사이버공격으로 인한 기업의 피해 비용과 주식시장에 미치는 영향

오 일 석[†] · 이 석 윤[††]

요 약

사이버공격으로 인하여 세계는 지속적으로 피해를 입고 있다. 2003년도 조사에 의하면 사이버공격에 따른 비용은 1996년에 비하여 226배나 증가하였다고 한다. 사이버공격으로 인한 피해 비용을 정확하게 파악하는 것은 곤란하지만 특정 분야와 일부 기업에 대하여 이에 대한 여러 조사와 연구는 적정한 정보보안 예산 투입수준을 결정하는데 좋은 참고자려가 될 것이다. 이는 적정한 정보보안 예산 투입수준을 결정하는데 좋은 참고자료가 될 것이다. 또한 사이버공격으로 인하여 기업들의 주식이 하락하는 것으로 조사되었다. 특히 순수한 인터넷 기업의 주식이 사이버 공격에 의하여 가장 크게 영향을 받는 것으로 조사되었다. 1.25 인터넷 대란으로 우리나라 주식시장도 전반적으로 하락한 것으로 파악되었다. 이렇듯 사이버공격으로 인하여 기업의 피해 비용이 증가하고 주가도 하락하고 있는 것으로 파악되었기 때문에 기업이 의사결정권자들로 하여금 이에 대한 책임을 부담하도록 하는 방안을 제안하고자 한다.

키워드 : 사이버공격에 따른 피해비용, 주가하락

A Study on cost damage of Cyber Attacks and their Impact on Stock Market

Il-Seok Oh[†] · Seok-Yun Lee[††]

ABSTRACT

Cyber Attacks have increased damages constantly in all over the world for several years. A survey said the cost caused by Cyber Attacks had increased 226 times from 1996 to 2003. It is very difficult to calculate the cost by the Attacks exactly but the calculating the cost of cyber attacks would be great helpful for a company to decide how much budget to spend to Information Security. In this research we could reach the conclusion : the cyber attacks has decreased the stock price of the companies, especially pure internet companies. But the stock market has not greatly impacted by the types of Cyber Attacks. Korean stock market also impacted by the Internet Destruction Accident happened Jan. 25. 2003. On the basis of this study we will recommend a policy or a regulation which force board of directors and officers of a company to have information security liability.

Key Words : Cyber Attacks, Economic Impact, Cost, Value of a Stock

1. 서 론

정보화 사회에 살고 있는 우리는 종종 "컴퓨터 바이러스에 주의하라"고 하거나 "00 기업에 대한 해킹공격 발생" 등의 뉴스를 접하고 있다. 그리고 사이버 공격이 발생한 후에 기업들이 수 십 억원의 재산 피해를 입었다는 보도를 듣기도 한다. 지난 1.25 인터넷 대란 때, 각종 언론 매체들은 온라인 쇼핑몰, 항공과 여행업계, 은행과 증권업계 및 PC 방 등에서 수 백 억원 이상의 피해가 발생하였다고 보도하였다. 사이버 공격으로 인하여 기업들이 입은 피해는 실질적으로 공격을 당한 컴퓨터와 저장된 정보 뿐만아니라 기업에 대한 이미지나 신뢰도 상실 등과 같은 무형의 자산에 까지도 이르고 있다.

그러나 사이버공격의 발생과 피해 건수 등에 대하여는 논의와 조사가 활발하게 진행되고 있으나 사이버공격에 따른 기업의 피해 비용에 대해서는 구체적인 논의와 조사가 거의 없는 실정이다. 오늘날 기업들은 정보통신기술의 발달로 인하여 기획, 연구개발, 마케팅, 인사 및 노무, 행정 등과 관련된 각종 활동과 주요 정보를 정보시스템에 의존하면서 이윤의 극대화와 효율적인 경영을 도모하고 있다. 그러나 기업들은 정보 시스템에 대한 의존성 증가로 인하여 사이버 공격에 따른 피해 위험에 항상 직면하고 있다. 이러한 상황하에서 사이버 공격으로 인한 피해 비용을 파악하는 것은

† 정 회 원 : 노스웨스턴대학교 법과대학 L.L.M 과정
†† 정 회 원 : 성균관대학교 정보통신공학부 박사과정
논문접수 : 2005년 11월 25일, 심사완료 : 2006년 1월 5일

기업의 이윤 극대화와 사회적인 비용 감소를 위하여 반드시 필요하다. 따라서 이하에서는 사이버공격으로 인한 기업의 피해비용을 파악하고 사이버공격이 주식시장에 미치는 영향을 고찰하여, 기업들이 정보보호 없이는 이윤을 극대화할 수 없다는 점을 보여주고자 한다. 나아가 이러한 연구결과를 바탕으로 기업의 이익 보호와 주주의 이익을 위하여 기업의 정보보호 책임 규정을 제안하고자 한다.

