Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.3, Jun. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.3.649

정보보안 사고가 기업가치에 미치는 영향 분석: 한국 상장기업 중심으로

황 해 수,† 이 희 상‡
성균관대학교 기술경영학과

The relationship between security incidents and value of companies : Case of listed companies in Korea

Haesu Hwang,† Heesang Lee‡
Sungkyunkwan University, Management of Technology

요 약

최근 IT환경의 변화와 해킹공격의 발전은 기업의 보안사고 발생위험을 높이고 있다. 특정 사건이 기업에 미치는 주가변화를 측정할 수 있는 사건연구방법론은 보안사고 기업의 시장가치의 피해비용을 분석하기 위한 대표적인 방법론으로 주로 사용되어 왔다. 그러나 기업의 일시적인 주가변화 분석은 모든 기업들에게 공통된 시사점으로 활용하는데 제약이 있고, 기업에 발생한 평판의 손실분석에 대한 필요성 또한 강조되고 있다. 본 연구는 국내에서 최근 10년간 발생된 상장기업의 보안사고 52건을 대상으로 기업의 가치평가 방법론인 Tobin's q가 제시한 기업의 기준을 세분화함으로써, 보안사고로 인한 평판손실이 유의하게 발생함을 정량분석하였다. 이러한 접근방법은 q로 분류된 기업 별 피해범위에 해당하는 정보보호 투자예산 책정과 효율적인 리소스 투입 산정의 판단기준으로 활용 가능할 것이다.

ABSTRACT

Recently, the risk of security incidents has been increased due to change of IT environment and development of new hacking methods. Event study methodology that measures the effect of a specific security incident on the stock price is widely adopted to analyze the damage cost of security incidents on market value. However, analysis of company's temporary stock price change is limited to immediate practical implication, and reputation loss should be considered as a collateral damage caused by security incidents. We analyzed 52 security incidents of listed Korean companies in the last decade; by refining the criteria presented by Tobin's q, we quantitatively showed that the companies has significantly higher reputation loss due to security loss than the other companies. Our research findings can be used in order that the companies can efficiently allocate its resource and investment for information security.

Keywords: Security incidents, Event study, Reputation analysis, Tobin's q, Valuation

I. 서 론

IT(Information Technology)시스템과 인터넷의 상호 연결성은 기업의 생산성과 시장가치 증대를 위한 긍정적인 면과 기업발전을 저해하는 사이버 공격의 위협과 같은 부정적인 면도 존재한다[1]. 이러한 부정적인 측면에도 불구하고 IT기반의 정보화는 기업의 경쟁우위 확보를 위해 지속적으로 발전하고

접수일(2014년 11월 22일), 수정일(2015년 2월 23일), 게재확정일(2015년 4월 13일)

† 주저자, haesuhwang@skku.edu
‡ 교신저자,leehee@skku.edu(Corresponding author)

있다. 특히, IT기반의 서비스를 통해 수집한 고객의 개인정보 뿐 아니라 서비스 이용, 구매상품 등의 정보들은 기업의 사업경쟁력 강화를 위한 주요 정보자산이다. IT발전과 함께 정보자산의 가치향상에 따른 정보의 수집과 활용은 증가하였으나, 정보자산의 관리 부족이나 해킹기술의 발전 등으로 인한 보안사고의 증가는 정보보호(information security)의 필요성을 높이고 있다[2].

최근까지 정보보호의 주요 연구주제는 암호화와 방화벽(firewall), 침입탐지/침입 차단시스템 (IDS ,IPS)등 솔루션 위주의 보안기술과 이를 활용한 관제, 관련법 준수를 위한 보안정책의 수립에 한정되었다. 2000년부터 기존의 기술과 관리 중심의 보안사고 예방에 한계를 인식하고, 보다 효과적인 대응책을 위해 정보보안 사고의 피해규모 산정과 정보보호 투자의 경제성 연구가 활발하게 진행되었다[3]. 보안사고의 발생을 예측할 수 없는 정보보호의 특성 상 보안시스템 도입에 필요한 경제성 관점의 최적화된 투자분석의 연구 또한 확대중이다[4]. 보안사고 사례의 피해 비용 분석은 미래의 예산투자 기준과 보안 Risk 예방에 활용될 수 있는 이유로 기업의 정보보안 사고가 주가에 미치는 손실의 정량분석 연구는 다양한 관점에서 지속적으로 발전하고 있다[5-16].

