The 6th International Conference on Economic Management and Green Development (ICEMGD 2022)
DOI: 10.54254/2754-1169/3/2022727

The Effectiveness of Information Disclosure under Cyber Attack

Shaojun Tong[1,a,*]

[1]University of Miami Coral Gables, FL 33124
a. sxt816@miami.edu
**corresponding author*

Abstract: With the global economy increasingly relying on electronic transactions, more and more companies are suffering from network attacks, which have a certain impact on the future development of their enterprises. I use the information of cyber attacks suffered by Listed Companies in the United States from 2005 to 2019 to analyze whether the cyber attacks will have a short-term impact on the stock prices of the companies under attack, and whether effective information disclosure can help the companies to stop the loss effectively to a certain extent. I find that effective information disclosure can help enterprises reduce the negative impact to a certain extent, and when the relevant information reaches a higher degree of openness and transparency, it can help enterprises go through the crisis more smoothly compared to the enterprises less so.

Keyword: cyber-attacks; stock price; Information disclosure

1. Introduction

The global economy is increasingly dependent on electronic transactions, digital data and electronic communications, so more and more companies and investors are paying attention to network security and the loss of cyber-attacks on companies. A 2020 survey from Allianz Corporation [1] shows the fact that the risk of global cyber attract has grown exponentially during the past 15 years, with the development on date analysis and IT infrastructure. So what is cyber-attack? Cyber-attack refers to any unauthorized access or attempt to enter other people's computer network. This kind of behavior includes the attack to the whole network, also includes the attack to the server or single computer in the network. The scope of the attack ranges from simply making the server unable to provide normal services to completely destroying and controlling the server. The intruder uses computer and network technology, uses the weak link of the network, invades the other party's computer and its system to carry out a series of destructive activities, such as collecting, modifying, destroying and stealing information. There are many types of network attacks, such as internal malicious leakage or device loss. CRP classifies the breach into 8 types, which I will use latter in the analysis.

Network attack will not only make its server denial of service, which will cause the company to suspend business and bring economic losses to the company, but also may affect the company's reputation and the subsequent compensation or other related issues. Therefore, it is not surprising that cyber security has become the focus of policy makers, participants and regulators in various economic sectors, pointed out that global enterprises spend more than one trillion US dollars on information technology investment, and the cost of network attack is also increasing [2]. More and more companies begin to include the risk of network attack in their main risks.

However, although more and more companies begin to pay attention to network security, the disclosure of network attacks is slightly insufficient. The 2011 guidance of the securities and Exchange Commission on cyber security disclosure requirements [3] states that "registrants should disclose the risk of cyber incidents in their MD&A if these issues are among the most significant factors that make an investment in the company speculative or risky." SEC specifies what factors companies should consider when assessing cyber-risk: "In determining whether risk factor disclosure is required, I expect registrants to evaluate their cyber security risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents." The guidance also states that: "As part of this evaluation, registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption." In practice, disclosure requirement may be relevant for multiple sections in 10k filings including: Risk Factors, MD&A, Description of Business, Legal Proceedings, Financial Statement, and Disclosures (e.g. material prevention costs, or losses sustained). In addition, some states have set up state laws to regulate the information disclosure of cyber attacks. However, there are two kinds of corporate disclosure: internal disclosure and external disclosure, so there is a big controversy about the effectiveness of information disclosure regulation in the past research.

As for how to define the impact of cyber-attacks, most of the early literatures are divided into two types. Part of the researches follow the original economic theory and regard reputation as a kind of market loss born in value, and the upper limit of its loss is unexplained market loss. It mainly analyzes the possible impact of cyber attacks by analyzing the change of error value in its market value. Another kind of research is to evaluate the impact of earnings or stakeholders, and directly analyze the changes of stock price or other interest indicators. In this paper, I use the second method, I analyze the change of its stock price after deducting the influence of other factors. Specifically, this paper argues that cyber attacks impact company value through the following ways:

- Direct financial cost and physical damage cost.
- Losses arising from intellectual property theft.
- Loss due to destruction or deletion of software and data.
- Business interruption and post attack / post default recovery costs.
- Loss of customer and price power.
- The cost of regulatory fines and legal settlement, as well as the cost of future premium increases.
- Potential cost of third party liability.