이를 위하여 우선 1.25 인터넷 대란으로 인한 국내 기업의 피해 비용과 각종 사이버공격으로 인한 미국 등 세계적 기업들의 피해 비용을 살펴본다. 또한 사이버 공격으로 인한 기업들의 피해 유형, 사이버공격과 주가 변동의 상관성, 기업유형과 사이버공격으로 인한 주가 변동 등을 파악하고 1.25 인터넷 대란과 우리나라 주식시장의 영향에 대하여 살펴본다. 마지막으로 기업의 이익 보호 등을 위하여 기업의 정보보호 책임을 규정하는 것을 제안하고자 한다.

2. 사이버공격에 따른 비용

2.1. 1.25 인터넷 대란으로 인한 기업들의 피해 비용

지난 2003년 1월 25일 슬래머 웜으로 인하여 전국의 인터넷 서비스가 7시간 가까이 중단되면서 기업들에게 막대한 피해가 발생하였다[2][1]. 그런데 이 사건은 사이버공격으로 인한 기업들의 피해 비용을 어느 정도 가늠해 볼 수 있는 계기를 마련하였다. 즉, 이 사건으로 인터넷 서비스의 중단으로 인한 인터넷 쇼핑몰 업체들의 손해와 항공사의 손해, PC방 영업 중단 및 인터넷 뱅킹의 마비로 은행과 증권사도 손해를 입었다. 이러한 피해를 비용으로 환산하면 온라인 쇼핑몰은 인터넷 거래 중단으로 업체당 2억에서 5억원 가량의 피해비용이 발생하였으며 PC방의 경우 약225억원의 피해비용이 발생하였다[2].

그러나 항공사와 여행사, 은행 및 증권 등의 손해액을 정확하게 측정한 자료는 없는 실정이다. 또한 기업들이 업무마비로 실제 발생한 비용과 복구비용 및 고객들이 인터넷을 이용하지 못함으로 인하여 받은 비용 등은 산정하지도 못하고 있다.

2.2 사이버공격으로 인한 세계적 피해 비용

2.2.1 CSI/FBI의 조사에 따른 사이버공격 피해 비용

미국 컴퓨터보안연구소(Computer Security Institute: CSI)와 FBI가 매년 공동으로 실시하고 있는 "컴퓨터와 보안에 관한 설문조사[3]"에 의하면 2005년도에 사이버공격으로 인하여 1억 3천만 달러의 피해 비용이 발생하였다고 한다. 이 보고서에 의하면 2005년도에 바이러스로 인한 피해 비용이 4천2백만 달러, 비인가적 접근으로 인하여 3천 1백만 달러, 정보 절취로 인한 피해 비용이 3백만 달러, 서비스 거부 공격으로 인한 피해 비용이 7백만 달러에 이른다고 한다[4][3].

2.2.2 영국 Mi2g사의 사이버공격으로 인한 피해 내용

사이버공격이 발생한 이후 컴퓨터 관련 국내외 언론들은 피해 비용 등에 대하여 보도하는데 대부분 컴퓨터 보안 기업인 영국의 Mi2g가 발표하는 비용을 가장 빈번하게 인용하고 있다. Mi2g는 1995년부터 웜, 바이러스, 기타 악성 소프트웨어 공격 등 각종 사이버공격으로 인한 피해 비용에 대한 추정치와 자료를 제공하고 있다[6]. Mi2g가 제공하는 비용에는 업무중단, 데이터 탈취 및 삭제, 서비스 거부 공격으로 인한 비용, 민감한 정보내지는 지적재산권 관련 정보의 상실, 기업 이미지의 추락, 주가하락 등이 반영되어 있다[6]. Mi2g는 각 은행, 보험회사는 물론 해커 게시판 및 해커 활동 모니터링 등을 통하여 수집된 자료를 기초로 비용을 추정한다고 한다. 또한 이렇게 수집한 정보를 기초로 자신들의 독창적인 방법론에 의하여 비용을 추정하였다고 한다.