최근의 보안사고가 미치는 경제적 손실과 평판손실의 영향이 높아짐에 따라 예방을 위한 관련 연구 또한 활발하게 진행되었다. Gordon 등[3]은 보안사고로 인한 매출수익저하와 지출비용 증가, 향후 매출의 불안전성과 시장가치의 하락이 발생하며, 보안사고로 인한 잠재적인 시장가치의 하락을 우려하여 언론 발표를 꺼려한다는 사실을 설명하였다. Nam 등[5]은 정보보안 사고로 인한 기업의 경제적 가치 하락을 예방하기 위해 고도화된 IT환경의 신규 사업과 서비스에서 전략적 경쟁우위 요소로 정보보호 기능을 부가가치 창출의 핵심요소로 적극 활용해야 함을 강조하였다.

보안사고로 인한 기업의 피해정보는 기업의 비즈니스에 민감한 정보이므로 외부공개가 제한되어 연구 데이터 수집에 한계가 있다. 기업의 시장가치를 반영하는 주가정보는 보안사고로 인한 기업의 가치변화에 대한 측정이 가능하므로, 보안사고로 인한 재무측면의 영향을 추정해 볼 수 있다[17]. 시장에 공개된 주가정보는 보안사고로 인한 피해분석 필요한 객관성과 신뢰성 있는 데이터의 분석기반을 제공한다[18].

기업의 시장가치는 외부의 다양한 주체들로부터 영향을 받는데, 사건연구(event study)는 이러한 외부의 영향에 따른 주가의 변동 수익률을 측정하는 주요 분석방법으로 연구되었다. 보안사고와 같은 특정 사건의 언론 발표일을 기준으로 특정 기간에 발생한 주가의 변화를 추정하여 측정결과의 통계적 유의성을 검정하는 방법이다. 주가변화의 추정과 통계분석을 위해 과거 주가정보를 분석한 예측치와 실제 주가 간의 차이인 비정상 수익률(abnormal returns)과 AR을 누적하여 합산한 누적비정상수익률(cumulative abnormal returns)을 기업별로 도출하여 보안사고가 기업의 주식시장 가치에 미치는 주가의 변화(stock market reaction)를 연구하였다.

한편 평판손실(reputation loss) 측정 연구는 금융산업을 중심으로 활발히 진행되었다. 평판손실은 언론에 보도된 손실이 실제 발생한 손실의 합을 초과하여 기업의 시장가치가 저하되는 경우를 의미한다[19]. 바젤 은행감독 위원회(Basel Committee, 2006)는 운영위험(operaional risk)이 내부의 잘못된 프로세스, 사람, 시스템 또는 외부 상황으로부터 발생된 손실로 정의하였고, 전략적 위험과 평판위험은 제외하였다[20]. 하지만, Basel Committee (2009)에서 평판위험(reputation risk)은 고객, 계약자, 주주, 투자자, 채권자, 시장분석가, 그 외 관련 단체로부터 부정적 시각으로 인해 위험이 발생하거나, 규제기관이 은행의 유지, 설립, 사업 관계에 불리한 영향을 미치는 것으로 정의하였다[21]. 최근의 연구들은 평판손실을 다양한 위험관리요소를 내포한 기존의 운영위험에서 분류하여 기업의 신뢰에 기반한 핵심 자산으로 구분하여 분석해야 하는 주요 대상임을 강조하였다[22].

Tobin's q 분석은 사건연구방법론과 비슷하게 기업의 시장가치를 측정하기 위한 방법으로 연구되었다[23]. Tobin's q는 기업의 총자산가치를 대체 가능한 비용의 시장가치 비율(ratio)로 금융학과 재무학, 경제학에서 기업성과의 측정지표 목적으로 활용되었다. Tobin's q로 분석한 q 비율이 1보다 크면 기업가치가 충분히 반영된 투자 수익성이 높은 효율적인 경영기업으로, 1보다 작으면 기업가치가 저평가되어 적대적 M&A의 대상으로 볼 수 있다[24]. Tobin's q의 장점은 기업의 위험요소와 미래 발생가능성을 포함한 기업가치를 측정하는 방법으로, 기업성과 측정에 있어 총자산수익률(return of assets), 매출수익률(return on sales)같은 회계측정 기준보다

