정보보안 사고와 사고방지 관련 투자가 기업가치에 미치는 영향

The Effect of Information Security Breach and Security Investment Announcement on the Market Value of Korean Firms

권 영 옥 (Young Ok Kwon) 미네소타대학교 경영대학 박사과정
김 병 도 (Byung-Do Kim) 서울대학교 경영대학 경영학과 교수, 교신저자

요 약

최근 인터넷의 급속한 발전과 기업의 정보 인프라 의존도가 높아지면서 정보 유출과 탈취, 변조 등 침해사고의 위험성이 급속히 확산되고 있다. 우리나라의 인터넷 사용빈도는 세계 최상위 수준이지만 정보보안은 그에 미치지 못하는 실정이다. 우리나라의 많은 기업들이 정보보안 사고로 인해 금전적 손실, 기업 이미지 훼손, 매출액, 순이익 감소 등 직간접적 피해를 경험하고 있다. 그러나 정보보안 사고에 대한 피해 규모를 계량화한 자료가 없어 올바른 정보보안사고 방지를 위한 투자의사 결정을 하기 어렵고 투자의 효과를 평가하기도 어려운 실정이다.

본 연구의 목적은 정보보안 사고에 따른 기업의 손실과 보안 투자로 인한 수익을 기업 시장가치의 변화를 이용하여 정량적으로 측정하는 데 있다. 사건연구방법론을 통해 분석한 결과에 따르면, 기업의 정보보안 사고는 평균 0.86%의 기업 가치 감소(시가총액 기준으로 약 540억)를 가져온 것으로 나타났다. 반면 기업의 보안 관련투자는 기업가치에 아무런 영향을 주지 않는 것으로 나타났다. 추가적으로 본 연구와 해외 연구결과와 비교해 보면, 국내 기업의 정보보안 사고가 기업 가치에 미치는 영향력이 상대적으로 매우 작은 것을 알 수 있었다. 이는 사회 전반에 걸친 보안 의식 제고가 무엇보다 시급함을 시사하고 있다.

키워드 : 사건연구, 정보보안, IT보안, 정보보안사고, 투자수익률

Ⅰ. 서 론

컴퓨팅 기술과 네트워킹 기술의 지속적인 발전은 인터넷의 폭발적인 성장을 가져왔으며 사회 전반에 걸친 기반시설 및 공공 인프라, 그리고 산업 인프라 및 문화환경을 인터넷 기반으로 변화시키는 중요한 역할을 수행했다. 하지만 인터넷의 발전과 정보 인프라의 의존도가 높아지면서 개인 정보 유출과 탈취, 변조 등 침해사고의 위험성이 급속히

† 본 연구는 서울대학교 경영대학 경영연구소에서 지원한 연구비로 수행되었음.

확산되고 있다. 특히 온라인이나 인터넷상에서의 상거래가 기업의 중요한 일상적인 활동으로 자리 잡아가고 있는 시점에서 기업들은 보안 사고로 인해 수많은 위험과 위협에 심각하게 노출되어 있어 우려하는 목소리가 높다. 보안 사고가 발생하면 기업은 단기적으로 사고 복구를 위한 막대한 비용을 지불해야 하는 것 외에도, 장기적으로 보안 사고 사실이 미디어에 공개되어 고객의 신뢰를 잃게 되고 결국 기업 이미지가 크게 실추된다.

우리나라는 2003년 인터넷대란 이후 정보보안에 대한 사회적 관심은 높아지고 있지만 정작 정보보안에 필요한 솔루션 도입 수준은 여전히 낮다. 대한상공회의소가 전국 243개 기업을 대상으로 조사한 '기업의 정보보안 위기관리 현황(2003)'에 따르면 정보보안을 위한 위기관리를 아예 하지 않거나 초보적인 수준에 머물러 있는 기업이 68.3%에 달했다. 또한 정보보안을 위해 위기관리 전담조직을 두고 있는 기업은 19.7%에 불과했다. 특히 응답업체의 69.5%는 과거 정보보안 관련 사고를 경험했음에도 기업들이 정보보안 사고에 무방비 상태로 노출된 것으로 분석됐다. 유사한 예로 선진국 은행들은 전체 IT 투자금액의 약 10%를 보안관련 예산으로 책정하는 것과는 달리 우리나라 주요 은행들은 2003년 1~3% 정도의 예산을 보안에 투자하고 있다고 한다(서울경제 2003). 인터넷뱅킹이 이미 전체 금융거래의 20~30% 이상을 차지하고 있는 것에 나라에서 이 정도밖에 보안에 투자하지 않는다는 것은 이해하기 어렵다.

우리나라 기업들이 정보보안에 대한 투자에 상대적으로 인색한 이유는 우리 사회 저변에 깔려 있는 정보보안 불감증에 기인한 바가 클 것이다. 이 문제를 근본적으로 해결하기 위해서는 정보보안의 위협요인[1]과 보안관리 실패로 발생하는 보안 사고의 피해 규모에 대한 정확한 이해와 평가가 있어야 한다. 예를 들어 보안사고에 대한 객관적인 피해 규모 산정기준이 없다면 동일한 보안사고에 대해 기업마다 다른 기준을 적용하여 피해 규모를 산정 및 발표할 것이고, 그 결과 피해규모가 과대 또는 과소 평가될 가능성이 클 것이다. 보안사고로 인한 피해규모가 정확히 파악되지 않기 때문에 우리나라 기업은 정보보안 관련 투자에 인색할 수밖에 없는 것으로 보인다.

본 연구의 목적은 우리나라 기업의 정보보안 사고로 인한 손실과 보안 투자의 가치를 정량적으로 측정하는 데 있다. 사건연구방법론(event study)을 통해 분석한 결과, 우리나라 기업의 정보보안 사고는 평균 0.86%의 기업 가치 감소(시가총액 기준으로 약 540억)를 가져온 것으로 나타났다. 반면 우리나라 기업의 보안 관련투자는 기업가치에 아무런 영향을 주지 않는 것으로 나타났다. 본 연구 결과와 해외 연구결과와 비교해 보면 국내 기업의 정보보안 사고가 기업 가치에 미치는 영향력이 상대적으로 매우 작았다.

우리는 다음 장에서 정보보안 사건을 정의하고 관련 연구와 본 연구가 어떤 점에서 다른가를 설명한다. 다음으로 국내 상장기업의 정보보안 사고 및 보안투자 관련 사건 데이터를 수집한 방법과 수집된 데이터의 특성을 설명한다. 다음 장에서는 59건의 정보보안 사고 사건과 107건의 보안관련 투자 사건에 사건연구 방법론을 적용한 결과를 분석하고, 마지막으로 본 연구의 결론과 미래 연구방향을 제시한다.