Mi2g의 조사에 의하면 <표 1>에서 보는 바와 같이 1996년부터 2003년까지 8년 동안 사이버공격으로 인한 피해 비용은 무려 226배나 상승하였다는 것을 알 수 있다. 특히, 1999년부터 사이버공격으로 인한 세계적 비용이 급격하게 상승하였다는 점을 알 수 있다. 이는 1999년부터 사이버공격이 세계적으로 증가하기 시작한 것과 무관하지 않은 것으로 판단된다. 즉, 미국의 경우만 예를 들어 살펴보면 1999년도에는 9,859건의 사이버공격이 발생하였으며 2000년도에는 이보다 121%가 증가한 21,756건이, 2001년도에는 52,658건이 발생하여 전년대비 145% 증가하였고 2002년도에는 82,094건이 발생하여 전년대비 56%나 증가하였다[7].

〈표 1〉 사이버 공격으로 인한 세계적 비용 추정치(1996-2003)

연도	비용 ($십억)		연도	비용($십억)	
	하한	상한		하한	상한
1996	0.8	1.0	2001	25	30
1997	1.7	2.9	2001	33	40
1998	3.8	4.7	2002	110	130
1999	19	23	2003	185	226

2) 더욱이 이 사건을 처리하는 와중에 보여준 정부와 민간 전문기관들의 대응책은 비효율적이었으며 적시에 대책을 제공하지 못하여 우리 정부로 하여금 국가차원의 정보보안 정책을 재정립하고 국가정보보안체계를 확립하도록 하는 계기를 마련하였다.

3) 이 조사는 1996년부터 실시하고 있으며 미국내 컴퓨터 보안 관련 기업, 정부기관, 금융기관, 의료기관 및 대학의 실무자를 대상으로 하고 있다.

4) 그러나 이 조사는 객관적으로 신뢰할 수 있는 통계 데이터를 제공하지 못하고 있다. 우선 표본 선정에 있어 의문이 제기된다. 이 조사에 대한 응답자들이 사이버공격에 노출되어 있는 업체, 기관, 또는 기타 단체의 대표적 표본이라고 말하기가 어렵다. 아울러 동 조사가 보안 전문가들의 단순한 설문 참여로 이루어졌기 때문에 전체적인 사이버 공격으로 인한 비용을 추정할 만한 정확한 통계학적 방법이 사용되었다고 할 수 없다. 보고된 사이버 공격 비용과 관련한 데이터 조차도 불완전하다. 2003년 조사에서는 응답자의 15%가 시스템에 대한 비인가적 접근 사실 조차 모르고 있었으며, 응답자 중 75%가 금전적 손실을 보고했는데 그 가운데 단지 47%만이 그 손실액을 측정할 수 있었다고 한다. 따라서 동 보고서가 언급한 피해 비용은 단지 측정 가능한 비용만을 추정한 것이며 실제의 비용에 크게 미치지 못하고 있다. 또한 비용을 계량화할 수 있는 표준 기법도 없다.
이와 같이 이 보고서의 사이버공격으로 인한 피해 비용에 대한 통계치의 신뢰성에 의문이 있는 것은 사실이지만 기업들에 대한 내부자 공격이 많았다는 사실, 응답 기관의 70% 이상이 외부로부터 사이버공격을 받았다는 사실, 사이버 공격이 있은 후 이를 법집행기관에 보고하지 않는 이유 등 사이버 공격에 대한 전반적인 동향과 각 기관의 대응 노력 등을 개괄적으로 살펴볼 수 있다는 점에서 의미를 가진다고 하겠다.

비록 Mi2g가 발표하는 사이버공격으로 인한 비용이 대부분 컨설팅 기업과 IT 보안 관련 당사자들과의 정보교류와 경험을 바탕으로 이 회사가 개발한 비용 산정 모델에 의한 것이어서 신뢰성에 대한 평가가 어려운 것은 사실이지만 사이버공격으로 인한 비용의 규모와 매년 증가되는 정도를 추정하여 볼 수 있다는 점에서 의미가 있다.

2.4 소결

사이버공격으로 인한 비용을 파악하는 것은 매우 어려운 작업이다. 각종 자료에 사이버 공격으로 인한 사고건수에 대한 통계 자료 등이 많이 발표되고 있으나 사이버공격으로 인한 피해액 내지는 사회적 비용을 제시하고 있는 경우는 매우 드물다. 이는 비용 산정을 위한 방법론, 피해범위, 시점 등 수많은 변수들이 존재하기 때문이다. 따라서 사이버 공격으로 인한 모든 사회적 비용을 산정하는 것은 거의 불가능하다고 생각된다.

