect investors by enabling them not to be 'exploited' by traders with superior information, such as insiders and professional investors. According to this view, without disclosure, amateur investors would systematically lose out when trading against such informed counterparts, soon leading them to withdraw their money from the market. Disclosure is said to establish a "level playing field" between amateur and professional investors or corporate insiders, to give the former "equal access" to the same range of information on which the latter base their decisions.[115]

Third, disclosure protects investors by discouraging fraud, self-dealing and various other kinds of opportunistic behaviour on the part of managers and controllers. From this standpoint, the goal of investor protection aligns with improved corporate governance, which is addressed in the next section.[116]

[112] Luca Enriques and Sergio Gilotta, 'Disclosure and Financial Market Regulation' (2014) SSRN Electronic Journal.
[113] Ibid.
[114] Ibid.
[115] Enriques and Gilotta (n 112).
[116] Ibid.

Although, technically speaking, the SEC Disclosure Guidance relating to cybersecurity is not a binding mandate, citing the optional nature of disclosures will give a weak defence in the event of an investor lawsuit. In contrast to the SOX Act of 2002, which strongly emphasises computer-based information systems, and is, therefore, focused on cybersecurity inputs, the SEC Disclosure Guidance is concerned with cybersecurity outputs, namely cybersecurity risks and incidents.[117]

In their 2010 study, Gordon et al. evaluated voluntary disclosures of information on security and corresponding market valuations between 2000 and 2004 and discovered a strong correlation between the two. Yet, their sample period predated both the SEC's mandates for obligatory risk reporting, which took effect in 2005, and its supplemental guidelines on cybersecurity disclosures, effective from 2011.[118] Gordon et al. proposed that in the early period under study, organisations that voluntarily disclosed information about cybersecurity risks demonstrated a commitment to mitigating those risks and thus enjoyed higher market valuations.[119]

Cybersecurity risk disclosures' release and duration, between the attacks and disclosing, are positively correlated with the chance of the firm subsequently reporting cyber-security incidents, according to Li et al., but this correlation was only found before the SEC's 2011 cybersecurity Disclosure Guidance came into force. The researchers contended that because these disclosures forecast that cybersecurity incidents were at risk of occurring, disclosures were instructive during the pre-guidance period.[120]

However, in the post-guidance period, cyber disclosures are no longer indicative of cybersecurity incidents to follow, possibly as a result of a rise in the disclosures of inconsequential cybersecurity concerns. This trend casts doubt on how informative cyber disclosures are under the post-guidance system.[121] Alternatively, the informativeness observed by Gordon et al. may have persisted after the guidelines were introduced, albeit with a wider impact on market valuations, given the more general nature of cyber disclosures in recent times.[122]

[117] Gordon and others (n 8).
[118] Berkman and others (n 45).
[119] Gordon and others (n 8).
[120] Gordon, Loeb and Sohail (n 48); Berkman and others (n 60).
[121] Li, No and Wang (n 21).
[122] Gordon, Loeb and Sohail (n 48); Berkman and others (n 60).

Many cyber-related disclosures made in the post-guidance period have taken the form of 'boilerplate' statements that were ambiguous or unspecific,[123] and as such, were uninformative to the market and of little importance or value. Finding these reports has become more challenging, too, as a result of the SEC's unclear guidance on what constitutes a 'disclosure' of a cyber event, concern or risk.[124]

Nevertheless, senators, professionals and executives hailed the new SEC disclosure standards for cybersecurity as making a substantial change with far-reaching repercussions that had been pushed for by regulators. Senator John Rockefeller, for instance, described how "intellectual property worth billions of dollars has been stolen by cyber criminals, and investors have been kept completely in the dark. This guidance changes everything, it will allow the market to evaluate companies in part based on their ability to keep their networks secure. We want an informed market and informed consumers, and this is how we do it". Reading into this, the significant economic costs of cyberattacks appeared to be the primary driver of his interest.[125]

In the European capital market, the cybersecurity and privacy laws, which include the GDPR and the directive on network and information systems security (NIS), may be interpreted to require the disclosure of cyber events. The obligation to disclose data incidents from a cybersecurity law perspective could incentivise the board to include information on this topic in the firm's annual financial reports, according to Eijkelenboom and Nieuwesteeg, even though doing so is not specifically mandated.[126] Yet, the archiving methods for disclosures may require further regulation still to come if we are to implement consistent systems in practice.

3.2. Ways of making disclosures

According to the 2011 Cybersecurity Guidance, a registrant must provide disclosures that are specific to their individual situation: "Registrants should avoid disclosing risks that may apply to any issuer or any offering and should avoid presenting hazards that could apply to any issuer". That is to say, registrants should offer information customised to their specific circumstances and avoid a generic 'boilerplate' disclosure. In addition to reiterating this point, the guidance sets forward the level of disclosure that is appropriate.

[123] Hilary, Segal and Zhang (n 87).
[124] Berkman and others (n 60).
[125] Hilary, Segal and Zhang (n 87).
[126] Ramírez and others (n 35).

The federal securities laws do not compel a registrant to make disclosures that might jeopardise their cybersecurity. Instead, registrants should disclose enough so that investors can understand the types of risks that specific involved, without the disclosure having that potential negative effect.[127]

So, to prevent cybersecurity compromise through disclosure, concealment through generalisation was somewhat expected and advised against. However, since a registrant is allowed to consider the "adequacy of preventative activities" when determining the magnitude of a cybersecurity risk, it can be argued that only those who believe their own measures to be insufficient are ultimately required to submit risk information. Then, even a broad disclosure may signal to the hacker underground community that the company is weak. Additionally, it can suggest to the financial community, authorities and possible claimants in lawsuits that the company may not be adequately protecting its assets.[128]

It seems, as a result, that firms seeking to implement the advice face a difficult decision. Businesses that adhere to the recommendations will be acknowledging a risk that is specific to their industry and recognising that it is "among the most important elements that make an investment in the firm speculative or dangerous". The disclosure identifies a vulnerability that the business cannot sufficiently address through preventative measures. The recommendations state that appropriate disclosures should cover "discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences", and "the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks". From a security standpoint, it does not seem appropriate to provide comprehensive information on either of these objects. Of course, the guidance specifically disclaims that securities rules are not intended to compromise a firm's cybersecurity, but surely this scenario will only be prevented if the firm is taking proper precautions. The underlying issue is that details of cybersecurity risks are what both investors and hackers seek to learn.[129]