Therefore, this paper selects the data of network attacks from 2005 to 2019, and selects 456 network attacks against listed companies in the United States from more than 4000 cases. In the research method, the OLS model is employed to compare the stock market performance of the attacked companies and the companies in the same industry to analyze whether the network attack will have an impact on the target company in the short term and whether the appropriate information disclosure can help the company stop loss effectively. By verifying the effectiveness of information disclosure stop loss, this paper analyzes what strategies companies should adopt for risk management of network attacks.

Firstly, I use the Fama-French three factor dataset to calculate the cumulative abnormal return of enterprise stock, and prove that the network attack will affect the company's stock price in the short term through multiple linear regressions. After verifying the impact of network attacks, I use cross-section regression to verify whether different degrees of information disclosure can reduce the cumulative abnormal returns of enterprise stocks. In the regression comparison divided by different groups, I find that effective information disclosure can inhibit the abnormal returns of enterprise stocks to a certain extent, And when the disclosure of network attack information reaches the highest level, it can completely offset the short-term impact of network attack on enterprise stocks.

The rest of this paper is organized as follows. In the second section, I mainly review and summarize the relevant literature, summarize the early literature analysis of the impact of network attacks and information disclosure. The third part analyzes the impact of network attacks on stock prices and the effectiveness of information disclosure stop loss. The fourth section studies the data results, and the fifth section gives some conclusions and suggestions according to the relevant data analysis.

2. Literature review

In the past, literature studies focused more on verifying whether cyber attacks will affect the stock price and whether there is spillover effect, which will affect the trading market. In the past, there was a lack of relevant supervision on the information disclosure of cyber-attacks, and few companies made self-disclosure about cyber defaults. Therefore, most of the studies were conducted on a small sample, and because the stock price was affected by more factors, it is difficult to accurately determine whether its value change was caused by cyber-attacks in the long run, Therefore, most of the studies are short-term and only focus on the correlation analysis within the short-term window.

In CRS's report to Congress [4], it is pointed out that cyber attacks will have an impact on the stock price of target enterprises in the short term, and they will suffer a loss of 1% - 5% within a few days after the attack. In addition, the cost of cyber attacks is also rising, and the expenditure of enterprises on it security is also increasing, However, in the report analysis, the effect curve of spending it security expenditure appears chimney curve, which indicates that the return on current security expenditure is gradually decreasing.

Kevin and kathleen [5] used the event research method to sample 77 events from 2004 to 2006, and found that the overall impact of data leakage on shareholders' wealth is negative and statistically significant. Companies with higher P / E ratio of research expenditure may suffer more negative impact, The size of the company and the status of subsidiaries can reduce its negative impact to a certain extent.

Shaen and Constantin [6] used EGARCH model to analyze the network events from 2000 to 2015, and found that network attacks not only affect the stock price of the target company, but also may have spillover effect on other companies related to the affected company through listing on the same exchange. And Onur Kemal Tosun [7] used DID model to examine the relationship between the unexpected corporate security breach and the CAR in the short and the long-term. The analysis found that the security breach may have more negative influence on the short term because it increased investor’s attention, but for the long-term, it may have influence on the firm’s policies.

However, the research of Karen [8] points out that the short-term return of network attacks is significantly negative in the time window between - 1 and 5 days of the release date. Gills and other studies on Internet risk disclosure point out that the impact of default announcement on the stock price of listed companies is relatively limited, but there is no lack of supervision in the market and regulatory agencies, so more research is needed for the lack of response to the market.

Most of the previous studies have proved that cyber attacks have a negative impact on the short-term stock price changes of the target enterprises, which is statistically significant. However, there is a lack of research on the information disclosure of cyber risks and attacks. Therefore, this paper will focus on whether information disclosure can restore the company's reputation to a certain extent and reduce its negative impact on the company, So that investors can be more rational and comprehensive analysis of the impact of network attacks on enterprises, so as to reduce overreaction.