기업의 금융과 회계정보를 기반으로 쉽게 산출할 수 있는 특징을 갖는다. 또한, 기업의 총자산과 기업에서 창조되는 무형자산가치의 증가에 비례하므로, 무형자산가치의 결정요소 연구나 정보보호와 같은 무형가치 측정 시 효율적인 측정방법이며,
다양한 영역에서 넓은 기초정보를 수용한 측정이나 특정 기술쟁점과 관련한 측정에서 투자에 필요한 의사결정을 도출하기 쉽다는 장점도 갖는다[25].

본 연구의 목적은 정보보안 사고가 기업의 시장가치에 미치는 영향을 분석하기 위해 사건연구방법론을 이용한 시장가치와 평판손실분석을 분석하고, Tobin's q를 적용하여 보안사고로 인한 국내 상장기업의 피해사례를 정량분석 하는 것이다. 이 후의 본 연구의 구성은 다음과 같다. 제 2절은 각 주제별 선행논문을 정리하였고, 제 3절은 방법론들과 데이터 수집, 적용기준을 서술하였다. 제 4절에서는 데이터의 분석 결과를 제시하였으며, 제 5절에는 도출된 결론, 연구의 시사점과 향후연구를 제시한다.

II. 문헌연구

2.1 정보보안 사고의 정의와 최근 동향

정보보호(information security)는 일반적으로 고의, 과실, 재해 등에 의해 정보시스템의 고장 및 파괴되는 등의 위해를 막기 위한 물리적, 논리적 대응을 말한다[26]. 본 연구에서는 사람의 실수나 고의적으로 발생 한 보안사고를 대상으로 한다. 고의적인 침해행위로 인한 사고는 해킹, 컴퓨터 바이러스, 메일폭탄, 서비스거부 등의 공격에 의하여 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 발생된 사태를 말한다(정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 참조).

보안사고의 피해유형 증가와 다양화로 경제성 측면의 보안사고 분석을 조사한 전문기관이나 정보기술 기업의 리포트 발간도 활발하게 증가하는 추세이다. Economist Intelligence Unit이 2014년 발표한 리포트에 따르면 아시아 기업의 40%가 데이터 유출로 심각한 경제적 손실을 경험했고, 특히 금융회사들의 피해가 가장 컸으며, 35%만이 2013년에 데이터유출을 경험하지 않은 것으로 조사되었다[27]. Juniper Networks의 2013년 리포트에서는 2012년부터 2013년 3월까지 발생한 모바일 악성코드가 총 276,259개로 전년 대비 614% 증가하였으며, 이러한 현상은 모바일 플랫폼이 사이버 범죄자들의 주된 대상이라고 주장하였다[28]. 모바일 보안사고로 인한 경제적 피해 증가와 대비책 마련이 시급한 이유는 악성코드가 이익창출을 목적으로 정교한 공격기능을 갖추기 위해 기획, 개발, 배포까지의 체계적인 방법으로 발전하고 있음을 전망하였다[28].

2.2 관련연구

Table 1은 보안사고를 사건연구방법론으로 분석한 주요 선행연구들로 분석대상 기업의 보안사고수(events)와 주가변화의 주요 분석기간(window), 이러한 변수들을 기반으로 도출된 CAR을 확인할 수 있다. 보안사고 외에 특정 사건으로 인한 시장가치의

Table 1. Studies on information security incidents

Year	Author	Period	The number of events	Events window (Day)	CAR
2003	Campbell et al.	1995 ~ 2000	43	[-1 , 1]	-1.90%
2003	Grag et al.	2000 ~ 2002	22	[0 , 2]	-5.60%
2004	Hovav and D'Arcy	1998 ~ 2002	186	[0 ,25]	-0.1~-0.01%
2004	Cavusoglu et al.	1998 ~ 2000	66	[0 , 1]	-2.10%
2006	Ko and Dorantes	1997 ~ 2001	19	[-365,365]	-
2007	Kannan et al.	1997 ~ 2003	41	[-1 , 1]	-5.00%
2007	Kwon and Kim	2001 ~ 2005	59	[-5 , 5]	-0.86%
2009	Bharadwaj et al.	1990 ~ 2000	213	[-1 , 0]	-2.00%
2009	Goel and Shawky	2004 ~ 2008	168	[-2 , 1]	-1.00%
2013	Bose and Leung	1996 ~ 2012	87	[0 , 1]	-0.63%
2013	Sinanaj and Muntermann	2004 ~ 2011	72	[-5 , 5]	-