On the contrary, as long as it does not indicate a security issue, merely outlining generalised hazards that may apply to others in the same business seems relatively harmless. However, such a

[127] Morse, Raval and Wingender (n 50).
[128] Morse, Raval and Wingender (n 50).
[129] Morse, Raval and Wingender (n 50).

disclosure may also be largely ineffective, which is probably why the advice discourages firms from making one. Although a company might use such a disclosure to credibly convey to investors that the management takes cyber-risks seriously, that would involve going against the guidance to avoid releasing 'boilerplate' generic disclosures. For many businesses, remaining silent may be the best course of action, especially if they are taking the necessary procedures to address recognised threats and classing those threats as 'not material'.[130]

Congress passed laws that provided a basic framework for disclosure, leaving it up to the SEC to establish more specific regulations. Form 10-K has become the required format for yearly reporting. Furthermore, at the conclusion of each of the first three fiscal quarters of each year, quarterly reports are required on Form 10-Q. In addition, on Form 8-K, which is only filed when specific material events occur, the current reporting may be required or permitted to be included. Forms 10-K, 10-Q and 8-K serve as the cornerstone for periodic reporting by domestic registrants, providing a means to inform investors, even though many other forms may be utilised for registrants with other particular characteristics.[131] Disclosures may be required on several sections of the 10-K filings, including the Risk Factors, Management discussion and analysis (MD&A), Description of Business, Legal Proceedings and Financial Statement Disclosures (e.g. material prevention costs, or losses sustained) sections.[132]

Periodic reporting requirements place a heavy load on registrants. According to government estimates, each firm must spend an average of 1,998.78 hours annually complying with Form 10-K. Form 8-K, only filed when specific material events occur, takes an average of 5.71 hours per response, and Form 10-Q, which must be filed three times annually, requires 187.43 hours per response on average.[133]

To add to those, the SEC created Regulation S-K, an integrated framework for disclosures detailing both registration and ongoing reporting responsibilities, as a result of worries about efficiency, effectiveness and compliance difficulties. The SEC staff finished compiling the Regulation S-K disclosure requirements in December 2013 and it has since been in effect.[134] Yet, although it

[130] Morse, Raval and Wingender (n 61).
[131] Ibid.
[132] Hilary, Segal and Zhang (n 87).
[133] Morse, Raval and Wingender (n 61).
[134] Morse, Raval and Wingender (n 61).

mandates that corporations must report all significant risks, the guidance does not specifically address the disclosure of cyber-risks, threats or attacks.[135]

Regardless of the forms and regulations now in place, managers remain strategic in their disclosure behaviour.[136] When it comes to specific cyber hazards, firms may become more vulnerable to assaults if they disclose too much or too precise information about them.[137] However, higher disclosure may also lower the likelihood that a breach will result in a lawsuit.[138] To walk the line between the two, the management may simply mention weak points in general terms when evaluating the company's material concerns.[139]

By using 'boilerplate' language that does not truly provide specific details, managers may, for instance, avoid disclosing confidential information about risks[140], or they may concentrate the conversation on significant concerns that the company is currently addressing. Accordingly, Gordon et al. speculated that an increase in cybersecurity spending will go hand in hand with the increased reporting of cybersecurity-related activities as a result of the SEC's 2011 guidance.[141] Such a trend reflects businesses concentrating the discussion on favourable aspects of cybersecurity. In this way, cyber-related disclosures become linked to the firms' cybersecurity awareness, given the significant dangers connected with disclosing vulnerabilities.[142]

Businesses must include, under Item 1A of Form 10-K, "the most significant characteristics that make the offering speculative or risky", according to the SEC. This is required to "present investors with a clear and succinct explanation of the material risks to an investment in the issuer's securities". Yet, since companies are only obligated to offer qualitative descriptions and not to quantify the likelihood or impact of the disclosed risks, they have a great deal of discretion over what information to reveal and how to present it. Since managers frequently report risks using

[135] Berkman and others (n 60).
[136] Ronald A. Dye, 'Disclosure of Nonproprietary Information' (1985) 23 Journal of Accounting Research; Robert S. DeWoskin, 'Information Resources on Quality Available on the Internet' (2003) 10 Quality Assurance.
[137] Jonathan L. Rogers and Andrew Van Buskirk, 'Shareholder Litigation and Changes in Disclosure Behavior' (2009) 47 Journal of Accounting and Economics.
[138] Gordon, Loeb and Sohail (n 48).
[139] Berkman and others (n 60).
[140] Ronald A. Dye, 'Disclosure "Bunching"' (2010) 48 Journal of Accounting Research.
[141] Gordon and others (n 8).
[142] Berkman and others (n 60).

imprecise words and list all the uncertainties they encounter, to disguise those of importance, practitioners criticise managers for giving investors little information.[143]

In a similar vein, Robbins and Rothenberg proposed that risk factor disclosures are the least expensive type of insurance, especially when deliberately completed incorrectly, since when the contents of completed forms are later pulled up in court, "firms that cannot point to such a risk factor when faced with a lawsuit" will come under legal protection. This implies that companies have an incentive to make unhelpful disclosures of risk factors. The SEC sent out comment letters as soon as they became aware of the matter, asking businesses for more risk information and urging them to "avoid risk factor disclosure that may apply to any issuer or any offering".[144]

Updates on risk factors have been the subject of several recent research studies. According to Filzen, companies that included risk factor updates in their quarterly reports had lower anomalous returns near the filing dates, fewer future unexpected earnings and a higher possibility of experiencing a future negative earnings shock.[145] Similarly, a second study by Filzen et al. showed that quarterly risk factor updates were negatively connected with future returns and that the association was larger for firms employing more direct language relating to firm fundamentals.[146]