Ⅱ. 정보보안 관련 연구

2.1 정보보안의 정의

정보보호(information security) 또는 정보보안이란 일반적으로 고의, 과실, 재해 등에 의해

1) 정보보안의 위협요인의 유형 및 분류에 대해서는 Loch, Carr and Warkentin (1992)의 연구에서 잘 다뤄져 있다. 그들은 위협요인을 내부/외부적 위협, 인간/비인간적 위협, 사고/의도적 위협으로 분류하고 있다. 그들의 연구모형에 따르자면 본 연구는 위협요인의 결과(consequence)인 정보보안사고의 비용을 측정하는 데 그 일차적 목표가 있다고 할 수 있다.

정보시스템이 고장 및 파괴되는 등의 위해를 막기 위한 물리적/논리적 대응을 말한다. 본 연구에서는 우연히 발생하는 자연재해나 사람의 실수에 의한 사고를 제외하고 고의적으로 발생하는 사고만을 대상으로 하고자 한다. 즉 정보보안을 조직 내의 중요한 정보를 스파이, 비양심적인 내부자, 호기심 많은 내부자, 인터넷 상의 악질적인 해커로부터 보호하는 것으로 정의할 수 있다.

전세계적으로 정보보안 사고는 최근 4년 사이에 10배 이상 증가하였다(CERT/CC Statistics 2005). 국내에서도 정보보호진흥원의 인터넷 침해사고대응센터에 접수된 신고 건수를 보면 2001년 5333건, 2002년 1만5192건, 2003년 2만6179건으로 매년 해킹 관련 피해가 급증하고 있는 것으로 나타났다. 즉 급속히 증가하는 사이버 테러, 해킹 등 정보기술 관련 위협요인으로 인해 정보보안 사고가 더 이상 간과될 수 없는 중요한 경영문제로 대두되고 있음을 보여주고 있다.

국제 정보시스템 보안 인증 컨소시엄(International Information Systems Security Certification Consortium)의 CBK(Common Body of Knowledge) 가이드에 따르면, 정보보안 사고는 정보보안의 목적에 따라 기밀성, 무결성, 가용성의 세가지로 나눌 수 있다. 기밀성(confidentiality)이 침해되는 경우는 정보의 소유자(개인/조직)가 원하는 대로 정보의 비밀이 유지되지 않고 인가되지 않은 자에 의해 정보가 노출되는 경우를 말한다. 예를 들면 기술 노하우나 원가정보 등이 경쟁 회사에 알려지는 경우이다. 무결성(integrity)이 침해되는 경우는 비인가자에 의해 정보가 변경, 삭제 및 생성되는 위험을 말한다. 오류 정보를 이용하여 정보처리를 하거나 이를 기초로 경영층이 잘못된 의사결정을 수행할 경우 발생하는 위험을 말한다. 가용성(availability)이 침해되는 경우는 정보나 정보서비스를 필요한 때에 얻을 수 없게 되는 위험을 말한다. 정보서비스의 사용 불능, 지연 등으로 고객에 대한 서비스 중단이나 업무 중단이 발생하는 위험을 말한다.

2.2 관련 연구

본 연구의 목적은 정보보안 사고와 보안관련 투자 효과를 정량적으로 측정하는 데 있다. 우리나라와 달리 미국에서는 지난 2000년 2월 Amazon .com, eBay, Yahoo 등 유명한 전자상거래 사이트들이 2일 동안 지속적으로 DDoS(Distributed Denial of Service, 분산 서비스 거부)라는 DoS[2]의 변종공격을 받아 사이트 운영이 불가능해진 사건을 계기로 정보보안 사고 효과를 측정하려는 연구들이 활발하게 진행되었다.

Ettredge and Richardson(2002)의 논문은 보안사고로 인한 기업가치 하락 정도를 사건연구로 측정한 최초의 연구이다. 그들은 2000년 2월 해커들의 DoS공격이 해당 기업의 주가에 어떤 반응을 미치는가를 조사하였는데, 전통기업보다 인터넷기업의 피해가 훨씬 더 심각하다는 사실을 밝혔다. Bharadwaj and Keil(2001)은 정보보안 사고를 포함한 IT 관련 사고가 기업가치를 현저히 떨어뜨린다는 사실을 발견하였다. Campbell, Gordon, Loeb and Zhou(2003)는 정보보안 사고의 종류에 따라 기업가치에 미치는 영향이 상이함을 보였다. 즉 기밀성 침해 사건의 결과 기업가치는 현저히 떨어졌지만 다른 종류의 정보보안 사고는 주가에 아무 영향을 미치지 않았다. Cavusoglu, Mishra and Raghunathan(2004a)은 1996년부터 2001년까지 발생한 미국 기업의 인터넷 침해 사고 66건에 대해 사건연구를 실시한 결과 사고 발표일과 다음날 이틀 동안 평균 2.1%(시장가치로 환산하면 약 17억 달러)의 주가가 감소됨을 보였다. 정보보안 사고와는 달리 정보보안 관련 투자의 경제적 효과를 측정한 연구는 거의 찾아볼 수 없다. 아마도 이 주제와 가장 가까운 논문은 Dos Santos, Peffers and Mauer(1993)의 연구로, 그들은 사건

2) DoS는 한 사용자가 시스템의 리소스를 독점하거나 모두 사용, 또는 파괴함으로써 다른 사용자들이 시스템의 서비스를 올바르게 사용할 수 없도록 만드는 것을 말한다.

연구를 사용하여 IT 투자가 기업가치에 미치는 효과를 측정한 결과 창의적인 IT투자만이 기업가치를 증대한다는 사실을 발견하였다. 이들의 논문은 정보보안 관련 투자 자체를 연구한 것은 아니지만 정보보안 투자가 IT투자에 일부를 구성한다는 점에서 본 연구와 어느 정도 관련성이 있다고 볼 수 있다. 한편 Cavusoglu, Mishra and Raghunathan (2004b)은 IT 보안 투자의 가치를 측정할 수 있는 모델을 제시하였다. 이들은 IT 보안 인프라를 방화벽(firewall), 침입탐지시스템(IDS, intrusion detection system), 모니터링(manual monitoring)의 보안 단계로 나누고 각 단계에 필요로 하는 보안 기술 비용과 해킹을 당할 확률을 이용하여 보안 투자로 인한 투자수익률을 산정하였다.

본 연구는 기존 연구와 다음 세 가지 점에 있어 다르다. 첫째, 본 연구는 2001년부터 2005년까지 5년 동안 국내 기업에서 발생한 정보보안 사고와 보안관련 투자의 경제적 효과를 사건연구 방법론으로 측정했다는 점이다. 즉, 본 연구는 국내기업의 정보보안 사고 및 보안관련 투자 사건이 기업가치에 미치는 영향을 정량적으로 측정한 최초로 시도한 논문이라는 것이다. 둘째, 사건연구 방법론을 통해 정보보안 사고의 경제적 손실을 정량적으로 측정한 기존 연구는 몇 편 있지만, 사건연구 방법론을 적용해 정보보안 관련 투자의 경제적 효과를 측정한 논문은 없다. 즉, 본 연구는 사건연구 방법론을 이용해 정보보안 관련 투자가 기업가치에 미치는 영향을 정량적으로 측정한 최초의 논문이라는 점이다. 셋째, 정보보안 사고의 범위를 인터넷 침해 사고뿐 아니라 내부 직원이나 이직 직원에 의한 첨단 기술 유출과 같은 사고까지 포함한다는 점이다. 즉, 정보보안 사고의 종류에 따라 기업가치에 미치는 영향이 다를 수 있다는 사실을 인식했다는 점이다.