변화를 분석하기 위해 사건연구 방법론을 적용한 다양한 연구들이 시도되었다. Bharadwaj 등[6]과 Konchitchki 등[23]은 기업의 IT환경에서 발생한 사건이 경제적 손실에 미치는 영향을 정량분석하였다. Bharadwaj 등[6]은 10년 동안 213개의 IT 사고뉴스를 수집하여 사고발표일 중심으로 2일 간 2%의 평균 CAR이 하락함을 보였고, 기존 시스템의 사고보다 신규시스템의 사고가 더 많은 영향을 미치는 것을 증명하였다. Konchitchki 등[23]은 IT환경의 핵심인 정보처리 시스템에서 발생 한 사건을 사건연구로 정리하는 시도를 보였다. 특히, 사건연구방법론과 같이 기업의 가치를 평가할 수 있는 방법론으로 Tobin's q를 제시하기도 하였다.

Campbell 등[7]은 시장성과측면의 보안사고 영향을 분석한 연구에서 기밀정보의 유출경험 기업은 그렇지 않은 기업에 비해 1.9%의 주식 하락을 증명하였다. 기밀정보의 침해사건은 CAR에 부정적인 영향을 발생시켜 기업가치를 현저하게 하락시키지만 다른 종류의 보안사고는 주가에 영향을 미치지 않았음도 보였다. Cavusoglu 등[8]은 인터넷 보안 사고의 발표가 기업의 시장 가치에 부정적으로 결부되며, 이러한 기업은 보안사고 발표 2일 이내에 평균적으로 약 2.1%(시장가치 17억 달러)의 초과수익률로 인한 시장가치가 하락함을 강조하였다. 그리고 기업의 크기와 유형, 사고유형에 따른 분석 결과 CAR의 주요 결정요소로 소규모기업이 대기업보다 주식가격 하락에 더 민감함을 보였다. 그와 달리 Kannan 등[9]은 보안사고의 언론발표가 재정성과 측정의 결정요소인 CAR에 미치는 영향이 매우 낮음을 강조하였고, 사고 유형과 기업의 유형, 사건연구의 분석기간은 장기간 동안 주식가격의 하락에 미치는 영향이 없음을 밝혔다.

Hovav 와 D'Arcy[10,11,12]는 보안사고가 바이러스(virus), 웜(worm), DoS(denial of service)에 의한 보안사고 피해 연구에서 보안사고의 언론보도가 기업가치에 미치는 영향은 명확하지 않음을 주장하였다. DoS공격이나 바이러스 공격에 의한 피해는 CAR의 결정요소가 되지 않으므로 기업의 주가에 영향을 미치지 않고, 보안사고를 경험한 기업의 절반정도는 언론보도 25일 이후에 비정상 수익률에 특별한 영향이 없음도 보였다.

국내연구로 Kwon 등[26]은 2001년부터 2005년 1분기까지의 시장가치 변화를 측정하여, 그 영향력이 사건발표 시점에 시장가치 대비 -0.86% 영향에 미치는 결론을 도출하였다. Nam 등[5]은 기업의 보안사고가 주가에 미치는 영향으로 정보보호 투자효과를 대체함으로써 정보보호 투자로 인한 가치 창출효과를 측정하여 투자기준으로 적용하는 방안을 제안하였다. Hovav와 Han[29]은 2001년부터 2011년까지 105개 보안사고를 분석하여 국내 인터넷 기업이 단기보다 장기간에 부정적인 영향이 발생함을 보임으로써, 서구의 나라에 비해 재무적 가치보다 무형의 가치에 비중이 많음을 보였다. 또한, 한국기업의 개인정보 유출사고는 다른 선행연구의 보안사고에 비해 부정적인 손실의 차이가 없음도 강조하였다. 사건연구 외에 Jeong 등[30]은 예산과 투자에 대한 상관관계를 정량분석하여 예산집행에 기반 한 정보보호 투자가 정보보호 수준향상에 긍정적인 효과가 있음을 밝혔다.