Furthermore, ex-post disclosures of data security breaches highly correlate with downward stock price movements, according to prior studies, and these correlations can last for lengthy periods. A breach disclosure most typically signifies fresh information reaching the market that could negatively impact the firm's financial outlook. Loss of investor trust in the management's capacity to protect the company's assets, as well as exposure to transaction costs associated with resolving claims, may detrimentally impact stock values.[147]

Gaulin highlighted the significance of reporting individual risk factors, demonstrating that managers add new risk factors and delete stale risk factors in a timely fashion, and such activities predict future economic changes even after controlling for the ex-ante risk and company performance.[148] Furthermore, corporations respond to SEC comment letters by increasing the

[143] Li, No and Wang (n 21).
[144] SEC Disclosure Regulation 2010; Li, No and Wang (n 21).
[145] Joshua J. Filzen, 'The Information Content of Risk Factor Disclosures in Quarterly Reports' (2015) 29 Accounting Horizons.
[146] Li, No and Wang (n 21).
[147] Morse, Raval and Wingender (n 61).
[148] Maclean Peter Gaulin, *Risk Fact or Fiction: The Information Content of Risk Factor Disclosures* (2017).

clarity of their reportage, whereas they respond to securities lawsuits by increasing the number of risks they identify without increasing the definitiveness of their disclosures.[149]

The SEC has utilised comment letters to compel disclosures of cybersecurity risks, even though the guidance specifically states that it is not a judgement. For instance, the SEC wrote in a comment letter addressing Freeport-McMoRan Copper & Gold Inc.'s 2011 annual report: "We note that none of your risk factors, or other sections of your Form 10-K, specifically address any risks you may face from cyberattacks, such as attempts by third parties to gain access to your systems to compromise sensitive business information, to interrupt your systems or otherwise try to cause harm to your business and operations. In future filings, beginning with your next Form 10-Q, please provide risk factor disclosure describing the cybersecurity risks that you face or tell us why you believe such disclosure is unnecessary". One could contend that the disclosure recommendation is evolving into a disclosure requirement because the SEC's comment letters are frequently seen as de facto judgements.[150]

Media stories on information security breaches, or what we refer to as "breach announcements", are a key source of information for investors. Breach notifications are often published on blogs, large media sites, etc. Investors' views on the impact of the breach may differ depending on the vocabulary used and other aspects of the individual media reporting. For instance, some publications might employ more precise phrases, whilst other articles may use ambiguous language instead, prompting varied responses from investors.

Additionally, different information security events may have different repercussions for the impacted company. Information security incidents are frequently categorised as those that compromise information availability, integrity or confidentiality. Depending on the type of information affected and the legal jurisdiction of the parties involved, availability-type incidents or attacks may most likely result in temporary income losses for a company, whereas confidentiality-type incidents often lead to legal action.[151]

[149] Li, No and Wang (n 21).
[150] Gerry H. Grant and Grant C. Terry, 'SEC Cybersecurity Disclosure Guidance is Quickly Becoming a Requirement' (2014) 84 The CPA Journal.
[151] Tawei Wang, Jackie Rees Ulmer and Karthik Kannan, 'The Textual Contents of Media Reports of Information Security Breaches and Profitable Short-Term Investment Opportunities' (2013) 23 Journal of Organizational Computing and Electronic Commerce.

Early studies on the motivations for disclosure found that full disclosure occurs when there is no cost to disclosing information because investors believe that firms that never make disclosures have the worst prospects.[152] However, businesses only share information when the advantages outweigh the costs and it is inexpensive to do so. Alternatively, transparency may be utilised to lower ex-post reputational and legal costs resulting from negative news or a company's underwhelming financial results.[153] Certain such disclosures are required by SOX, while others are left to the discretion of the individual firm.[154]

The language style (tone) was the main topic of research by Davis et al., who demonstrated how the stock market can respond to various linguistic styles. According to Balakrishnan et al., news pieces can be classified as press- or firm-initiated, with firm-initiated media prompting significantly worse market reactions than press-initiated media.[155] According to Tetlock et al., when estimating a firm's fundamentals, the textual material in news items provides qualitative information. Loughran and McDonald expanded on Tetlock et al.'s findings and demonstrated how an alternative negative word list might accurately represent the tone of financial material.[156] According to further research by Kothari et al. into news reports, analyst reports and annual reports, the volatility of the stock price is lower when the information is reported more favourably.[157]

In response to the SEC's 2011 Cybersecurity Guidance, businesses appear to have reacted carefully. Although cybersecurity threats are ubiquitous across a wide range of industries, only a tiny proportion of the organisations potentially impacted by these risks appear to have made affirmative risk factor disclosures in response to the guidelines. Although not all businesses opt to include the phrase "cybersecurity" in their disclosures, its use is growing. Looking ahead, as this

[152] Sanford J. Grossman, 'The Informational Role of Warranties and Private Disclosure about Product Quality' (1981) 24 the Journal of Law and Economics.
[153] Douglas J. Skinner, 'Why Firms Voluntarily Disclose Bad News' (1994) 32 Journal of Accounting Research.
[154] Wang, Ulmer and Kannan (n 151).
[155] Balakrishnan, Karthik, Anindya Ghose and Panos Ipeirotis, 'the Impact of Information Disclosure on Stock Market Returns: The Sarbanes-Oxley Act and the Role of Media as an Information Intermediary' (2008) WEIS.
[156] Tim Loughran and Bill McDonald, 'When Is a Liability Not a Liability? Textual Analysis, Dictionaries, and 10-Ks' (2011) 66 the Journal of Finance.
[157] S. P. Kothari, Xu Li and James E. Short, 'The Effect of Disclosures by Management, Analysts, and Business Press on Cost of Capital, Return Volatility, and Analyst Forecasts: A Study using Content Analysis' (2009) 84 The Accounting Review.

phrase comes to be used more consistently by the management and their professional advisers, it is anticipated that this expansion in its inclusion in reportage will continue.[158]