2.3 사건연구

사건연구(event study)는 어떤 사건이 발생하거나 특정 정보가 시장에 공시되었을 때 그 사건으로 인한 주가변화를 측정하는 연구 방법론이다. 사건연구 방법론은 시장의 효율성을 연구하던 재무 이론가들에 의해 처음 개발되었다(Fama, Fisher, Jensen and Roll 1969). 효율적인 시장에서 주가(stock price)는 기업이 현재 보유하고 있는 자산으로부터 기대할 수 있는 미래 현금흐름을 현재가치로 환산한 값이다. 효율적인 시장에서 어떤 한 시점의 주가는 기업의 현재 및 미래의 이익에 영향을 미치는 모든 정보를 반영하고 있다. 그리고 예상하지 못한 사건이 발생하고 그 새로운 사건 정보가 기업의 현재 및 미래 수익에 영향을 미칠 것이라면, 이 정보는 주가에 즉시 반영된다. 그러므로 우리는 주가변화의 관찰을 통해 기업가치 변화를 측정할 수 있다. 즉 어떤 특정 사건발생 전후의 주가 변화를 측정함으로써 그 사건의 경제적 가치를 정확하게 측정할 수 있다는 것이다(Brown and Warner 1985).

사건연구는 주식분할(stock split)이 주가에 미치는 영향을 분석한 연구를 시작으로(Fama *et al.*, 1969) 경제학, 회계학, 재무, 전략, 조직, 마케팅 등 다양한 분야의 여러 문제에 적용되었다. 최근에는 정보시스템 관련 분야에도 사건연구가 성공적으로 적용되었다. IT 투자(Dos Santos, Peffers and Mauer, 1993; Im, Dow and Grover, 2001), 정보보안사고(Ettredge and Richardson, 2001; Campbell, Gordon, Loeb and Zhou, 2003; Cavusoglu, Mishra and Raghunathan, 2004), CRM 투자(김병도, 김지경, 우상진, 2004)가 기업가치에 미치는 영향 등이 그 대표적 예들이다.

어떤 사건이 기업가치에 미치는 영향을 조사하기 위해서 우리는 비정상 수익률(abnormal return)을 측정해야 한다. 비정상 수익률이란 통상적인 시장의 움직임으로 인한 것 이상의 주가변화를 말한다. 비정상수익률은 정상수익률(normal return)을 측정하기 위해 사용할 기준모델(benchmark model)로 어떤 모형을 선정하는지에 따라 달라질 수 있다. 본 연구에서는 시장모형(market model)을 기준모델로 사용했다. 시장모형은 다양한 시장 여건 하에서 기준모

델의 역할을 성공적으로 수행한 것으로 평가 받고 있다(Brown and Warner, 1985).

Ⅲ. 국내기업의 정보보안 사고와 사고 방지 관련 투자

본 연구에서 사건 일(event day)은 중요 일간지에 정보보안 사고 또는 사고방지 관련 투자 사실이 처음 발표된 날짜로 정의한다. 우리의 관심은 사건 일을 전후한 주가 변화이므로 검색 범위를 거래소(KOSPI)와 코스닥(KOSDAQ)에 상장된 기업으로 제한하였다. 주가 자료는 KIS-FAS/SMAT와 Fnguide.com에서 제공하는 개별 종목 일별 시계열 자료를 사용하였다. 또한 시장모형으로는 거래소 상장기업의 경우 종합 주가지수, 코스닥 등록 기업의 경우는 코스닥 지수를 사용하였다.

정보보안 사고 및 투자 사건은 KINDS(Korea Integrated News Database System)와 네이버 뉴스 검색 사이트에서 2001년 1월1일부터 2005년 3월 31일까지의 뉴스 기사 중 키워드 검색을 통해 도출되었다. 사건 일은 국내 10개 종합 일간지(경향, 국민, 동아, 문화, 세계, 연합뉴스, 조선, 중앙, 한겨레, 한국일보), 9개 경제 일간지(머니투데이, 매일, 서울, 제일, 한국, 헤럴드, 스탁데일리, 파이낸셜뉴스, 이데일리)와 4개 IT전문 신문(디지털타임스, 전자신문, 아이뉴스24, ZDNet Korea)에 실린 기사들 중에서 해당 기업의 이름이 정확히 명시된 기사만을 고려 대상으로 삼았다. 보안 사고에 대한 검색 키워드로는 '해킹', '공격', '인터넷 침해', '기술 유출', '정보 유출', '데이터 변조', '홈페이지 변조', '보안 사고', '사이버 범죄' 등을 사용하였고 보안 투자에 대한 검색 키워드로는 '보안 투자', '보안 솔루션', '보안 서비스', '보안 컨설팅' 등을 사용하였다.

하나의 기사에 여러 기업의 이름이 동시에 게재된 경우 각 기업별로 사건이 발생한 것으로 보았고, 같은 내용의 기사가 여러 신문에 발표된 경우 가장 먼저 발표된 기사를 최종 표본으로 선정하였다. 사건 일은 사건 기사가 발표된 날로 하되, 석간신문이나 주식거래일이 아닌 날 발표된 기사의 경우 기사 발표일 이후 최초 주식거래일로 정했다. 또한 다음 조건에 해당하는 기사는 연구 대상에서 제외되었다.

(1) 사건 발생일 2주 전부터 과거 1년 동안의 주가 자료를 얻을 수 없는 경우
(2) 과거 1년 동안의 주가 자료를 통해 추정한 베타값이 유의하지 않은 경우
(3) 본 연구의 대상 사건 외 다른 중요한 사건이 사건 연구 기간에 발생한 경우
(4) 한 기업 내에서 사건이 2주 미만 간격으로 연속적으로 발생한 경우

(1)의 경우 데이터 부족으로 비정상 수익률 도출을 위한 시장모형 추정이 불가능하였기 때문에 표본에서 제외하였다. (2)의 경우는 추정된 베타값이 유의하지 않으면 도출된 비정상 수익률이 무의미하기 때문에 표본에서 제외한 경우에 해당한다. (3)의 경우는 연구의 대상이 되는 사건과 관련 없는 중요한 사건이 사건 연구기간 내에 발생하면 순수한 '보안 사고' 또는 '보안 투자'에 대한 효과를 측정하기 어렵기 때문에 표본에서 제외하였다. (4)의 경우는 앞의 사건이 다음 사건에 영향을 미칠 가능성이 존재하기 때문에 표본에서 제외한 경우이다. 2001년부터 2005년 3월까지 국내에는 많은 보안 사고 및 보안 투자 기사가 발표됐지만, 총 59건의 보안 사고와 총 107건의 보안 투자가 위 조건을 충족하였다.