평판손실은 특정사고로 기업에 발생한 실 손실 비율과 사건연구방법론에서 도출한 비정상 수익률의 합으로 도출한다. 주가의 변화와 실 손실비율을 반영한 평판손실 연구는 금융기관을 중심으로 운영손실의 피해분석 연구에서 시작되었다. Perry 등[19]은 기업의 평판에서 부정적인 사건의 영향을 정량화하여 평판위험을 분석하였다. 1974년부터 2004년까지 전 세계 금융기관에서 발생한 운영손실을 사건연구로 분석함으로써, 언론에 보도된 손실보다 실제 발생된 손실의 합을 초과하여 기업의 시장가치가 줄어드는 경우를 평판손실로 정의하였다. Gillet 등[31]은 운영손실에서 평판의 영향을 구분하여 정밀한 평판손실을 통해 주가의 주요 하락에 따른 비정상 거래규모가 있음을 보였다. 총 자산의 부채비율이 높은 기업은 더 많은 지분을 보유한 기업에 비해 운영손실로 인한 평판손실이 더 크게 발생함도 증명하였다. 금융 산업에서 운영손실에 따른 평판손실에 대한 증명은 Fiordelisi 등[22]의 연구에서 제시되었다. 430개의 운영손실 사례를 분석하여 운영손실로 인한 평판손실이 발생함을 보였고, Perry 등[19]과 유사하게 운영손실로 인한 사고들이 주가에 부정적인 영향을 발생시켜 평판손실의 원인임을 밝혔다. Sinanaj 등[32]은 6개 국가를 대상으로 보안사고의 언론보도가 기업의 주가와 평판에 미치는 영향을 미국의 정보 및 보안 연구단체인 포네몬연구소에서 발표한 리포트[33]의 직/간접 손실비용산정 방식으로 분석하였다.

기업의 시장가치를 측정할 수 있는 Tobin's q 연구도 지속적으로 진행되었다. IT에 해당하는 전반적인 사건을 대상으로 Tobin's q를 분석한 Bharadwaj 등[25]은 IT비용변수에서 Tobin's q

가 증가함을 통해 Tobin's q에서 변화를 설명할 수 있는 유일한 정보가 IT변수임을 제시하였다. 반면, Vlieghe 등[34]은 기업의 Tobin's q가 기대성과를 측정에 매우 강력한 방법이나, 다른 요소가 함께 미치는 영향력을 추가로 조사해야 할 필요가 있음을 강조하였다. Tobin's q는 정보보호에서도 가치분석 연구에 활용되었다. Zafar 등[35]은 정보보안 사고 발생 시 CIO(chief information officer)가 기업 성과에 미치는 영향을 Tobin's q를 적용하여 분석하였다. CIO가 갖는 역할과 권한이 기업의 성과에 영향을 미치며, 이러한 영향은 최초의 보안사고 발생 시 기업의 회복성과에 긍정적인 영향이 발생함을 CIO가 없는 기업과의 차이를 제시하였다.

III. 데이터 수집과 방법론

본 논문은 보안사고의 정량분석을 위해 총 세 가지 방법론을 적용하였다. 보안사고 발생 기업의 언론보도 일을 기준으로 분석 기간 동안 주가에 미치는 변화 분석을 위해 사건연구방법론을 적용하고, 사건연구방법론에서 도출한 비정상수익률과 실제발생한 손실비용 비율의 합을 평판손실로 측정하였다. 또한, 재무관점의 기업가치 평가를 위해 Tobin's q를 적용함으로써, Tobin's q를 통해 제시된 그룹을 기준으로 보안사고로 인한 주가변화와 평판손실을 분석하였다. 이러한 분석을 위해 수집된 데이터의 수집방법과 선정기준도 함께 제시한다.