Yet, contrary to the idea that progress is being made, the empirical evidence suggests otherwise. Investors have been noted to penalise companies that include a new disclosure for cybersecurity and related risks, in response to the Cybersecurity Guidance, on the annual Form 10-K. This negative market response indicates that, at least from the firm's perspective, caution may remain the best course of action. Although some businesses may believe disclosures will be beneficial for showing that the management is aware of cybersecurity issues, the market reaction implies that investors instead receive a different, warning signal.[159]

Businesses have the option to both comply with the Cybersecurity Guidance and opt to refrain from adding a new disclosure item because the guidance does not contain any new regulations demanding further disclosures be made. Securities regulators rarely interpret this quiet as an actionable statement, and those who chose to remain silent and make no further disclosures may infer that their cybersecurity activities are sufficient to manage the threats in their environment. Unfortunately, those who add cybersecurity risk factor disclosures may find that their message is misunderstood by the market, which typically results in a decline in the stock price as a result of more firm-specific risk being signalled. Silence is indeed golden, as it is said.[160]

Yet, the SEC seems to think more needs to be done. Back in 2014, Commissioner Luis A. Aguilar stated that “there is no doubt that the SEC must play a role in this area. What is less clear is what that role should be”. In a recent move, the agency censured RT Jones Capital Equities, a local investment firm, after a cyberattack revealed information concerning 100,000 brokerage clients. The SEC also unveiled a plan to assess how US-registered investment advisers and broker-dealers fare in terms of cybersecurity.[161] These two moves represent efforts on the part of the SEC to improve the current approaches to making disclosures.

3.3. Impact of disclosing incorrectly (Rule 10b-5)

The company and the officers and directors in charge of its disclosures may be held liable for mistakes in and omissions from company disclosures. Failure to adequately oversee operations,

[158] Morse, Raval and Wingender (n 61).
[159] Ibid.
[160] Ibid.
[161] Morse, Raval and Wingender (n 61).

and thus safeguard the firm's assets, exposes corporate directors to liability risk (in contrast to those directors who take responsibility for investors' losses, as covered in Chapter 2 Section 2).

Federal securities regulations do not mandate that registered companies disclose every significant fact that shareholders might be interested in learning about. Liability for failure to disclose can, nevertheless, be determined under section 10(b) of the Exchange Act, which makes it unlawful to "use or employ, in connection with the purchase or sale of any security... any manipulative or deceptive device or contrivance in contravention of SEC rules and regulations". Rule 10b-5, which implements this provision, then states: "It shall be unlawful for any person... to make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading... in connection with the purchase or sale of any security".[162]

To prevent claims from misleading investors, the legislation specifically targets false statements of a material fact, as well as information that should not be omitted. To break Rule 10b-5, such unlawful assertions or omissions must be made. Courts have recognised an implied private right of action to enforce rule 10b-5, which has become the primary basis for damages paid in settlements and judgements as a consequence of private actions involving federal securities laws. Corporate directors are thus exposed to liability risk if they do not properly oversee operations and protect assets.[163]

Investor damages that may not otherwise be actionable under federal securities laws may instead be remedied otherwise under state law. A shareholder derivative claim, rather than a securities class action, may be utilised to seek compensation for damages brought on by a board of directors' conduct or inaction when this results in a violation of fiduciary duty. Yet, the standard for responsibility in this sector is high, making it challenging for shareholders to hold directors accountable for losses, as was shown previously in Chapter 2.[164]

3.4. Benefits of disclosure

Various estimates of market responses to publicly disclosed attacks can be found. When businesses immediately announced a cyberattack, their stock prices typically fell 0.33 per cent in the first

[162] Ibid.
[163] Morse, Raval and Wingender (n 61).
[164] Ibid.

three days and 0.72 per cent in the following month. In contrast, when companies concealed an assault and third parties later learned about it, market values fell by a substantially greater amount—1.47 per cent in the three days following the attack's discovery and 3.56 per cent in the month that followed.[165]

Companies often suppress information about more dangerous attacks, while they disclose information about less dangerous ones. Withholding firms have been noted to have poorer analyst coverage, weaker corporate governance and lower litigation risk than disclosing firms. They have a low likelihood of discovery since investors pay closer attention to companies with greater analyst coverage. Yet, such companies receiving investors' attention may have stronger corporate governance, meaning they are less likely to keep bad news from investors, so there is no withheld information to uncover. For these firms, the high legal risk of withholding information, and the anticipated loss associated with that, make disclosures an attractive alternative.[166]

Home Depot announced in a statement that their credit card systems had been compromised on 8 September 2014. In a several months-long security incident, the corporation went on to lose 56 million customers' credit card details. On 6 November, the business disclosed that the compromise was more serious than it had initially believed. Ultimately, 53 million customers' email addresses were also stolen, according to Home Depot. A slight, temporary decline in the stock price was caused by the original statement, but nothing more.[167]

In a statement made available to the public on 4 February 2015, Anthem acknowledged that nefarious hackers may have accessed its servers and seized control of 37.5 million records including personally identifiable information. On 24 February 2015, Anthem increased the total to 78.8 million people whose personal information had been exposed. As a result of the announcements, the firm's stock price briefly and slightly decreased.[168]

Only one of the five most prominent cyber-breaches in recent years, which received widespread public attention, seems to have had a major effect on the associated company's stock price, and this effect was still only temporary, with the stock price later recovering. It seems, at least for

[165] Amir, Levi and Livne (n 39).
[166] Amir, Levi and Livne (n 39).
[167] Hilary, Segal and Zhang (n 87).
[168] Ibid.

corporate giants such as Anthem and Home Depot, that a cyber-breach must have a huge economic impact before it affects their stock price in any meaningful way.[169]

Some scholars propose that despite the best efforts of various actors including the SEC, not all market cyber-dangers will be addressed. Appropriate disclosure remains crucial, but this is a sobering truth. The SEC itself has been the target of a number of successful malicious assaults and intrusion attempts that are ongoing, showing that these can be developed and directed at even the most reliable organisations. Market participants now regularly suffer high remediation costs, as well as regulatory, litigation and reputational issues, as a result of cyber events. Investors, customers and other significant stakeholders ultimately bear many of the expenses associated with these risks, including the costs of mitigation.[170]