<표 1>은 총 59건의 보안 사고 사건을 연도별로 요약한 표로, 보안 사고 건수는 매년 꾸준히 증가하고 있는 추세라는 사실을 확인할 수 있다. 한편 <표 2>는 보안 사고가 기사화된 기업을 산업별로 분류한 표이다.[3] 전기, 전자, 통신을 포함한 IT 관련 기업이 전체 표본의 81.4%로 대부분을 차

<표 1> 보안사고의 연도별 분포

연도	사고 건수
2001	6
2002	9
2003	18
2004	18
2005 Q1	8

<표 2> 사고기업의 산업별 표본 분포

산업 구분	사고 건수
은행/금융/증권	9
IT종합/서비스	24
통신업/전기/전자	24
유통/제조업/기타	2

지하였고, 다음으로 금융 관련 기업이 15.4%를 차지하였다. 또한 인터넷 기업의 보안 사고는 12건으로 20.3%를 차지하였다. 한편 연구에 포함된 보안 사고를 유형별로 분류한 결과 전체 보안사고의 79.7%가 정보 유출 관련 사고였고, 64.4%가 인터넷 관련 사고였다.

<표 3>은 연구에 포함된 사고 기업들의 기술 통계량을 요약한 표이다. 사고 발생 기업의 평균 시가 총액은 6조 2,830억, 평균 당기 순이익은 5,821억, 매출액은 6조 122억이었다. 매출액 규모가 가장 작은 기업은 165억 원의 매출을 달성한 데 비해 매출액이 가장 큰 삼성전자는 이의 2,000배에 해당하는 34조 2,838억 원의 매출을 보여 표본 간 편차가 큰 것으로 나타났다. 단, 금융사의 경우 비 금융사의 매출액과 직접 비교가 어려워 매출액 통계량 산출에서 제외하였다.

한편 <표 4>와 <표 5>는 정보사고 방지 관련 투자 연구에 사용된 총 107개의 표본을 투자 발표 연도와 투자 기업의 산업별로 분류한 표이다. 산업별로 보면 금융관련 기업이 전체 표본의 42.99%로 차지하여 보안 관련 투자를 가장 활발히 하는 것으로 나타났다. 금융기관은 전자 금융 거래가 빈번하고 고객의 자산을 안전하게 관리한다는 신뢰성을 주는 것이 매우 중요하기 때문에 다른 산업보다 많은 투자를 하고 있는 것으로 보인다.

보안투자 관련 기사는 대부분 보안업체가 자사

〈표 3〉 사고기업의 기술 통계량[4]

	최소값	최대값	평균	표준 편차
시가총액 (억원)	61	479,533	62,830	90,317
총 매출액 (억원)	165	342,838	60,122	90,944
당기순이익(억원)	-17,450	60,145	5,821	12,670
주당순이익(원)	-3,933	35,006	4,315	8,030
총자산(억원)	224	1,714,876	131,160	309,642
총자본(억원)	119	194,737	34,817	44,503
종업원수(명)	49	58,964	9,829	16,679

3) 각 기업의 산업별 분류는 KOSPI 와 KOSDAQ에 등록된 기업 종목 자료를 이용하였다. 본 연구대상에 포함된 서비스업체는 모두 온라인 게임업체이었기 때문에 IT기업과 함께 분류하였다.

4) Fnguide.com에서 제공하는 기업별 시가총액과 재무제표 자료를 이용하였다. 시가총액은 사건 일의 시가총액, 그 외의 데이터는 사건 발생 시점 이전해의 값이다.

〈표 4〉 보안투자의 연도별 분포

산업 구분	보안 투자 건수
금융/은행/증권/보험	46
IT종합/서비스업	19
통신/전기/전자	25
기타	17

<표 5> 보안투자 기업의 산업별 분포

년도	보안투자 건수
2001	12
2002	35
2003	28
2004	27
2005 Q1	5

의 보안 솔루션 판매 및 보안 프로젝트의 수행을 알리기 위한 목적으로 경제 일간지와 IT 전문 신문에 발표된 것이었다. 또한 보안투자의 규모도 시장에 영향을 줄 만큼 크지 않았고, 대기업은 보안업체의 솔루션을 구매하지 않고 자사가 직접 보안 솔루션을 개발 및 구축하는 경우가 많고 기사화되지 않는 경우가 많다는 점이 본 연구 자료 수집의 한계라 볼 수 있다.

Ⅳ. 정보보안 사고로 인한 기업가치의 변화

정보보안 사고로 인한 기업가치의 변화 정도를 측정하기 위해 우리는 정보보안 사고가 발표 전후한 시점에 해당 기업의 정상수익률이 어느 정도인지를 측정해야 한다. 즉 비정상수익률을 도출하기 위해 우선 정상수익률을 도출하기 위한 기준모델이 필요하다는 것이다. 본 연구에서는 기준모델로 다음의 시장모형을 채택하였다(Brown and Warner, 1985).

$$r_{it} = \alpha_i + \beta_i r_{mt} + \varepsilon_{it} \quad (1)$$

r_{it}: 주식 i의 t일의 수익률
r_{mt}: t일의 시장포트폴리오 수익률
α_i: 주식 i의 고유 위험
ε_{it}: 주식 i의 t일의 오차항(error term)

위 식에서 $\beta_i r_{mt}$은 시장 전체의 변화에 따른 주식 i의 수익률 변화를 나타내고, 오차항은 시장 전체의 변화로 설명할 수 없는 특정 기업/시점의 수익률 변화를 설명하기 위한 항으로 본 연구에서는 ε_{it}는 *i.i.d.* $N(0,\sigma_i^2)$을 따른다고 가정한다. 시장포트폴리오 수익률 r_{mt}로는 거래소 상장기업의 경우는 종합주가지수, 코스닥 등록기업의 경우는 코스닥 지수를 사용하였다.

본 연구의 분석대상 59개 기업에 식 (1)을 각각 적용하여 모수 벡터 $\{\alpha_i, \beta_i, \sigma_i^2\}$를 추정하였다. 우리는 보안사고 사건이 발표된 날에서 2주 전부터 시작해 거꾸로 과거 1년 동안의 일별 주가 데이터를 사용해 식 (1)의 모수를 추정하였다. 사건 발생일로부터 이전 2주간의 기간을 추정에서 제외한 이유는 이 기간 중에는 이 기간 중에는 정보보안 사고가 정상수익률 추정에 영향을 미쳐 추정편의를 일으킬 가능성이 높고, 너무 오랜 기간의 데이터를 추정에서 제외하면 모수의 비정태성(non stationarity) 문제가 발생할 가능성이 증대하기 때문에 2주 정도의 데이터를 제거하는 것이 적당하다(Beaver, 1968).