3.1 데이터 수집

본 연구의 분석 데이터는 2005년 5월부터 2014년 5월까지 국내에서 발생된 보안사고 중 언론에 보도된 기사를 대상으로 하였다. 보안사고 기사의 검색을 위한 주요 키워드는 '해킹', '사이버공격', '인터넷침해', '정보유출', '개인정보', '기업비밀유출', '피싱', '악성코드', '디도스' 등을 사용하여 검색하였다. 한 사건에 대해 복수의 기사가 검색되는 경우 최초 발표를 기준으로 하였고, 단일 보안사고 기사에 복수의 기업이 대상이면 개별사건으로 보았다. 단일 보안사고가 복수의 기업에 피해 발생 시 각 기업의 피해 정도가 다르고, 분석 대상이 각 기업의 가치변화를 측정하는 것이므로 독립사건으로 반영하였다.

보안사고 관련기사는 네이버 뉴스 검색 사이트에서 국내 종합 일간지(조선, 중앙, 동아, 경향, 국민, 문화, 세계, 연합뉴스, 한겨레, 한국일보), 경제일간지(머니투데이, 매일, 서울, 제일, 한국, 헤럴드, 파이낸셜뉴스, 이데일리), IT전문 신문(디지털 타임스, 전자신문, 아이뉴스 24, ZDNet Korea), 정보보호 뉴스(보안닷컴, 시큐데일리)에 실린 기사들을 대상으로 하였다. 언론에 공개된 총 125개의 보안사고 중 65개(공공기관 21개, 불특정대상 및 대상기업 확인불가 25개, 사고일자와 피해범위 불분명 및 외국계기업 등 19개)를 대상기준에서 제외하였고, 비상장기업(14)과 합병기업(2)을 제외한 총 52개의 보안사고 발생 기업을 대상으로 분석하였다. 주가의 변화분석을 통한 시장가치 측정을 위해 KOSPI (Korea Composite Stock Price Index)와 KOSDAQ (Korea Securities Dealers Automated Quotations)에 등록된 기업을 대상으로 하였다.

이러한 방법으로 수집 한 보안사고 기업을 독립데이터로 선정한 기준은 Table 2와 같고, 최종 분석대상으로 52개의 보안사고 기업을 산업별로 분류한 표는 Table 3과 같다. 최근 10년간 각 산업별 발생한 총 보안사고 회수는 유사하나, 2011년에는 정보통신(IT)에서 보안사고 발생이 증가하기도 하였고, 최근에는 모든 산업에서 증가하는 추세이다.

산업별 보안사고의 발생분포 현황은 Fig.1에서 확인할 수 있다. 제조업은 2010년 이전까지 기술정

Table 2. Sample selection criteria

Criteria	Number of an announcements	Companies remaining
Initial set of corporate information security breaches or attacked reports in major newspapers	125	127
After filtering announcements that were irrelevant, redundant, and non-Korean companies	65 (-60)	67
After filtering announcements associated with non-listed or thinly traded stocks or stocks with insufficient historical data or merger company	49 (-16)	52

Table 3. Industry distribution of security incidents

Classification	SIC	Description	Event	Distribution(%)
Manufacture/ Wholesale trade	26000	Manufacture of Electronic Components	1	17 events (32.7%)
	10000	Manufacture of Sugar	1	
	29000	Manufacture of Other Machinery and Equipment	1	
	30000	Manufacture of Electronic Components, Computer, Radio, Television and Communication Equipment and Apparatuses	3	
	26000	Manufacture of Electronic Components, Computer, Radio, Television and Communication Equipment and Apparatuses	4	
	35000	Electricity, gas, steam and air conditioning supply	1	
	46000	Wholesale Trade and Commission Trade, Except of Motor Vehicles and Motorcycles	1	
	47000	Department Stores	1	
	52000	Storage and support activities for transportation	2	
	72000	Architectural, Engineering and Other Scientific Technical Services	1	
	75000	Business Support Services	1	
IT/ Broadcasting	60000	Broadcasting	1	16 events (30.8%)
	61000	Telecommunications	7	
	63000	Information service activities	7	
	75000	Business Support Services	1	
Banking/ Insurance/ Stock	64000	Financial Institutions, Except Insurance and Pension Funding	12	19 events (36.5%)
	65000	Insurance and Pension Funding	1	
	66000	Activities Auxiliary to Financial Service and Insurance Activities	6	

보의 유출사고가 주로 발생하였고, 2011년부터는 인터넷 서비스의 성숙과 확대로 전기, 전자, 통신을 포함한 정보통신 기업 대상의 고객정보 유출사고가 주로 발생하였다. 최근에는 금융기관 대상의 보안사고가 주로 발생함에 따라, 금융기관의 보안사고 예방[36]과 금융기관 중심의 보안 Risk에 관한 연구[37] 등 금융권의 보안 예방에 관한 연구가 활발하게 진행되고 있다.