3. Data and research methodology

3.1 Data sources

First, I collected information about companies that suffered cyber attacks from 2004 to 2016 from the privacy clearing house (PRC) website. The relevant information includes the basic information of the attacked company (such as enterprise name, registration place, time, etc.), the type of network attack, a brief description of the network attack, and the number of records affected (if any). In addition, in order to simplify the relevant research on the later financial market response, I only retained the relevant information about the cyber attacks on American listed enterprises, and deleted the relevant cases describing and defining the problems. Finally, the sample size of network attack events will be reduced from more than 4000 to 456.

Secondly, I obtain daily data on company's share prices (in US dollars), traded volume, and bid-ask spreads for publicly traded US firms from Yahoo finance and financial variables from SEC Electronic Data Gathering, Analysis, and Retrieval (EDGAR).

3.2 Empirical strategy

First, I test whether the data leakage has a short term negative impact on the stock price. To do this, I directly analyze the short-term stock market response around the publicly announced cyber-attacks. And abnormal returns are measured using an estimation window of 3-month, which ends 30 days before a breach publicly disclosed. the CAR is calculated based on an event window of [-1, +3], which indicates the number of trading days relative to the data breach disclosure date. The expected return is estimated using the three factor Fama-French model, and the Fama-French three factor dataset from Kenneth R. French's website1. According to the convention of event analysis, the discernibility assumption is that after controlling the tradable risk factors, the disclosure of securities default is not related to the expected return of the company. Secondly, because the abnormal rate of return may be affected by the market and industry, and the choice of controlling enterprises should try to reduce unnecessary artificial control, so in the selection of controlling companies, I will include the companies in the same industry as the target company into the control group, so as to reduce the error caused by artificial selection.

First of all, I use the target company and the control company to conduct regression tests to test the relationship between safety violations and cumulative abnormal returns conditional on firms' characteristics. My first regression takes the form:

$$CAR_i = \alpha + \beta_1 attacked + \beta^{'} x_i + \varepsilon_i \tag{1}$$

where CAR_i represents the cumulative abnormal returns for that data breach for firm i over a given event window which is [-1, +3] days surrounding the attack date, x_i represents a vector of firm characteristics calculated over the year prior to the event, and attacked is a dummy variable which takes the value of one for the firms experienced cyber-attacks and zero otherwise.

Among the relevant control variables of the company, I selected the company size, ROA, leverage, cash and cash equivalents and market to book ratio as the relevant control factors of multiple linear regression. Where size is log (asset + 1), Che_At is cash and cash equivalents

[1] http://mba.tuck.dartmouth.edu/pages/faculty/ken.french/data_library.html

divided by assets, and leverage is total liabilities divided by total assets. These three variables are used to evaluate the operating status of the enterprise. The calculation method of ROA is net income in total assets, and the calculation formula of market to book ratio is the total equity of the company divided by the market value of the company, These two indicators measure the performance of its stock in the stock market. Therefore, selecting these five factors as control variables can reduce the interference of other factors to a certain extent, so as to better verify whether the network attack will have a short-term impact on the company's stock.

Secondly, I graded the information disclosure of the company according to the description of the enterprise network attacks on the PRC website. Level 0 means that the company does not have any description of the situation of the network attack and does not know the cause of the incident. Level 1 means that the company has disclosed the cause of the network attack. Level 2 companies have not only disclosed the cause of the network attack, but also announced the possible losses caused by the network attack. On the basis of level 2, the level 3 company also announced the time when it discovered the attack. Four level companies not only point out the cause of the event and the loss content, but also disclose the exact time of the event. Grade 5 companies have more comprehensive information disclosure for network attacks. In the announcement, they will accurately explain the causes and events of the events, and will accurately explain the loss content and damage scope, which can help stakeholders to understand and evaluate the network attacks more rationally and objectively. By this definition, the higher the grade, the more details are disclosed in the statements.

After defining the level, I use the cross section regression to test whether different degrees of information disclosure will affect the negative impact of network attacks on the target enterprises, so as to verify whether information disclosure is an effective way to stop loss.