각 기업에 대해 식 (1)의 모수를 추정한 후 주식 i에 대한 t일의 비정상수익률 A는 다음과 같이 도출할 수 있다.

$$A_{it} = r_{it} - \hat{\alpha}_i - \hat{\beta}_i r_{mt} \quad (2)$$

식 (2)에서 첨자 $i = \{1,2,...N\}$ 이고 N은 분석대상의 기업 수(본 연구의 경우 $N = 59$)를 나타낸다. 그리고 차후 논의의 편리를 위해 시간을 나타내는 첨자를 사건 중심으로 변환하기로

〈표 6〉 보안사고로 인한 평균 비정상수익률 및 누적 평균 비정상수익률

사건 날짜	평균 비정상수익률	t - 검정통계량	P - value	누적 평균 비정상수익률
- 5	0.390	0.906	0.369	0.390
- 4	0.234	0.631	0.531	0.624
- 3	- 0.034	- 0.095	0.924	0.591
- 2	0.107	0.280	0.780	0.698
- 1	0.769	1.911	0.061	1.467
0	- 0.863	- 2.763	0.008	0.604
1	0.526	1.316	0.193	1.130
2	0.284	0.769	0.445	1.414
3	0.245	0.609	0.545	1.659
4	- 0.118	- 0.338	0.737	1.541
5	0.044	0.128	0.898	1.586

한다. 즉 정보보안 사고가 발표된 날의 t는 0, 사건이 발생한 다음 날의 t는 1, 사건이 발생하기 바로 전 날의 t는 -1과 같이 표기한다. 우리는 사건이 발표된 날로부터 -5일부터 +5일까지의 기간을 사건의 영향력이 존재할 수 있는 사건기간으로 정하고 이 기간 동안의 비정상수익률의 추이를 살펴보기로 한다. 즉 식 (2)에서 첨자 $t \in \{-5,...,5\}$ 이다.

<표 6>은 59개 기업의 보안사고 발표일 주변의 평균 비정상수익률($\overline{A_t}$)과 t-검정통계량(T_{st}), 그리고 누적 평균 비정상수익률(CAR_t)을 나타내고 있다. 평균 비정상수익률은 기업별로 도출한 비정상수익률의 기업간 평균값을 의미하고 누적평균 비정상수익률은 평균 비정상수익률의 $t \in \{-5,...,5\}$ 기간 내 누적 값을 의미한다. t-검정통계량은 기업별로 도출한 비정상수익률이 0인지를 검증하기 위한 통계량이다. 이상의 3가지 통계량은 다음의 식으로 도출할 수 있다.

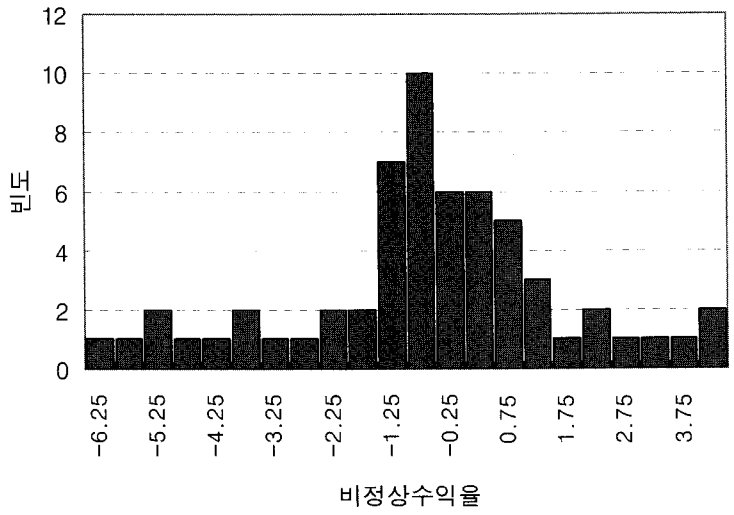
$$\overline{A_t} = \sum_{i=1}^{N} \frac{A}{N} \text{ for } t \in \{-5,...5\} \text{ for} \qquad (3a)$$

$$CAR_t = \sum_{t=-5}^{5} \overline{A_t} \qquad (3b)$$

$$TS_t = \sum_{t=1}^{N} \frac{A/\sigma_i}{\sqrt{N}} \text{ for } t \in \{-5,...5\} \qquad (3c)$$

<표 6>의 결과에 의하면 보안사고가 발표된 당일(사건 날짜0)의 비정상수익률은 - 0.863으로 유의수준 0.05에서 통계적으로 유의하다.[5] 즉 우리는 보안사고가 주가 또는 기업가치에 통계적으로 유의한 영향을 미친다고 할 수 있다. 통계적으로 유의한 것으로 검증된 보안사고 사건 당일의 비정상수익률이 59개 표본 기업들 간에 어떻게 분포돼 있는가를 보기 위해, 우리는 보안사고 사건 당일의 비정상수익률(A_{i0})의 빈도분포를 보기로 한

5) 보다 구체적으로 우리의 귀무가설은 '정보보안사고는 기업가치에 아무 영향을 미치지 않는다'라고 표현할 수 있다. 정보보안사고 사건 당일 비정상수익률의 p-value가 0.008로, 우리는 유의수준 0.05에서 귀무가설을 기각한다. 즉 우리는 대립가설 '정보보안사고는 기업가치에 영향을 미친다'를 지지한다.



〈그림 1〉 보안사고 발표 당일의 비정상수익률 분포

다. <그림 1>은 59개 표본기업에 대한 A_{i0}의 빈도 분포를 보여주고 있는데, 통계적으로 유의한 것으로 검증된 보안사고의 영향이 소수의 극단적인 값에 의한 것이 아니라는 사실을 보여준다. <그림 1>에 따르면 전체 표본기업의 67.8%가 음의 비정상수익률 값을 갖고 있고, 중앙값(median)도 -0.822로 이는 통계적으로 유의하게 0보다 큰 값이다.

이상의 분석결과를 요약하면 우리나라 주식시장의 투자가는 기업의 정보보안 사고가 기업가치에 부정적 영향을 미친다고 평가했다. 표본에 포함된 보안사고 59건 기업의 사고 당일 평균 시가 총액은 6조 2,830억 원이므로, 0.86% 수익률 하락은 평균 540억 원의 기업가치 하락을 의미한다. 미국에서 발생한 인터넷 침해 사고를 대상으로 한 Cavusoglu *et al.*(2004)의 연구에서는 보안사고의 결과 사고 당일과 익일에 2.1%의 시장가치가 떨어지고 17억 달러 정도의 손실을 가져왔다. 본 연구는 국내 정보보안 사고는 사고 당일에만 주가에 영향을 미치며 기업가치 손실도 1% 이하로 주식시장에 미치는 영향력이 미국에 비해 상대적으로 매우 적음을 알 수 있다. 이는 아마도 우리 국민들이 사회 전반적으로 미국인에 비해 정보보안을 소홀히 다루기 때문일 것이다. 정보보안 사고가 터질 때마다 정보보안에 대한 경각심 제고를 위한 각계의 행사는 있었지만 대부분 단발성 캠페인에 그쳤다. 보다 지속적으로 고객과 투자자에게 정보보안의 중요성을 인식시키는 노력이 필요하다.