모든 사회는 자연재해, 화재, 재난사고 등의 위험 요소를 가지고 있으며, 이러한 위험에 따르는 비용을 분담하고 있다. 따라서 사이버 공격으로 인한 비용도 일정한 위험을 부담하기 위한 비용으로 인식하여야 한다.

그러나 일정 기업, 특정 분야 및 순수 인터넷 기업들에 대하여 고객 면담, 보안지출비용, 공격 후 복구비용, 생산성 상실분, 매출액 감소분 등의 일정 변수를 지정하여 사이버 공격으로 인한 비용을 산정하는 것은 어느 정도 가능하다고 생각된다. 이는 기업과 정부가 어느 정도의 예산을 정보보안에 투입하는 것이 바람직할 것인가를 가늠해 볼 수 있는 중요한 자료가 될 것이다. 그러나 무엇보다도 주목하여야 할 사실은 사이버 공격으로 인한 기업의 피해 비용이 정보통신 기술의 발달과 더불어 지속적으로 증가하고 있다는 사실이다.

3. 사이버공격이 주식시장에 미치는 영향

3.1 사이버공격과 주가 변동의 상관성

기업의 주식은 기업의 산출물에 대한 기대를 반영한 자금흐름에 대한 현재 가치에 따라 값이 결정된다. 이 같은 자금의 흐름은 배당금이나 기업의 자본 이익 등과 같은 형태로 주식소유자에게 배분되는 것이다. 따라서 일정한 사건이나 상황이 기업의 미래 수입 흐름에 대한 투자자의 예상에 대하여 변화를 준다면 주가에 영향을 미칠 수 있다. 이러한 투자자의 예상변화를 가져오는 요인들에는 여러 가지가 있을 수 있지만 정보시스템에 더욱 의존하고 있는 오늘날의 기업들에게는 사이버공격으로 인한 피해 비용도 중요한 요인이 된다.

따라서 사이버 공격이 주가에 대하여 영향을 미치고 있음은 분명하다. 이러한 사실은 사이버 공격으로 인한 침해는 기업가치에 부정적인 영향을 미치고, 사이버공격으로 인하여 영향을 받은 기업은 그렇지 않은 기업에 비해 주가가 2.1%나 더 하락하였다는 미국의 연구 결과[5]에서도 잘 나타난다[8].

3.2 기업유형에 따른 주가의 영향

사이버공격이 기업에 대하여 피해 비용을 발생시키고 이로 인하여 기업의 주가가 하락하였다. 이러한 주가변동을 기업 유형에 따라 살펴보면 사업상 컴퓨터 네트워크에 대한 의존도가 높은 인터넷 기업들이 사이버공격으로 인한 피해 위협이 가장 큰 것으로 조사되었다. 이는 인터넷으로 영업하는 기업들이 사이버공격에 가장 많이 노출되어 있어 주가 하락의 가능성이 크기 때문이다.

그러나, 오프라인 활동만 하는 기업이라고 할 수 있는 전통적인 기업들은 사업상 인터넷에 대한 의존도가 최저 수준이기 때문에 사이버공격을 받을 가능성 또한 낮다[6]. 오프라인과 온라인 활동을 병용하고 있는 기업들은 인터넷을 통해 수행 중인 사업이 중단될 수 있는 위험을 안고 있기 때문에 사이버공격으로 인한 취약성 및 피해 가능성이 증가하고 있다. 반대로, 컴퓨터 보안을 제공하는 기업들은 사이버공격으로 인하여 주가상승을 기대할 수 있다. 컴퓨터 네트워크의 취약성이 증가하고 사이버공격이 발생하면 이들 기업은 수입이 늘어날 것이기 때문이다.

사이버공격으로 인하여 인터넷에 의존하는 기업들의 주가가 오프라인 활동을 주로 하는 전통적인 기업들의 주가보다 더 하락한다는 것은 2002년도에 서비스 공격으로 인하여 인터넷 기업들의 주가가 다른 기업들의 주가에 비하여 2.8% 더 하락하였다는 사실에서도 알 수 있다[8]. 또한 이러한 사실은 66개의 사이버공격 사례에 대한 조사에서도 인터넷 기업들의 주식가격이 사이버공격 직후 다른 기업들의 주가보다 평균 5% 더 하락하였다는 조사결과를 통하여도 알 수 있다[7][9].