It is not all doom and gloom, however. An organisation can let the market know that it is actively working to avoid, detect and fix security breaches by voluntarily disclosing cybersecurity issues in its annual report. The net present value (NPV) of a company, and consequently, the value of its stock on the market, should both rise as a result of these signals. For instance, by reducing the uncertainty around conducting business online linked to cybersecurity concerns, these signals may boost consumers' willingness to engage in e-commerce. The predicted net cash flows of a company, as well as the company's NPV and market value, should rise as consumer confidence to conduct e-commerce with the company increases.[171]

Due to the reduction in liability brought on by the enhanced openness linked with disclosures, voluntary disclosures relating to cybersecurity may also help to reduce possible lawsuit expenses.[172] Additionally, financially minded computer hackers who seek monetary rewards for their efforts may be reluctant to invest resources in attacking systems where there is a reduced likelihood of success and a higher cost. In either of these two scenarios, a company should retain more of its cash flows thanks to its voluntary disclosures relating to cybersecurity, which will raise the firm's NPV and market value.[173]

[169] Ibid.
[170] Jay Clayton, 'Statement on Cybersecurity' (VitalLaw, 20 September 2017) <http://business.cch.com/srd/SEC_3.pdf> accessed.
[171] Gordon, Loeb and Sohail (n 48).
[172] Ron Kasznik and Baruch Lev, 'To Warn or Not To Warn: Management Disclosures in the Face of an Earnings Surprise' (1995) 113–134.
[173] Gordon, Loeb and Sohail (n 48).

Ultimately, by eliminating knowledge asymmetry between a firm's management and its investors, as well as among its investors, voluntary disclosures about a firm's cybersecurity may lower the firm's cost of capital.[174] Since the rate used to discount anticipated future cash flows will be lower (as it is dependent on the firm's cost of capital), a firm's NPV, and consequently, its market value will rise under this lower cost of capital scenario. If companies with chances to generate high returns cannot distinguish themselves from businesses with only opportunities to generate low returns, investors will support both at the same level, which is that associated with low returns. To indicate to the market their high return potential, organisations can create large profits by voluntarily disclosing information on their strong cybersecurity measures. Since at least one company has already benefited from voluntary disclosures about cybersecurity, other companies undoubtedly can as well.[175]

In essence, managers must strategically decide whether or not voluntary disclosures about cybersecurity will benefit their company in terms of its market value. Managers may be aware of the need for them to make this decision given the obvious trend toward greater voluntary disclosures related to cybersecurity. However, nobody has yet conducted an empirical analysis to determine whether or not choices regarding voluntary disclosures have the desired effect of raising firms' value.[176]

4. Conclusion

A robust cybersecurity regulatory framework and financial commitment ensure the safety and stability of the securities market. This dissertation determined how cybersecurity laws affected investor confidence in the banking industry. The relevant parts of SOX, GDPR and the SEC's financial regulation's cyber rules were included within the scope of the analysis. For cybersecurity plans to be successful, according to the findings presented in this dissertation, they must be built around adaptable regulations that consider the nature of the Internet while also increasing investment in the sector.

The importance of this research is indicated by the common acknowledgement that poor cybersecurity in financial markets around the world has a significant influence in the failure of

[174] Paul M. Healy and Krishna G. Palepu, 'Information Asymmetry, Corporate Disclosure, and the Capital Markets: A Review of the Empirical Disclosure Literature' (2001) 31 Journal of Accounting and Economics.
[175] Gordon, Loeb and Sohail (n 48).
[176] Ibid.

many securities prices and the decline in investor confidence. Despite the importance of cyber threats to financial markets, this sector received little attention. This dissertation demonstrated that a framework for cyber regulation and investments prioritising risk avoidance significantly contributes to national institutions' underappreciation of cyber challenges. Following the financial cyber incidents, a flurry of regulatory legislation aimed at preventing attacks was implemented. These measures primarily involved exposing previous attacks to safeguard investors and provide them with an opportunity to make a choice. Some now think that the regulation is insufficient because of several significant cyberattacks in recent years. Increasing investment in cybersecurity might be a viable approach to reducing these risks.

4.1. Content

This dissertation explored the role that cybersecurity protection plays in boosting investor confidence in the securities markets. Because the US offers a unique impact on the world and sets the bar for financial regulation for many countries, the US approaches are highlighted. As Chapter 2 showed, the risks in cyberspace are detrimental to financial markets, including much discussion on who should oversee protecting investors' interests. As a result, investors tend to be powerless to hold a particular person or organisation accountable if they lose their assets due to cyberattacks. For the security preparation projects to protect investors, which top executives must direct, every organisation member is expected to share joint ownership, responsibility, and accountability. However, the amount of regulatory attention given to the financial sector has diminished because cyberattacks have impacted financial rules. The continuing cyberattacks provided convincing evidence that legislation may be ineffective in protecting the securities markets compared to robust cyber investment efficacy.

To demonstrate the applicability of the disclosure strategy from actual regulation, in particular, the SEC, SOX, and Dodd-Frank Act, Chapter 3 reviewed available facts. The case studies presented suggested how disclosures minimise cyber risk in securities markets. The impact of disclosure on the environment of the financial industry was featured in Chapter 3, especially with markets that avoid disclosing because they do not want to reveal their status to the government, which could result in undesired remediation efforts. Also, the decision to disclose could be detrimental to share prices, which has important implications for the position of disclosure as a guideline to the markets. Finally, the chapter detailed the disclosure process and demonstrated that the defendant is charged

under regulation 10b-5, exposing company directors to liability risk if they fail to supervise activities and safeguard assets adequately.

4.2. Key findings

The following summarises the findings of the examination of cybersecurity regulation. Since the Cold War, cyberattacks evolved to be more sophisticated and intense, with financial infrastructure being a notable target. These incidents are increasingly common in this sector because most products rely on digital technology than on physical goods or paper money. Even though markets prioritise maximising investors' value, few studies consider the effects of investor data breaches on valuation. Evaluations of the market show that investments in cybersecurity have received only minimal attention. Also, many markets typically disregard the cost analyses of these situations, and the significant economic harm they can inflict is either disregarded or excluded from the standard definitions of cyberattacks. Another common adverse impact of regulation is the stagnation of checklists.