Fig.1의 보안사고 발생건수는 본 논문에 적용한

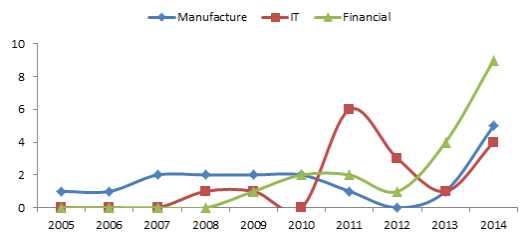

Fig.1. The number of security incidents changes by industry trends and per year from 2005~2014 May

방법론으로 분석 가능한 보안사고만을 대상으로 선정하였다. 인터넷침해대응센터(www.krcert.or.kr)의 2014년 6월 해킹사고 접수건수는 비상장기업, 공공기관, 외국계기업 등을 포함한 총 1,009건으로 기업별 시장가치의 변화분석이 어려운 소규모의 보안사고까지 모두 대상으로 하였다. 본 연구의 분석대상은 Table 2의 기준에 따라 발생한 52건의 중요 보안사고를 대상으로 기업의 시장가치 변화를 분석하였다.

3.2 사건연구 방법론과 평판손실 분석

3.2.1 사건연구방법론

사건연구방법론(event study methodology)은 특정 사고가 발생하거나 언론에 기사로 발표되어 그 사고가 주가에 미치는 영향을 연구하는 방법론으로, 기업성과에 직접적인 결과를 갖거나 기업의 실제 결점에 관련한 사건(event)의 가치영향분석에 주로 이용되었다. 사건연구 방법론은 주식시장이 효율적으

로 반응을 해야 하며, 기업의 주가는 시장에 즉시 반영되어야 한다는 가정을 기반으로 한다. 본 논문에서는 사건연구 방법론을 Fama 등[38]이 수립한 시장모델(market model)을 기본적으로 사용한다. 시장모델은 기업의 현재가치가 보유하고 있는 자산과 향후 기대할 수 있는 미래의 현금흐름을 함께 반영한 것으로 본다. Fama 등[38]은 또한 기업의 시장성과인 주가 등락율이 과거시점의 활용 가능한 정보가 반영된 기업의 현재 기대수입에 의해 예측될 수 있으며, 이러한 기대수익과 현재 실 주가수익의 차이를 기업의 초과수익(excess returns) 또는 비정상 수익(abnormal returns) 이라고 하였다. 비정상 수익률 도출을 위한 사고 전후의 정상수익률은 다음 식과 같다.

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + \epsilon_{i,t}, \quad (1)$$

$R_{i,t}$:주식 i의 t일 수익률
$R_{m,t}$: t일의 시장 포트폴리오 수익률
a_i:주식 i의 절편치, 고유위험
β_i: 주식 i의 베타계수, 기울기(slope)
ε_i:주식 i의 t일 오차항 또는 등락률

$\beta_i R_{m,t}$ 는 시장 전체의 변화에 따른 주식 i의 수익률 변화를 나타내며, 오차항은 시장 전체의 변화로 설명할 수 없는 특정기업 i의 t시점에 해당하는 수익률 변화를 설명하기 위한 항이다. $\square_i + \square_i R_{m,t}$는 특정 사건이 발생되기 이전 과거성과가 지속될 때 해당 기업이 얻게 되는 기대수익(expected return)을 의미한다. 시장포트폴리오 수익률$R_{m,t}$는 KOSPI, KOSDAQ에 해당하는 상장기업의 수익률을 의미한다. 비정상수익률 AR은 특정기업의 예상된 시장모델에서 예측된 오차범위를 벗어난 실 수익률이다. 오차예측으로 볼 수 있는 AR과 AR의 특정 기간을 누적한 누적비정상수익률인 CAR의 식은 각각 다음과 같다.