순수 인터넷 기업에 대한 사이버 공격으로 인한 주가 하락의 대표적인 사례는 지난 1999년의 eToys 사건을 들 수 있다. 세계 최대의 온라인 인형·완구 판매업체인 e-Toys가 해커의 공격을 받아 웹 사이트 접속속도가 현저하게 둔화되어 고객들이 접속을 포기하는 경우가 속출하였다. 더구나 eToy가 해커들에 의하여 마비되었다는 소식이 전해지면서 이 회사 주가가 하루 만에 주당 45달러에서 39달러로 15%나 하락하였다. 하지만 순수 인터넷 기업은 자신들의 취약성을 충분히 인지하고 사이버 공격에 대비하고 있기 때문에 그 피해를 감소시켜 나갈 가능성도 가지고 있다.

---

5) Huseyin Cavusoglu, Birendra Mishra, Srinivasan Raghunathan, 'The Effect of Internet Security Breach Announcements on Market Value : Capital Markct Reactions for Breached Firms and Internet Security Developers', *International Journal of E-Commerce*, 2002년. 이 연구는 1996부터 2001년 사이에 발생한 66개의 각기 다른 특성을 보여주는 사이버 공격사례를 조사하여 사이버공격이 주가에 미치는 영향에 대해 연구하였다.

6) 그러나 오늘날 대부분의 기업들이 인터넷 홈페이지를 운영하면서 기업 홍보와 채용 및 일부 계약 등을 처리하고 있기 때문에 오프라인 활동만 전적으로 하고 있는 기업들은 거의 찾아보기 힘들다고 할 것이다.

7) Michael Ettredge, Vernon J. Richardson, 'Assessing the Risk in E-Commerce', *Proceedings of the 35th Hawaii International Conference on System Sciences*, 2002년. 이 논문에서 2002년 2월에 서비스거부 공격의 인터넷 기업들에 대한 영향력을 연구하였다.

3.3 사이버공격 발생 이후 3일 이내의 주가 변화[8]

사이버공격 발생 직후 주식시장은 가장 민감하게 반응할 것이고 시간이 지나면서 기업들이 정보 및 정보시스템을 복구하고 사이버 공격에 대하여 대응을 하기 때문에 주가는 회복될 것이라고 생각된다.

그러나 사이버공격 발생 이후 3일 동안의 주가 변화는 이러한 예상과는 다르게 나타났다. 즉, 1996년부터 2002년 사이에 미국에서 발생한 22건의 사이버 공격으로 인해 영향을 받은 기업들은 공격 다음날 다른 기업들에 비해 2.7%의 주가 하락을 경험하였으나 공격 발생 3일 후 이들 기업의 주가는 다른 기업들에 비하여 4.5% 하락하였다[10]. 또한 1995년부터 2000년까지 마이크로소프트, 콤팩, 뉴욕 타임즈, 보잉, AT&T, GE, 노스웨스트 항공 등 미국의 상장 기업들을 상대로 서비스 거부 공격, ILOVEYOU 바이러스, Melissa 바이러스, 웜 및 무단침입 등 43건의 사이버 공격 가운데 38건의 사이버 공격이 기업들에게 악영향을 미쳤으며 사이버 공격 후 3일 동안 이들 기업들의 주가가 큰 폭으로 하락하였다[11]. 결국, 사이버공격 후 3일 동안 주가는 계속 하락하는 것으로 조사되었다.

3.4 사이버공격 유형과 내용에 따른 주가변화

기술의 발전과 더불어 사이버공격도 지능화·첨단화되고 다양화되고 있다. 웜·바이러스 공격, 서비스 거부 공격, 불법 접근 등을 포함한 다양한 공격이 나날이 발전하고 있다. 사이버공격으로 인한 주가의 변동은 그 공격 유형에 따라서 다소 차이를 보이고 있다. 즉, 웹사이트 외관변조의 경우 평균 주가 하락은 이틀째에 2%였고 3일째는 1.1%로 나타났다. 그러나 서비스 거부 공격에 의해서는 이틀째에 2.9% 하락을 초래했고 3일째는 3.6%의 하락을 보여주었다. 또한 기업의 일반 정보에 대한 공격의 경우 공격 당일 주가는 평균 0.5% 하락한 반면에 3일째는 총 1.5% 하락하였다. 이는 서비스 거부 공격 보다 낮은 수치이다. 그러나 신용카드 정보와 같은 기업의 기밀정보를 침해한 공격의 경우 주식가치에 대하여 가장 큰 손실을 초래하였다. 즉, 이러한 공격 당일 영향을 받은 기업들의 주가는 평균 9.3% 하락했고 3일째는 14.9%에 이르렀다.[12].