V. 정보보안 사고로 인한 기업가치 하락의 요인

우리는 이상에서 정보보안 사고가 기업가치에 부정적인 영향을 미침을 보았다. 그러나 <그림 1>에서 본 바와 같이 정보보안 사고로 인한 비정상수익률의 값(A_{it})은 넓게 분포돼 있다. 본 장의 목표는 개별기업의 비정상수익률(A_{it})의 분산을 설명하는 데 있다. 즉 정보보안 사고로 인한 비정상수익률 A_{it}를 종속변수로 하고 정보보안 사고를 경험한 기업의 특성, 사고의 특성, 사고발생 연도 등을 독립변수로 하는 회귀분석을 적용하여 비정상수익률이 발생하는 원인을 보다 심층적으로 분석한다는 것이다. 이런 종류의 분석결과

는 향후 정보보안 사고 방지를 위한 전략을 수립하는 데 매우 유용할 것으로 기대한다. 사실 사건연구를 수행하면서 각 주식의 비정상수익률을 종속변수로 하고 기업의 특성을 독립변수로 하는 연구는 보편화되고 있는 추세다(Binder, 1998).

<표 7>은 비정상수익률의 분산을 설명하는 여러 회귀분석 결과를 요약한 표이다. 비정상수익률의 분산을 설명할 수 있는 무수히 많은 독립변수가 존재하겠지만 우리는 일반투자자가 쉽게 접할 수 있는 독립변수로 분석을 제한하였다. 이는 종속변수의 값을 결정하는 것은 이들 일반 투자자이고 이들은 시장에서 누구나 얻을 수 있는 정보를 갖고 사건의 가치를 판단하기 때문이다.

<표 7>에 따르면 우리가 고려한 독립변수 모두가 유의수준 0.05에서 비정상수익률의 표본간 분산을 설명하지 못했다.

첫째, 독립변수 기업유형은 보안사고 기업을 인터넷기업과 전통기업으로 나누는 더미변수로, 우리는 인터넷기업을 인터넷 상에서 모든 비즈니스가 이뤄지는 기업으로 규정하였다. 인터넷 기업은 모든 업무가 인터넷을 통해 이뤄지기 때문에 고객들이 정보보안을 더욱 중요하게 생각할 것이기 때문에 정보보안 사고에 따른 기업가치 하락 폭이 더욱 클 수 있을 것으로 생각되었다. 그러나 <표 7>에 따르면 정보보안 사고로 인한 기업가치 하락 정도는 인터넷기업과 전통기업 간 차이가 없는 것으로 나타났다.

둘째, 시가총액, 당기순이익, 자산 및 종업원 수의 독립변수는 보안사고 기업의 규모를 측정하는 변수들이다. Bharadwaj and Keil(2001)은 기업의 규모가 작을수록 IT 실패가 기업에 미치는 영향이 크다고 주장하였다. 그러므로 우리는 정보보안 사고로 인한 피해 역시 기업의 규모가 작을수록 기업가치에 미치는 영향이 더 클 것으로 생각하였다. 그러나 기업규모를 측정하는 어떤 변수도 비정상수익률의 차이를 설명하지 못하였다. 즉 기업규모에 따라 정보보안 사고로 인한 기업가치 하락 정도는 차이가 없는 것으로 나타났다.

셋째, 앞서 언급한 바와 같이 정보보안 사고는 정보 보호의 세가지 목적인 기밀성, 무결성, 가용성 사고로 나눌 수 있다. 기밀성 사고는 고객정보, 신용정보, 기술정보, 회사기밀정보가 유출된 경우로 전체 정보보안 사고의 절반을 차지하고 있다. 독립변수 정보유출여부는 정보보안사고가 기밀성 사고인지 아니면 기타(무결성과 가용성) 사고인지를 구분하는 더미변수이다. <표 7>에 따르면 정보보안 사고로 인한 기업가치 하락 정도는 보안사고의 유형(기밀성 여부)에 따라 아무 차이가 없는 것으로 나타났다.

넷째, 독립변수 인터넷관련여부는 정보보안 사고를 온라인 상에서 발생한 사고와 오프라인 상에서 발생한 사고로 구분하는 더미변수이다. 우리는 온라인 상에서 발생한 정보사고가 오프

〈표 7〉 비정상수익률에 영향을 미치는 요인

요인 변수	F 값	p-value	비고
기업유형	1.993	0.163	전통/인터넷
시가총액	1.272	0.264	<표 3>의 정보보안 사고 기업의 시가총액
당기순이익	1.907	0.173	<표 3>의 정보보안 사고 기업의 당기순이익
자산	1.422	0.238	<표 3> 의 정보보안 사고 기업의 자산
종업원 수	0.767	0.385	<표 3>의 정보보안 사고 기업의 종업원 수
정보유출여부	1.885	0.175	정보유출사고/기타(웹사이트 변조 및 다운)
인터넷관련여부	1.723	0.195	온라인시고/오프라인사고
사고발생 시점	0.674	0.613	2002/2003/2004/2005

라인에서 발생한 사고보다 고객 및 투자자들이 그 위험성을 더 심각히 받아들일 것으로 생각했으나 결과는 아무 차이가 없는 것으로 나타났다. 마지막으로 정보보안 사고는 사고 발생 시점에 따라서 시장에 미치는 효과가 다를 수 있다고 생각하여 독립변수 사고발생 시점을 검증하였다. 결과는 역시 사고 발생 시점에 따라 비정상수익률의 차이는 없는 것으로 나타났다.

IV. 정보보안 관련 투자로 인한 기업가치의 변화

<표 8>은 정보보안 투자 관련 107건에 대해 보안투자 발표일 주변의 평균 비정상수익률과 *t*-검정통계량, *p*-value 및 누적 평균 비정상수익률 값을 요약하고 있다. 이들 각 통계량의 정의는 이전 정보보안 사고의 분석에서와 동일하다.

<표 8>에 따르면 정보보안 관련 투자는 전체 사건기간 동안 비정상 수익률에 통계적으로 유의한 영향을 미치지 않았다고 결론지을 수 있다. 정보보안 투자는 투자발표 당일에 (통계적으로 유의하지 않았지만) 다소 기업가치를 상승(0.04)시키는 효과가 있었지만, 사건 다음 날 오히려 기업가치를 감소(-0.403)하는 효과가 있었다.

IIV. 결론 및 미래 연구과제

한국인터넷통계집(2004)에 따르면 우리나라는 인터넷 이용자 비율에 있어 아이슬란드에 이어 세계 2위라 한다. 그러나 인구 100만 명당 인터넷 보안서버 보유 대수에 있어서는 조사 대상 50개 국가 중 28위에 머물렀다. 보통 인터넷 이용률과 정보보안 수준은 비슷한 양상을 보이는데 우리나라는 그 간극이 매우 크다. 결과적으로 우리나라는 컴퓨터 바이러스, 해킹 등 사이버 테러에 취약할 수 밖에 없다.