4. Results and analysis

4.1 Fundamental analysis of network attack

As shown in Figure 1, cyber-attack related incidents in the United States have been on the rise since 2005. On one hand, with the gradual development of Internet economy since 2005, more and more companies began to use electronic transactions, and analyzed and summarized through big data; On the other hand, since 2000, the United States has gradually transformed from cash payment to credit card payment, and more personal information has been stored in the bank database, so network attacks have become a more effective way of illegal information collection.

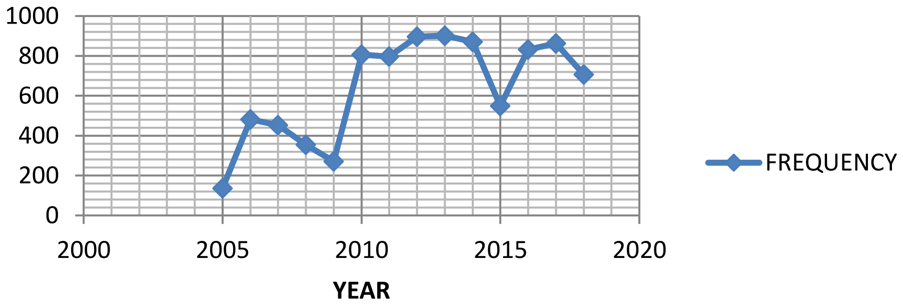

Figure 1: Summary of total network attack cases every year.

There are many reasons for network attacks, which are summarized by PRC website as follows: fraud involving Debit and Cards not via hacking (CARD), hacked by an outside party or infected by malware (HACK), insider such as employee or contractor (INSD), paper document that are lost, discarded or stolen (PHYS), portable device lost ,discarded or stolen (PORT), stationary computer loss(STAT), unintended disclosure not involving hacking, intentional breach or physical loss (DISC), and unknown reason(UNKN). As shown in Figure 2, hack accounts for 28% of all the causes of network attacks. It can be seen that network attacks are mostly caused by malicious attacks or infection of malicious websites by hackers, followed by information leakage or equipment damage and loss caused by unintentional. Therefore, in order to avoid the risk of network attack, I should not only strengthen the construction of firewall to reduce the risk and loss of hacker attack, but also strengthen the internal training and management to reduce the information leakage caused by unintentional equipment loss or damage, and strengthen the supervision, so as to reduce the malicious information leakage and equipment theft.

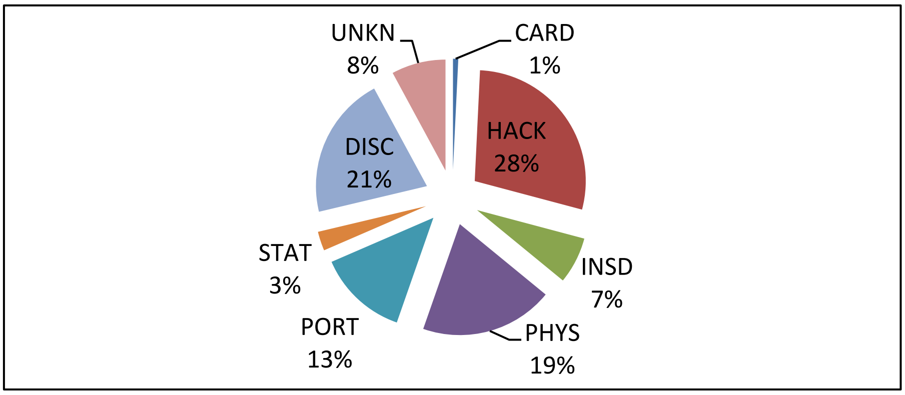

Figure 2: Scale chart of causes of network attacks.