따라서 사이버 공격의 유형은 주가변화와 크게 상관이 없는 반면에 사이버 공격으로 인하여 기업의 기밀 정보에 대한 접근이 있는 경우에는 주가가 크게 하락하였다. 이는 고객들이나, 주주 등이 서비스 거부 공격이나 웜·바이러스 등과 같은 사이버공격들을 일상적인 위험이나 영업비용의 일부로 인식하고 있지만, 기밀정보가 외부에 노출되었다는 것에는 민감하게 반응하기 때문이다. 또한, 사이버공격으로 기업의 기밀정보에 대한 무단 접근이 발생하면 기업에 대한 지속적인 피해 가능성이 높다고 인식되기 때문이다. 그러나 기업의 기밀정보에 대한 접근이 없는 사이버공격들은 기업의 장기 수익성 등에 대하여 별다른 영향을 주지 못하는 것으로 인식되어 주가에 거의 영향을 주지 못하였다.

3.5 1.25인터넷 대란과 우리나라 주식시장의 영향

위에서 논의된 모든 결과를 종합하면 순수 인터넷 기업이 사이버 공격으로 인하여 주가가 가장 많이 하락하였으며 사이버 보안 관련 기업들의 주가는 오히려 상승하였다는 사실을 명백하게 알 수 있다. 이러한 사실을 고려하여 우리나라 1.25 인터넷 대란 이후의 주가 변동을 살펴보기로 한다. 우선 기업 유형을 순수 인터넷 기업, 인터넷과 오프라인 활동을 병행하는 통신사업자 업체, 오프라인 기업 및 정보보안 기업으로 분류하고 대표적인 기업 각 2곳을 선정하여 1.25 인터넷대란이 발생하기 전인 1월 24일의 주가와 1월 27일의 주가를 단순 비교해 보기로 한다.

"NHN"과 "다음"과 같은 순수인터넷기업은 1.25인터넷대란이 있기 전인 24일 대비 동 사건 이후 열린 27일 주식시장에서 각각 2,200원(4.1%)과 1,150원(2.98%) 하락한 것에 비하여 정보보안기업인 안철수연구소와 인젠의 경우는 각각 15,200원에서 17,000원으로 11.8%, 2,560원에서 2,860원으로 11.7%나 급등하였다. 따라서 사이버 공격으로 인하여 정보보안 기업의 주가가 상승한다는 사실은 1.25 인터넷 대란을 통하여도 알 수 있다.

〈표 2〉 1.25 인터넷 대란과 주요기업의 주가변동

구분	기업명	24일	27일	비율(%)
순수 인터넷	NHN	53,700	51,500	-4.09
	다음	38,500	37,350	-2.98
통신사업자	(주) KT	50,050	49,050	-1.99
	데이콤	13,400	12,750	-4.85
오프라인	현대자동차	25,550	25,100	-1.76
	현대중공업	20,500	19,850	-3.17
정보보안기업	안철수연구소	15,200	17,000	+11.8
	인젠	2,560	2,860	+11.7

1.25 인터넷 대란의 직접 당사자인 (주)KT의 경우 24일 50,050원에서 27일 49,050원으로 1.99% 하락하였으며 같은 통신사업자인 데이콤의 경우 13,400원에서 12,750원으로 4.85%나 하락하였다. 그러나, 오프라인 기업이라고 할 수 있는 현대자동차의 경우 25,500원에서 25,100원으로 1.76%하락하였다. 그렇지만 같은 오프라인 기업이라고 할 수 있는 현대중공업의 경우는 20,500원에서 19,850원으로 3.17% 하락하였다.

1.25 인터넷 대란 직후 순수 인터넷 기업, 통신사업자 및 오프라인 사업자가 평균 3.14% 하락한 반면에 우리나라 대표적인 정보보안 기업은 11.8% 상승하였다. 또한 순수 인터넷기업이라고 할 수 있는 NHN과 다음이 평균 3.535% 하락한 반면 데이콤과 (주)KT 등의 통신사업자가 평균 3.42%, 오프라인 기업이 평균 2.465% 하락하였다. 이러한 사실에 비추어 볼 때 1.25 인터넷 대란 이후 순수 인터넷 기업의 주가가 다른 기업들에 비하여 더 하락하였다는 사실을 알 수 있다.