Investors are kept in the dark about the most harmful attacks, while managers only disclose information about less severe attacks. Furthermore, choices made by the corporate board to use personnel or technological solutions to address cybersecurity issues are likely to be safeguarded from liability claims lawsuits. Therefore, if the directors can demonstrate they behaved honestly, then accusations that they failed to monitor or exercise supervision over cybersecurity concerns are unlikely to succeed. Yet, markets are forced to work against information exchange on the risks and vulnerabilities even when they consider it beneficial because understanding these actions and security flaws is related to an organisation's competitive advantage. Also, markets are apprehensive about disclosing information about threats and vulnerabilities to the government for fear of being held further liable.

Multiple studies showed a connection between falling stock prices and unfavourable cybersecurity incidents. So, a data leak involving investors is likely to have one of two effects on the securities market. First, the market might react negatively to hearing about the breach, demonstrating that it is aware of the clear repercussions of breaches. Second, the news of a data breach may not cause the financial market to react significantly. Instead, the effect could be felt long-term or deeply, or the market is not disclosed. Moreover, most significant marketplaces have insurance to cover a portion of their cyber risk.

By assisting investors in selecting the investment type that most closely matches their preferences, disclosure lowers the risk of making "wrong" investment decisions, provides them with the ability to avoid being "exploited" by traders with better information and deters fraud. Even though these statements tend to be boilerplate comments that may be vague or unspecific, cyber disclosures made in the post-guidance era are uninformative to the market and less significant for valuation. Therefore, using boilerplate language does not offer more insight.

Studies showed that ex-post disclosures of data security breaches are highly correlated with declining stock price movements, and these relationships can last for an extended time. The decline in investor confidence in management's ability to safeguard the company's assets and exposure to the transaction costs related to resolving claims may negatively affect stock prices. Also, while the disclosure guidance explicitly indicates that it is not a judgement, the SEC has leveraged comment letters to compel cybersecurity risk disclosures.

Corporate directors are exposed to being held liable if they fail to follow section 10(b) of the Exchange Act's requirements for asset protection and disclosure operations oversight. Resulting from individual lawsuits involving securities regulations, this rule emerged as the primary basis for damages awarded in settlements and court rulings.

Unfortunately, those who include cybersecurity risk factor disclosures discover that their message is often misconstrued by the market, which results in decreased stock prices from other firm-specific risks being signalled. A common practice is keeping quiet when in doubt, so most markets may potentially comply with the Cybersecurity Guidance by choosing not to introduce a new disclosure item. The SEC appears to believe that more work needs to be done, so attempts to enhance the disclosure method are in progress.

However, with voluntary disclosure of cybersecurity situations, increasing the value of stocks on the market and lower litigation costs may be possible. Such a decision should be made by the managers. However, no empirical investigation has yet to be performed to ascertain if decisions regarding voluntary disclosures result in the desired effect of increasing market value.

4.3. Discussion

This investigation revealed a shortage of previous studies on the effects of investor data breaches. Valuation may be the first step markets need to take to comprehend the true impact of a cyberattack on investors' confidence. Because regulators seem to have recognised the impact of cyberattacks

on financial markets, these issues are now being addressed, which marks a significant turn in regulators' approach to developing current regulations. While considering why markets do not share their cyber data with researchers may be acceptable, structural adjustments to the sector create additional defences against a build-up of cyber risk.

The financial sector is complex and opaque due to the sector's dynamic nature, particularly in technological breakthroughs. This thesis illustrated how national efforts are progressing to organise cybersecurity within financial markets. However, global regulation or a clear strategy agreeable across all markets is required due to the way markets function and how they are interconnected globally to prevent an attack that would split the consequences among them.

In relation to investors and markets, managers may also be held to conflicting obligations, as they must consider their respective interests to avoid conflicts. For them, the market's stability comes first, and in some circumstances, investors' interests come second. Therefore, they should accept responsibility for their actions if they have affected investors' conditions while not discounting their good faith actions.

This dissertation demonstrated the significance of the cybersecurity concept in the financial market industry and the potential need for field expansion in the context of concept research. Attention was provided to how significant the impact cyberattacks may have that resemble an armed assault. The analysis demonstrated that when the concept expands, the need to safeguard investors and markets may receive more focus and serious consideration because investors would be regarded as citizens with markets perceived as public spaces.

The analysis of the dissertation also demonstrated that regulation must be replaced because it leads to stagnant checklists. On the other hand, markets can be encouraged to increase investment in cybersecurity for financial markets because it gives investors confidence that they are secure from competitors and attacks. Specifically, when the cybersecurity scale is advanced in the securities market, attacks may not be able to catch up. Therefore, continuous improvement instead of adhering to standards can be more important for cybersecurity success.

Given the widely acknowledged concerns about disclosure, a thorough re-examination of its effectiveness is necessary. There is no benefit to the common, unclear and shallow methods of disclosure, which do not provide usefulness to investors in making decisions, as is evident from the varied opinions presented in this research.

Future research must consider the practical ramifications of transparency to guarantee that such discoveries are advantageous. This dissertation supports this goal by describing the advantages and disadvantages of disclosure.

A successful plan must be devised to fulfil the disclosure's goals of maximising market and investor returns. Also, successful disclosures occurred before the 2011 financial markets rules. Therefore, determining how disclosure generates acceptable outcomes and benefits is crucial, accomplished through empirical market research and considering other perspectives to create a just and efficient balance in the market. Even if disclosure decreases stock values, the effect cannot be prevented because prices could eventually fall even if the disclosure is not made because information could eventually be discovered. The disclosure must be provided in a reasonable manner that is determined by the Securities Commission or other party based on solid foundations.