In addition, the PRC website also classifies the types of organizations that have suffered from cyber-attacks, including BSR(retail/merchant including online retail), BSF(financial and insurance services), BSO(other business), EDU(educational institution), GOV(government or military) , NGO (nonprofits), MED(healthcare, medical providers and medical insurance services), and UNKN(unkown). Surprisingly, the most vulnerable organizations are not commercial organizations, but medical organizations. The main reason for this phenomenon is that the personal information stored in medical organizations is more comprehensive, and the firewall is weaker than that of commercial organizations, which makes it easier for hackers to obtain relevant information successfully. In the network attacks against commercial institutions, the proportion of listed companies is relatively small, only 18%. On the one hand, it is because the listing rate of their own companies is low, and more enterprises are more willing to finance by issuing bonds. On the other hand, listed companies are subject to the supervision and management of China Securities Regulatory Commission, which will have better protection measures for information security, because it is more difficult for hackers to succeed.

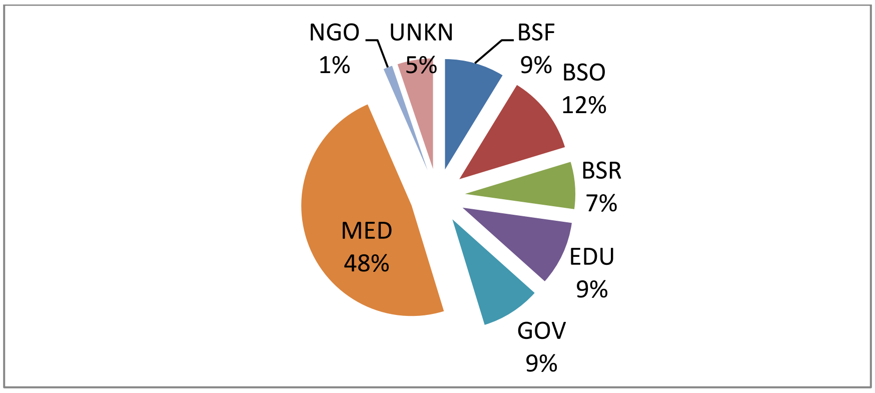

Figure 3: Proportion of organizations suffering from cyber attacks.

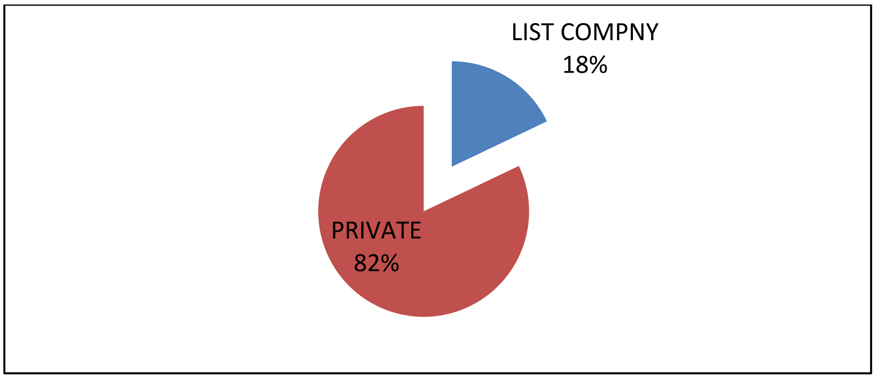

Figure 4: Proportion of listed companies.

4.2 Security breaches and stock return

According to the results of regression analysis, I find that cyber attacks have a short-term negative impact on the company's stock price, which is statistically significant at 1% level. Although on the whole, the company's stock price is more affected by the company's size, ROA, leverage and other conventional company operating indicators, but in the car after cyber attack, the correlation coefficient of cyber attack can reach -0.0139, and its P-value is 0.003, which is statistically significant at 1% level.

The result suggests that the firms being attacked endure a 1.56% decrease in CAR compared to the same industry peers that are not attacked in within the [-1, +3] event window surrounding the cyber attack. This negative relationship is consistent with prior literature and builds the common ground for me to further study whether information disclosure can help the attacked enterprises stop loss effectively.

Table 1 : The result of the OLS regression.