8) Ettredge와 Richardson에 의하면 3일이 넘어가면 주가변화가 다른 사건으로 인해 영향을 받을 가능성이 커지게 된다고 한다. 따라서 다른 요소를 배제하고 사이버 공격을 직접적인 원인으로 한 주가변동의 결과를 알 수 있는 시간은 사이버 공격발생 이후 3일 이내라고 한다.

그러나, NHN의 경우 1.25 인터넷 대란이 토요일 오후 인터넷 시간이 뜸한 시간대에서 발생하였기 때문에 피해규모가 크지 않아서 4.09%의 하락에 머무른 것으로 파악되고 있다. "다음"의 경우 1.25 인터넷 대란이전에 이미 서비스 지연 사고를 겪고 있었기 때문에 2.98% 하락에만 그친 것으로 파악되고 있다. 그렇지 않았을 경우 하락 폭은 더 컸을 것으로 생각된다. 결과적으로 1.25인터넷 대란 전후로 조사대상 6개 업체가 평균 3.14%의 주식 하락을 경험한 것으로 파악되었다.

그러나 이 통계치를 근거로 우리나라 1.25 인터넷 대란으로 주가가 평균 3.14% 하락하였다고 주장하기에는 다소 섣부른 감이 있다. 1.25 인터넷 대란과 우리기업들의 주가 하락과의 인과관계에 대한 보다 깊이 있는 고찰이 필요하다. 즉, 2003년 1월 27일의 주가하락에 있어 1.25 인터넷 대란 이외의 다른 요인이 있었는지를 고려하고 우리 기업 전체에 대한 통계자료를 통하여 1.25 인터넷 대란이 우리 주식시장에 미친 영향을 보다 면밀하게 분석할 수 있을 것이다.

4. 사이버 공격에 대응하기 위한 기업의 책임 규정을 위한 정책적 제안

사이버공격으로 인하여 기업은 평판이나 신뢰도에 대하여 부정적인 영향을 받게 된다. 즉, 사이버공격은 기업의 신뢰성에 대하여 의문을 제기하게 만들어 고객의 신뢰를 상실하게 한다. 이로 인하여 경쟁기업이 경쟁우위를 점할 수 있다[5]. 또한 주식시장과 채권시장의 부정적 반응으로 인하여 기업의 자본비용도 늘어나게 된다. 그 결과 기업은 비용이 증가하게 되고 이익이 감소하게 되어 손실이 발생하고 궁극적으로는 주주 등에게 손해가 발생하게 된다. 따라서 기업의 정보보호 책임을 규정하는 것이 사이버 공격으로부터 기업과 주주의 이익을 보호하고 사이버 공격으로 인한 사회경제적 부담을 경감시켜줄 것으로 기대된다.

이와 관련하여 미국은 지난 2002년 "상장 기업 감사와 투자자 보호법(the Public Company Accounting and Investor Protection Act of 2002"을 통과 시켰다. Sarbanes-Oxley Act라고도 불리는 이 법은 "상장 기업 감사 감독위원회(the Public Company Accounting Oversight Board(PCAOB)"의 설립을 규정하고 있을 뿐만 아니라 이 법 제404조에서 내부통제(internal control)를 규정하고 있다[13]. 내부통제라는 것은 기업의 재정에 대한 정확한 보고가 적절하게 보호되었다는 것을 확인하는 절차와 과정을 의미하는 것이다. 이는 기업의 재정에 대한 보고가 정보시스템에 의존하고 있는 대부분의 미국 기업들에 대하여 정보시스템에 대한 적절한 보호와 그 보호 절차를 확립할 책임을 부과한 것으로 파악되고 있다[14].

사이버 공격으로 인하여 기업의 피해 비용이 증가하고 있으며 사이버 공격으로 인한 주가 하락으로 사회 경제적인 손실이 발생하고 있다. 이러한 사회 경제적 비용에 효율적으로 대처하기 위해서 우리나라도 미국의 "상장 기업 감사와 투자자 보호법"과 같은 특별법을 제정하여 기업들에 대한 감사에 있어 컴퓨터와 정보시스템에 대한 적절한 보호와 방법을 명시하고 이를 감독하도록 하여야 할 것이다. 아울러 감사와 관련하여 내부통제 관련 규정을 삽입하여 기업의 이사와 고위 간부들로 하여금 기업의 정보보호 관련 절차와 방법을 확립하도록 하여야 한다. 나아가 이를 소홀히 하여 사이버공격으로 인한 손해를 발생하게 한 기업의 이사와 고위 간부들에 대하여 피해를 본 회사와 주주들이 손해 배상을 청구할 수 있는 적극적인 법적 수단을 확보해주는 방안도 고려해 보아야 할 것이다.