Finally, this dissertation demonstrated that the SEC left a systemic gap by failing to identify the party accountable for an incorrect disclosure. To improve our comprehension of the processes involved in cyberattacks on the securities markets, a more interdisciplinary study is required to identify the culprit, making it possible for disclosure to be viewed in a more nuanced and realistic light. Specifically, the investor could feel confident in regaining their right or holding those accountable for failing to uphold it accountable. Ultimately, in accordance with the SEC's policy of compulsion, it must modify or clarify the status of its regulations, even if they are not enforceable in the financial markets. In other words, the commission must be precise in its directions and avoid ambiguity, regardless if the phrasing indicates mandatory action.

5. Acknowledgements

Many thanks go to my supervisor, Dr Catherine Coleman, for her guidance on this project. I am also grateful to my family for their continuing support. Without them, this study would not be possible.

6. Table of Legislation

Sarbanes-Oxley Act 2002

Dodd-Frank Wall Street Reform and Consumer Protection Act

New York 23 NYCRR 500

SEC Disclosure Regulation 2010

Securities and Exchange Act: Rule 10b-5 1934

7. Bibliography

Amir E, S Levi and T Livne, (2018). 'Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets' 23 Review of Accounting Studies.

Andoh-Baidoo F, K Amoako-Gyampah and K Osei-Bryson, (2010). 'How Internet Security Breaches Harm Market Value' 8 IEEE Security & Privacy Magazine.

Arner D W, J Barberis and R P Buckey, (2016). 'FinTech, RegTech, and the reconceptualisation of financial regulation', Nw. J. Int'l L. & Bus. 37: 371.

Atkins S and C Lawson, (2021). 'Cooperation Amidst Competition: Cybersecurity Partnership In The US Financial Services Sector' 7 Journal of Cybersecurity.

Balakrishnan K, Ghose A and Ipeirotis P, (2008). 'the Impact of Information Disclosure on Stock Market Returns: The Sarbanes-Oxley Act and the Role of Media as an Information Intermediary' WEIS.

Berkman H and others, (2018). 'Cybersecurity Risk Mitigation, Private Information Leakage and Earnings Announcements' (SSRN Electronic Journal, 1st December 2018) <https://www.researchgate.net/profile/Jonathan-Jona/publication/325752038_Cybersecurity_Awareness_and_the_Cost_of_Liquidity/links/5d726f0b92851cacdb23ff46/Cybersecurity-Awareness-and-the-Cost-of-Liquidity.pdf> accessed.

Berkman H and others, (2018). 'Cybersecurity Awareness and Market Valuations' 37 Journal of Accounting and Public Policy.

Bosworth S and M Kabay (eds.) (2002). *Computer security handbook*.

Callen-Naviglia J and James J. (2018). 'FinTech, RegTech and the Importance of Cybersecurity' Issues in Information Systems.

Campbell K and others, (2003). 'The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market' 11 Journal of Computer Security.

Cavusoglu H, B Mishra and S Raghunathan, (2004). 'the Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms And Internet Security Developers' 9 International Journal of Electronic Commerce.

Cavusoglu H, H Cavusoglu and S Raghunathan, (2004). 'Economics Of IT Security Management: Four Improvements To Current Security Practices' 14 Communications of the Association for Information Systems.

Chai S, M Kim and H Rao, (2011). 'Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior' 50 Decision Support Systems.

Chatterjee D, (2019). 'Should Executives Go To Jail Over Cybersecurity Breaches?' 29 Journal of Organizational Computing and Electronic Commerce.

Chatterjee P K, (2018). 'City Hosts a Highly-Heralded Cyber Security Event' Free Press Journal.

Clayton J, (2017). 'Statement on cybersecurity' (VitalLaw, 20 September 2017) <http://business.cch.com/srd/SEC_3.pdf> accessed.

Dahlgren S J, (2015). 'The importance of addressing cybersecurity risks in the financial sector' no.160.

DeWoskin R, (2003). 'Information Resources on Quality Available on the Internet' 10 Quality Assurance.

Dye R, (2010). 'Disclosure "Bunching"' 48 Journal of Accounting Research.

Dye R, (1985). 'Disclosure of Nonproprietary Information' 23 Journal of Accounting Research.

Enriques L and S Gilotta, (2014). 'Disclosure and Financial Market Regulation' SSRN Electronic Journal.

Ettredge M and V Richardson, (2003). 'Information Transfer among Internet Firms: The Case of Hacker Attacks' 17 Journal of Information Systems.

Ferraro M, (2013). 'Groundbreaking' or Broken? An Analysis of SEC Cyber-Security Disclosure Guidance, Its Effectiveness, and Implications' SSRN Electronic Journal.

Filzen J, (2015). 'The Information Content Of Risk Factor Disclosures in Quarterly Reports' 29 Accounting Horizons.

Fischer E, (2014). 'Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation'

Garg A, J Curtis, and H Halper, (2003). 'The Financial Impact Of IT Security Breaches: What Do Investors Think?' 12 Information Systems Security.

Gatzlaff K and K McCullough, (2010). 'The Effect of Data Breaches On Shareholder Wealth' 13 Risk Management and Insurance Review.

Gaulin M, (2017). *Risk Fact or Fiction: The Information Content of Risk Factor Disclosures* (Rice University 2017).

Gervais M, (2012). 'Cyber Attacks and the Laws of War' Journal of Law & Cyber Warfare 1.

Goel S and H Shawky, (2009). 'Estimating the Market Impact Of Security Breach Announcements on Firm Values' 46 Information & Management.

Goldsmith J, (2007). 'Who Controls the Internet? Illusions of a Borderless World' 23 Strategic Direction.

Goldstein I and L Yang, (2017). 'Information Disclosure in Financial Markets' 9 Annual Review of Financial Economics.

Gomes A R and others, (2017). 'Analyst coverage networks and corporate financial policies' Available at SSRN 2708935.

Gordon L and others, (2015). 'Increasing Cybersecurity Investments in Private Sector Firms' Journal of Cybersecurity.

Gordon L, Loeb M and Sohail T, (2010). 'Market Value of Voluntary Disclosures Concerning Information Security' 34 MIS Quarterly.

Gordon L, M Loeb and L Zhou, (2011). 'the Impact of Information Security Breaches: Has There Been A Downward Shift In Costs?' 19 Journal of Computer Security.

Grant G and T Grant, (2014). 'SEC cybersecurity disclosure guidance is quickly becoming a requirement' The CPA Journal 84, no. 5.