Note: The symbols ***, ** and * indicate statistical significance at the 0.01, 0.05 and 0.1 level, respectively.

	cumulative_abnormal_return
attacked	-0.014***
	(0.003)
size	-0.000
	(0.595)
roa	0.005
	(0.459)
leverage	0.003
	(0.705)
che_at	0.025***
	(0.001)
mkt_bk	0.000
	(0.554)
_cons	-0.013**
	(0.028)
N	1744
adj. R-sq	0.017

4.3 Cross section regression results

In this paper, I conduct cross-sectional regression analysis according to different groups. First, I conduct regression analysis with grade 2 as the cutoff, because the main difference between the groups above grade 2 and the groups involved in grade 0, grade 1 and grade 2 is that the companies in the low-level group only disclosed the general causes of the network attack and the approximate types of lost content, and did not specify the value of the lost content, the scope of the lost content and the time of the attack, Therefore, I think that the low-level group does not have effective information disclosure, so I think that level 3 is the lowest limit for effective information disclosure, Therefore, taking the standard of level 2 as the boundary, I divide the network attack cases into two groups according to the degree of information disclosure. The network attack information disclosure rating of the cases contained in the high-level group is higher than level 2, while the information disclosure rating of the relevant cases contained in the low-level group is less than or equal to level 2. And conduct cross-sectional regression analysis to verify whether information disclosure can reduce the negative impact of network attacks on companies to a certain extent. According to the comparison of regression analysis results, I can see that whether in the high-level group or the low-level group, network attacks are statistically significant, but the value of the coefficient has changed greatly. In the low-level group, the correlation coefficient is -.0154011, while in the high-level group, the coefficient decreases to -.0122399, and the absolute value of the correlation coefficient decreases by 20.5258%, Therefore, I think that effective information disclosure can reduce the negative impact of network attacks on the stock price of enterprises to a certain extent.

Table 2 : Cross-section regression’s result.

Note: this table presents cross-section regression result, the first regression result is the OLS regression results without classification, the second is the regression results of low-grade group, and the column is the regression results of high-grade group. And The symbols ***, ** and * indicate statistical significance at the 0.01, 0.05 and 0.1 level, respectively.

	cumulative_abnormal_return		
	(1)	(2)	(3)
attacked	-0.014***	-0.015**	-0.012*
	(0.003)	(0.022)	(0.080)
size	-0.000	-0.001	0.001
	(0.595)	(0.220)	(0.594)
roa	0.005	0.025*	-0.006
	(0.459)	(0.063)	(0.481)
leverage	0.003	0.026**	-0.014
	(0.705)	(0.043)	(0.153)
che_at	0.025***	0.024*	0.025***
	(0.001)	(0.062)	(0.004)
mkt_bk	0.000	0.000	-0.000
	(0.554)	(0.348)	(0.428)
_cons	-0.013**	-0.007	-0.016**
	(0.028)	(0.468)	(0.021)
N	1744	649	1095
adj. R-sq	0.017	0.023	0.017

Secondly, I do cross-sectional regression analysis with different levels as the boundary. In the regression analysis results with level 2 and level 3 as the boundary, the coefficients of both high-level and low-level groups of network attacks do not change significantly, but when partitioning with level 4, Regression analysis results show that different levels of effective information disclosure will also have different results on the negative impact of network attacks. First of all, when the group is divided into two groups using level 4 as the cutoff, the high-level group is the target enterprise whose degree of information disclosure reaches level 5, and the enterprises in this group will make a very detailed announcement for their network attack event, including the cause of this event, Therefore, I generally believe that under the level 5 information disclosure level, there will be no information inequality for this network attack event. At this time, the company stakeholders can use their announcement information to objectively and rationally analyze the impact of this event. The regression analysis results also show that when the degree of information disclosure reaches level 5, the p value is 0.19, so I can think that the negative impact of network attacks on enterprises is not statistically significant. Therefore, I believe that a high level of information disclosure can help the attacked enterprises effectively control the abnormal return of theirs stock, so as to reduce the loss of enterprise value. help the attacked enterprises stop losses effectively.

Table 3: Cross-section regression's result.