2005년 IT이슈는 ERP와 보안투자가 될 것이라 하는 반가운 보고서가 있다(2005년 한국 기업 IT 지출 전망보고서). 정보 보안에 민감한 정부·금융·대학 및 통신 분야에서 보안 솔루션 투자가 지속될 것으로 전망하고 있다. 정보통신부도 보안설비 투자 기업에 대해 2005년 7월부터 투자금액의 3%까지 법인세나 소득세를 감면해 주기로 결정하

〈표 8〉 정보보안 관련 투자 평균 및 누적 평균 비정상수익률

사건 날짜	평균 비정상수익률	t - 검정 통계량	p - value	누적 평균 비정상수익률
-5	0.102	0.338	0.736	0.102
-4	-0.128	-0.511	0.611	-0.027
-3	-0.011	-0.043	0.966	-0.037
-2	-0.107	-0.438	0.663	-0.145
-1	-0.045	-0.192	0.848	-0.190
0	0.040	0.142	0.888	-0.150
1	-0.403	-1.724	0.088	-0.553
2	0.282	1.174	0.243	-0.271
3	0.044	0.168	0.867	-0.227
4	0.154	0.544	0.588	-0.073
5	-0.125	-0.520	0.604	-0.198

였다(디지털타임스, 2005년 1월 7일). 그러나 실질적 혜택이 미미하고, 정보 보안에 대한 기업들의 일반적 인식이 부족하고 실제 투자로 이어질 수 있을지는 미지수이다.

본 연구는 사건연구 방법론을 통해 국내 정보보안 사고 및 보안관련 투자의 경제적 가치를 정량적으로 측정했다는 점에 그 의의가 있다. 본 연구는 정보보안 사고로 인한 피해규모를 정확히 파악하여 우리 사회 저변에 깔려 있는 정보보안 불감증에 경종을 울리는 계기가 되었으면 한다. 정보보안 사고에 대한 피해 규모와 같은 기본적인 자료가 없다면 올바른 정책 결정을 하기 힘들고 정책의 효과를 평가하기도 어렵다. 따라서 본 연구 결과는 향후 정보보안 투자를 고려하는 국내 기업의 최고경영자와 관리자들이 보안 투자 관련 전략적 의사결정을 할 때 도움이 될 것으로 판단된다. 본 연구의 결과를 요약하면 다음과 같다.

첫째, 본 연구에서 분석한 국내 기업 보안 사고 59건의 경우, 보안 사고가 발생한 사고발표 시점에 평균 0.86%의 주가가 감소하였다. 이를 시가는 환산해 보면 보안 사고가 발생한 경우에 평균 540억 원의 기업가치가 하락한다는 것이다. 이 금액 또는 주가 하락률은 미국 기업의 보안사고 경우보다 매우 작은 값으로, 우리나라 사회 전반에 깔려 있는 정보보안 결핍증을 원인으로 볼 수 있을 것이다. 따라서 2003년 1월의 인터넷 대란과 같은 사고가 발생하지 않도록 기업뿐 아니라 정부 차원에서 정보보안 의식의 제고가 무엇보다 시급하다. 기업경영자는 보안 관련 투자를 비용이 아닌 투자로 보는 마인드 변화가 필요하다.

둘째, 정보보안 사고로 인한 기업가치 감소율은 사고가 발생한 기업의 특성(인터넷/전통기업, 규모), 사고의 특성(정보유출 여부, 인터넷 관련여부), 사고의 발표 년도 등에 따라 통계적으로 차이가 없었다. 미국 기업의 연구이기는 하지만 이들 요인들이 기업가치 감소율 차이를 보인 기존 연구들이 있다. 그러므로 본 연구 결과로 우리나라에서는 요인 별 차이가 존재하지 않는다고 결론을 내리는 것은 타당하지 않다. 59건의 샘플 사이즈로 이들 요인 별 기업가치 감소율 차이를 구분하기는 쉽지 않았을 지 모른다. 미래 연구에서 보다 많은 정보보안 사고 건을 확보하는 것이 필요할 것이다.

셋째, 본 연구에서 분석한 정보보안 관련 투자 사건 107건의 경우, 정보보안 투자는 기업가치에 통계적으로 유의미한 영향력을 행사하지 못하였다. 주식시장 투자자들은 우리나라 기업들의 보안관련 투자가 기업가치에 영향을 미칠 정도로 그 규모가 크지 않다고 평가하고 있음을 시사하는 결과이다. 기업가치에 아무 영향을 미치지 않는 정보보안 투자를 기업이 왜 해야 하는지에 대한 의문이 드는 결과지만, 보안관련 투자를 하면 보안사고의 수를 줄일 수 있다는 간접적 효과를 생각해 볼 수 있다. 즉 미래연구에서는 보안관련 투자가 기업가치에 직접적인 영향을 미치는 경우(가설: '보안관련투자→기업가치')와 정보보안사고를 통해 기업가치에 간접적으로 영향을 미치는 경우(가설: '보안관련투자→정보보안사고→기업가치')를 동시에 검증하는 구조방정식(structural equation model) 모형을 검증해 보는 것도 생각해 볼 수 있다.

앞서 지적한 미래 연구 과제 외에도 정보보안 사건 및 보안투자 효과를 측정하는데 있어 사건연구 방법론이 갖는 한계를 극복할 방법론 개발이 필요하다. 예를 들어 주식시장 데이터를 이용하지 않는 Cavusoglu, Mishra and Raghunathan(2004b)의 IT 보안 투자 가치 측정 모델이 그 대표적 예다. 사건연구 방법론은 주식시장에 상장된 기업의 정보보안 사고 중에서 언론에 공개된 사건만을 연구 대상으로 삼는다. 보안 관련 사고는 기업 이미지에 악영향을 미치기 때문에 기업들이 해킹 사고를 당해도 신고를 하지 않아 언론에 공개되지 않는 경우가 많다. 또한 정보보안 사고는 상장기업보다 상장되어 있지 않은 중소기업에서 훨씬 더 빈번하게 발생하고 있지만 이 경우 일별 주가 데이터가 존재하지 않기 때문에 사건연구를 적용하기

어렵다.

참 고 문 헌

김병도, 김지경, 우상진, "CRM 투자와 기업가치", 경영학연구, 제33권, 제4호, 2004년 8월, pp. 1185-1199.

디지털타임즈, "조세특례제한법 개정안", 2005년 1월 7일.

서울경제신문, "은행 보안투자 쥐꼬리", 2003년 9월 2일.

한국인터넷통계집 2004, 한국인터넷진흥원(NIDA), 2004년 11월 30일.

2005년 한국기업 IT 지출 전망 보고서, 한국 IDC, 2005.

Beaver, W., "The Information Content of Annual Earnings Announcement", *Journal of Accounting Research*, Supplement, 1968, pp. 67-92.

Bharadwaj, A. and Keil, M., "The Effect of Information Technology Failures on the Market Value of Firms: An Empirical Examination", *INFORMS 2001 Miami*, November 2001.