Greenstone M, P Oyer and A Vissing-Jorgensen, (2006). 'Mandated Disclosure, Stock Returns, and the 1964 Securities Acts Amendments' 121 the Quarterly Journal of Economics.

Grossman S, (1981). 'The Informational Role of Warranties and Private Disclosure about Product Quality' 24 the Journal of Law and Economics.

Healy P and K Palepu, (2001). 'Information Asymmetry, Corporate Disclosure, and the Capital Markets: A Review of the Empirical Disclosure Literature' 31 Journal of Accounting and Economics.

Higgs J and others, (2016). 'The Relationship Between Board-Level Technology Committees And Reported Security Breaches' 30 Journal of Information Systems.

Hilary G, B Segal and M Zhang, (2016). 'Cyber-Risk Disclosure: Who Cares?' SSRN Electronic Journal.

Hinz O and others, (2015). 'The Influence of Data Theft on the Share Prices and Systematic Risk of Consumer Electronics Companies' 52 Information & Management.

Hovav A and J D'Arcy, (2005). 'Capital Market Reaction to Defective IT Products: The Case Of Computer Viruses' 24 Computers & Security.

Hovav A and J D'Arcy, (2003). 'The Impact of Denial-Of-Service Attack Announcements on the Market Value Of Firms' 6 Risk Management and Insurance Review.

Kabanda S, M Tanner and C Kent, (2018). 'Exploring SME Cybersecurity Practices in Developing Countries' 28 Journal of Organizational Computing and Electronic Commerce.

Kashmiri S, C Nicol and L Hsu, (2016). 'Birds Of A Feather: Intra-Industry Spillover Of The Target Customer Data Breach And The Shielding Role Of IT, Marketing, And CSR' 45 Journal of the Academy of Marketing Science.

Kasznik R and B Lev, (1995). 'To warn or not to warn: Management disclosures in the face of an earnings surprise' 113-134.

Kaur G, H Z Lashkari and H A Lashkari, (2021). *Understanding Cybersecurity Management In Fintech*, (Cham: Springer, 2021).

Kilovaty I, (2014). 'Rethinking the prohibition on the use of force in the light of economic cyber warfare: towards a broader scope of Article 2 (4) of the UN Charter', JL & Cyber Warfare 4: 210.

Ko M and D Carlos, (2006). 'The impact of information security breaches on financial performance of the breached firms: an empirical investigation' Journal of Information Technology Management 17, no. 2 13-22.

Kosutic D and F Pigni, (2020). 'Cybersecurity: Investing For Competitive Outcomes' 43 Journal of Business Strategy.

Kothari S, X Li and J Short, (2009). 'The Effect Of Disclosures By Management, Analysts, And Business Press On Cost Of Capital, Return Volatility, And Analyst Forecasts: A Study Using Content Analysis' 84 The Accounting Review.

Kubo Mačák, (2016). 'Is the international law of cyber security in crisis?' IEEE 8th international conference on cyber conflict (CyCon) 127.

Lawson B and D Samson, (2001). 'Developing Innovation Capability in Organisations: A Dynamic Capabilities Approach' 05 International Journal of Innovation Management.

Li H, W No and T Wang, (2018). 'SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors' 30 International Journal of Accounting Information Systems.

Loughran T and B McDonald, (2011). 'When Is A Liability Not A Liability? Textual Analysis, Dictionaries, and 10-Ks' 66 the Journal of Finance.

McNutt J, (2004). 'Analysis of the US-CERT DAC' Carnegie-Mellon University Pittsburgh Pa Software Engineering Inst.

Mitchell D and C Coles, (2003). 'The Ultimate Competitive Advantage Of Continuing Business Model Innovation' 24 Journal of Business Strategy.

Morse E A, V Raval and J R Wingender Jr., (2017). 'SEC cybersecurity guidelines: Insights into the utility of risk factor disclosures for investors' The Business Lawyer 73, no. 1 1-34.

Morse E, V Raval and J Wingender, (2011). 'Market Price Effects Of Data Security Breaches' 20 Information Security Journal: A Global Perspective.

Mossburg E, J Gelinne and H Calzada, (2016). 'Beneath the surface of a cyberattack: A deeper look at business impacts'.

Pirounias S, D Mermigas and C Patsakis, (2014). 'The Relation Between Information Security Events And Firm Market Value, Empirical Evidence On Recent Disclosures: An Extension of the GLZ Study' 19 Journal of Information Security and Applications.

Prince B, (2015). 'Shifting Priorities: How Enterprises are Safeguarding against Cybersecurity Threats' 196 Forbes 119–124.

Ramírez M and others, (2022). 'The Disclosures Of Information On Cybersecurity In Listed Companies In Latin America—Proposal For A Cybersecurity Disclosure Index' 14 Sustainability.

Robbins R and P Rothenberg, (2005). 'Securities disclosure' Insights: The Corporate & Securities Law Advisor 19, no. 5.

Rogers J and A Van Buskirk, (2009). 'Shareholder Litigation and Changes in Disclosure Behavior' 47 Journal of Accounting and Economics.

Sample C and others, (2017). 'Culture + Cyber: Exploring the Relationship' In Advances in Human Factors in Cybersecurity, 593:185–196. Cham: Springer International Publishing.

Skinner D, (1994). 'Why Firms Voluntarily Disclose Bad News' 32 Journal of Accounting Research.

Telang R and S Wattal, (2007). 'An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price' 33 IEEE Transactions on Software Engineering.

Wang T, J Ulmer and K Kannan, (2013). 'The Textual Contents of Media Reports of Information Security Breaches and Profitable Short-Term Investment Opportunities' 23 Journal of Organizational Computing and Electronic Commerce.

Yadron D, (2014). 'Boards Race to Fortify Cybersecurity' the Wall Street Journal.

Yayla A and Q Hu, (2011). 'The Impact Of Information Security Events On The Stock Value Of Firms: The Effect Of Contingency Factors' 26 Journal of Information Technology.

Doi: https://doi.org/10.52132/Ajrsp.e.2023.54.1