Note: this table presents cross-section regression result, the first regression result is the OLS regression results without classification, the second is the regression results of low-grade group, and the column is the regression results of high-grade group. And The symbols ***, ** and * indicate statistical significance at the 0.01, 0.05 and 0.1 level, respectively.

	cumulative_abnormal_return		
	(1)	(2)	(3)
attacked	-0.014***	-0.013**	-0.017
	(0.003)	(0.023)	(0.190)
size	-0.000	-0.001	0.001
	(0.595)	(0.256)	(0.476)
roa	0.005	0.022*	-0.007
	(0.459)	(0.074)	(0.436)
leverage	0.003	0.025**	-0.016
	(0.705)	(0.034)	(0.111)
che_at	0.025***	0.032***	0.020**
	(0.001)	(0.006)	(0.030)
mkt_bk	0.000	0.000	-0.000
	(0.554)	(0.411)	(0.558)
_cons	-0.013**	-0.013	-0.015*
	(0.028)	(0.139)	(0.051)
N	1744	760	984
adj. R-sq	0.017	0.024	0.009

5. Conclusion

According to the results of regression analysis, I can see that cyber attacks do have a short-term negative impact on the stock price of enterprises. Therefore, enterprises should take preventive measures against cyber attacks and stop loss effectively after the attacks. The cross-sectional analysis results show that effective information disclosure and improving the degree of information disclosure can reduce the negative impact of network attacks to a certain extent. In the past, some enterprises would like to reduce the negative impact by concealing or deliberately reducing the situation of the incident. Therefore, most of the current US policies and regulations have new requirements for the information disclosure of cyber attacks. According to the relevant regulations, the attacked enterprises should timely inform of the occurrence of the incident, quickly respond to the attack and conduct internal investigation, However, there are not too many restrictions on the content of information disclosure, so many enterprises do not know whether it is beneficial to improve the degree of disclosure. Our research has proved that effective information disclosure can help enterprises reduce the negative impact to a certain extent. Therefore, enterprises should take the initiative to disclose their findings after internal investigation, so as to help investors view the attack objectively and rationally, improve investors' information and reduce its subsequent impact.

However, the current research still has some limitations. Firstly, with the continuous development of electronic information, more and more Internet start-ups appear, and a lot of network attacks are no longer only aimed at listed companies, but start to attack emerging start-ups. On one hand, because they are in the early stage of entrepreneurship, information security is weak, on the other hand, its internal information can help hackers find the next target. However, because it is in the initial stage of entrepreneurship, the enterprise does not issue stocks and bonds, and its related information disclosure is less, it is difficult for us to make an effective analysis of the network attacks it suffered, so I can not point out whether the stop loss effect brought by information disclosure is also effective for it. Secondly, the impact of the current network attack has a certain joint effect. A network attack may not only have a negative impact on the enterprise, but also may have a certain degree of impact on its subsidiaries and network security cooperation companies. However, the current research can not explain whether information disclosure has an impact on the joint effect, This requires us to gradually improve the later research.

References

[1] *Allianz Global Corporate and Specialty. Allianz Risk Barometer: Identifying the Major Business Risks for 2020. (2020).*

[2] *Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-risk Disclosure: Who cares? (Georgetown McDonough School of Business Research Paper No. 2852519).*

[3] *Li, H., No, W. G., & Wang, T. SEC's cyber-security disclosure guidance and disclosed cyber-security risk factors. International Journal of Accounting Information Systems, 30, 40-55. (2018).*

[4] *Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. The economic impact of cyber-attacks. Congressional research service documents, CRS RL32331 (Washington DC), 2. (2004).*

[5] *Kevin M. Gatzlaff and Kathleen A. McCullough. The Effect of Data Breaches on Shareholder Wealth. Risk Management and Insurance Review 13(1):61-83 (2010).*

[6] *Shaen Corbet, Cons tantin Gurdgiev,What the hack: Systematic risk contagion from cyber events, International Review of Financial Analysis, Volume 65, (2019)*

[7] *Tosun, Onur Kemal, Cyber Attacks and Stock Market Activity. (2019)*

[8] *Hogan, Karen M., A Global Comparison of Corporate Value Adjustments to News of Cyber Attacks. Journal of Governance and Regulation 9(2). (2020)*