Binder, J., "The Event Study Methodology since 1969", *Review of Quantitative Finance and Accounting*, Vol.11, 1998, pp. 111-137.

Brown, S. and Warner, J., "Using Daily Stock Returns: The Case of Event Studies", *Journal of Financial Economics*, Vol.14, 1985, pp. 3-31.

Campbell, K.,L. Gordon, M. Loeb and Zhou, L.,"The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidencefrom the Stock Market", *Journal of Computer Security*, Vol.11, 2003, pp. 431-448.

Cavusoglu, H., Mishra, B., and Raghunathan, S., "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developer", *International Journal of Electronic Commerce*, Vol.9, No.1, 2004a, pp. 69-104.

Cavusoglu, H., Mishra, B., and Raghunathan, S., "A Model for Evaluating IT Security Investments", *Communications of the ACM*, Vol.47, No.7, 2004b, pp. 87-92.

CERT/CC Statistics 1988 2006, Total Incidents Reported, *Carnegie Mellon Software Engineering Institute*, www.cert.org/stats.

Dos Santos, B., K. Peffers and Mauer D, "The impact of Information Technology Investment Announcements on the Market Value of the Firm", *Information Systems Research*, Vol.4, No.1, 1993, pp. 1-23.

Ettredge, M. and Richardson, V., "Assessing the Risk of in E commerce", in R. H. Sprague, Jr. (ed.), *Proceedings of the Thirty fifth Hawaii International Conference on Systems Sciences*, Los Alamitos, CA: IEEE Computer Society Press, 2002.

Fama, E., L. Fisher, M. Jensen and Roll, R., "The Adjustment of Stock Prices to New Information", *International Economic Review*, Vol.10, 1969, pp. 1-21.

Im, K., K. Dow, and Grover, V., "A Reexamination of IT Investment and the Market Value of the Firm: An Event study Methodology", *Information Systems Research*, Vol.12, No.1, 2001, pp. 103-117.

〈부록: 기사예문〉

1. 정보 보안 사고 기사의 예

[한국경제2003년 5월 22일]

다음 '인터넷 카페' 해킹 당했다

인터넷포털 다음커뮤니케이션(대표 이재웅)이 운영하는 인터넷 커뮤니티(다음카페)가 해킹 당한 사실이 밝혀졌다. 다음커뮤니케이션은 21일 뉴스서비스인 '미디어 다음'을 통해 다음카페의 아이디(ID)와 비밀번호가 도용 당했다는 사실을 시인하고 경찰청 사이버수사대에 수사를 의뢰했다고 밝혔다.

이번에 해킹 당한 카페는 다음카페 중 회원수가 1백50만 명으로 가장 많은 '장미가족의 태그교실'로 지난 20일 오전 운영자의 아이디(ID)와 비밀번호를 도용, 운영자를 사칭한 금융피라미드 사기메일이 전 회원들에게 발송됐다.

다음은 그러나 이같은 사실을 해당 카페 회원에게 곧바로 알리지 않고 사고 발생 8시간이 지나서야 공지사항을 내보내 빈축을 사고 있다. 또 미디어 다음에서는 논란이 일자 기사제목을 '회원 1백50만명 카페 해킹'에서 '금융피라미드 사기 주의!'로 바꾸었다가 해당 내용을 사이트에서 아예 삭제했다.

2. 정보 보안 관련 투자 기사의 예

[전자신문 2003년 9월 17일 08:30]

엔터라시스, LG유통에 침입탐지시스템 공급

엔터라시스네트웍스코리아(대표 안희완)는 LG유통에 침입탐지시스템인 '드래곤 IPS'를 공급했다고 16일 밝혔다.

엔터라시스는 네트워크 컨설팅 및 보안업체 엔클루(대표 임초순)와 공동으로 LG유통 본사 및 지사 등 총 6개 사이트에 '드래곤 IPS'를 공급했으며 최근 시스템 구축을 완료했다.

이번 시스템 구축을 통해 불법적인 해킹 시도나 바이러스 전파를 사전에 감지, 차단함으로써 보다 안전한 네트워크 환경을 제공하게 됐다고 엔터라시스는 설명했다.

Information Systems Review
Volume 9 Number 1
April 2007

The Effect of Information Security Breach and Security Investment Announcement on the Market Value of Korean Firms

Young Ok Kwon* · Byung-Do Kim**

Abstract

With the fast development of the Internet and the increasing dependence on information infrastructures, companies are faced with various information security threats such as information leakages, modifications, and information breaches. South Korea is one of the leading countries in the Internet usage, but is ranked relatively low when it comes to information security. In fact, many Korean firms have suffered financial losses and damaged corporate images from the information security breaches. However, because of the difficulties in quantifying the costs of the information security breaches, Korean companies tend to delay their investment decisions on information security.

The purpose of this study is to measure the cost of information security breach and the economic value of security investment using the event study methodology. Our results show that the announcement of an information security breach negatively influenced the market value of the corresponding company. The effect was statistically significant at the significance level of p = 0.05. The breached companies lose, on average, 0.86% of their market values on the day of the announcement - an average loss in market capitalization of $55 million. On the other hand, the investment on information security had no effect on the stock price or the market value of the firm.

Keywords: ***Event Study Methodology, Information Security, Information Technology Security, Security Breach Announcement, Return on Investment***

* Ph.D. Candidate, Carlson School of Management, University of Minnesota
** Professor, Graduate School of Business, Seoul National University

◐ 저 자 소 개 ◑

권 영 옥 (ykwon@csom.umn.edu)

연세대학교 컴퓨터과학과에서 이학사, 서울대학교 대학원 경영학과에서 경영학 석사를 취득하고, 현재 University of Minnesota에서 Information Decision Sciences 전공으로 박사과정에 재학 중이다. 직장 경력으로는 한국 오라클 응용기술팀에서 Sales Consultant로 3년반 동안 근무하였다. 주요 관심 분야는 Personalization, Data mining, Business Intelligence등이다.

김 병 도 (bxk@snu.ac.kr)

현재 서울대학교 경영대학 교수로 재직 중이다. 서울대학교 경영대학을 졸업한 후, 뉴욕대학(NYU)에서 경영학 석사, 시카고대학(The University of Chicago)에서 경영학 박사학위를 취득했다. 서울대학에 부임하기 전 카네기멜론 대학(Carnegie Mellon University) 경영학과에서 약 4년간 마케팅 교수로 재직하기도 했다. 그는 지난 10여년 동안 CRM, 상용고객보상제도, 제품/서비스 추천모형, 최적 마케팅 전략의 개발 등 첨단 경영학 문제를 연구하여, 관련논문을 Journal of Business & Economic Statistics, Journal of Interactive Marketing, Journal of Marketing Research, Journal of Retailing, Management Science, Marketing Letters, Marketing Science and Journal of Database Marketing 등 학술지에 발표했다.

논문접수일 : 2006년 10월 09일 **게재확정일 : 2007년 03월 06일**
1차 수정일 : 2006년 11월 13일 **2차 수정일 : 2007년 02월 12일**