5. 결 론

이상에서 사이버공격으로 인한 피해 비용을 산정하는 것이 매우 곤란한 작업임을 파악하였다. 또한 사이버 공격으로 인한 비용도 자연재해나 화재 등과 같이 사회가 분담하여야 할 일종의 비용이라고 인식하게 되었다. 그러나 특정분야와 일부 기업에 있어서 사이버공격으로 인한 비용을 측정할 수 있다면 어느 정도의 정보보안 예산을 투입하는 것이 바람직할 것인가를 가늠해 볼 수 있을 것이다.

또한 사이버공격이 주가에 미치는 영향을 살펴보았다. 사이버공격으로 순수한 인터넷 기업의 주식이 가장 크게 하락하였으며 사이버 공격 후 3일 이내까지는 대부분의 주식이 하락하였다. 사이버공격의 유형은 주식에 크게 영향을 미치지 않았으나 사이버 공격으로 인한 기밀자료의 유출로 인하여 주식 가치는 크게 하락하였다.

이와 같이 사이버 공격으로 인하여 기업의 피해 비용이 증가하고 있으며 주가 하락을 불러오고 있다. 이러한 상황에 효율적으로 대처하기 위해서는 각 기업의 이사와 고위 간부들에게 정보보호의 중요성을 인식하고 이를 실행하기 위한 구체적인 절차와 과정을 확립하도록 하는 것이 필요하다.

참 고 문 헌

[1] 정보화 대국 구멍 뚫렸다, 한국일보 2003년 1월 27일.
[2] 삼성경제연구소, 인터넷강국의 취약성과 대응과제, CEO Information, 2003년 2월 5일.
[3] 2005 CSI/FBI 컴퓨터 범죄와 보안에 관한 설문 조사.
[4] 2003 CSI/FBI 컴퓨터 범죄와 보안에 관한 설문 조사.
[5] 미국 의회조사국, 사이버공격의 경제적 효과, 2004년 4월.
[6] Mi2g, *FAQs : SIPS and EVEDA, v1.00,* 2004년2월6일.
[7] 국가정보원, 2003년 국가정보보호백서, 2003년 5월.
[8] Huseyin Cavusoglu, Birendra Mishra, Srinivasan Raghunathan, 'The Effect of Internet Security Breach Announcements on Market Value : Capital Market Reactions for Breached Firms and Internet Security Developers', *International Journal of E-Commerce,* 2002년.

[9] Michael Ettredge, Vernon J. Richardson, 'Assessing the Risk in E-Commerce', *Proceedings of the 35th Hawaii International Conference on System Sciences*, 2002년.

[10] Ashish Garg, Jeffrey Curtis, Hilary Halper, 'Quantifying the Financial Impact of IT Security Breaches', *Information Management & Computer Security*, vol. 11, no. 2. 2003년 4월 2일.

[11] Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, Lei Zhou, 'The Economic Cost of Publicly Announced Information Security Breaches : Empirical Evidence From the Stock Market', *Journal of Computer Security*, 제11권, 3호, 2003년.

[12] Fred H. Cate, "Information Security Breaches and the Threat to Consumers", 2005년 9월.

[13] Reed Warner, Information Security and Section 404 of the Sarbanes-Oxley Act, 2004년 12월 16일.

[14] R. Mark Halligan, Duty to identify, Protect trade secrets has arisen, *The National Law Journal*, 2005년 8월 29일.

오 일 석

e-mail : i-oh2005@law.northwestern.edu
1994년 한국외국어대학교 영어과
1997년 고려대학교 대학원 법학과(법학석사)
2001년~2005년 한국전자통신연구원 부설 국가보안기술연구소 선임연구원
현 재 미국 노스웨스턴대학교 법과대학 L.L.M 과정
관심분야 : 정보보호 정책 및 법제도, 개인정보보호, 불법행위법

이 석 윤

e-mail : syunlee@imtl.skku.ac.kr
1988년 인하대학교 산업공학과
1991년 KAIST 산업공학과(공학석사)
현 재 성균관대학교 정보통신공학부 박사과정
관심분야 : 정보보호 정책 및 법제도, 개인정보보호