$$AR_{i,t} = R_{i,t} - (\hat{\alpha} + \hat{\beta} R_{m,t}), \quad (2)$$

$$CAR_i = \sum_{t=-5}^{5} AR_{i,t}, \quad (3)$$

총 52개의 사건 N을 반영하기 위한 평균 CAR은 다음 식과 같다.

$$\overline{CAR} = \frac{1}{N}\sum_{i=1}^{n} CAR_i . \quad (4)$$

3.2.2 평판손실 분석

본 연구에서는 평판손실을 분석하기 위해 Gillet 등[31]이 제시한 방법론과 보안사고 사건을 고려하여 분석한 Sinanaj 등[32]의 예상피해비용분석 식을 적용하였다. 즉, 평판손실은 기업 주식에 미친 영향을 손실 총 비용과 시가총액 비율을 합하여 평판손실로 정량화 하는 방식이다.

$$AR_{i,t}(Rep) = AR_{i,t} + (Expected\ Loss_i / MarketCap_{i,t}), \quad (5)$$

$AR_{i,t}(Rep)$= 주식 i의 t일에 비정상수익률에 데이터 유출 및 침해로 인한 피해 비용 반영,
$AR_{i,t}$ = 주식 i의 t일 비정상수익률,
$Expected\ Loss_i$ = 주식 i의 보안사고로 인해 발생한 직접/간접 비용(기대손실),
$Market\ Cap_{i,t}$ =주식 i의 t일 시가총액.

$AR_{i,t}$는 보안사고가 언론보도 이 후 주식시장에 반영된 측정치이며, $AR_{i,t}(Rep)$는 보안사고로 인한 손실을 반영한 주식의 변화를 표현한 것이다. 본 연구의 $Loss_i$는 보안사고 기사에서 예상 피해비용이 명시된 경우 해당 비용을 사용하였고, 명시되지 않은 경우에는 포네몬 연구소의 직/간접비용 산정방법[33]을 DataLossDB (www.datalossdb.org)에 적용하여 유출정보 건 당 $60로 반영한 방법을 사용하였다. 직접비용은 법무기업이나 서비스 보호에 소요된 비용 등 주어진 행위 달성에 소요된 경비를 의미하며, 간접비용은 총 소요 시간과 노력, 관련 조직에서 사용한 자원으로 보안사고 조사나 인지하기 위한 투입 인력의 활용에 해당한다[33].

DataLossDB의 피해비용 기준을 적용한 이유는 대량의 정보유출 사례가 잦은 국내 보안사고의 특성상 유출건수 별 피비용산정은 평판손실에 미치는 주요한 측정변수로 판단되었기 때문이다. 최근의 연구사례인 개인정보보호협회의 개인정보 침해로 인한 사회적 비용분석[39]에서 포네몬 연구소의 2013년 리포트가 제시한 측정방법은 해외의 보안사고사례 중 10만 건 미만의 유출사고에서 산정한 기준이므로, 국내 보안사고 주요 특징인 유출건수를 반영하지 않아 기업의 피해비용을 평판손실에 반영하는데 부적합

한 것으로 판단하였다. 또한, 보안사고의 특성 상 손실비용이 기업외부에 공개되지 않는 민감한 정보이기 때문에 정확한 피해비용의 산정에 제한이 있으므로, 불확실한 기업의 상황을 추정하는 방식보다 유출정보에 일관된 비용을 적용하여 기업의 평판손실을 단일 기준으로 분석하기 위함이다. 이러한 기준을 적용한 특정 기간 동안 누적된 평판의 누적비정상수익률인 $CAR_{i,t}(Rep)$은 다음 식과 같다.

$$CAR_i(Rep) = \sum_{t=-5}^{5} AR_{i,t}(Rep), \quad (6)$$

3.2.3 Tobin's q 분석

기업의 시장가치 대체비용을 정의하는 Tobin's q 산정은 Chung 등[40]의 연구를 토대로 하였다. Chung 등의 방법은 공시된 재정회계 정보를 이용하여 전통적 방법인 Lindenberg 등[24]의 방법보다 간단한 식으로 96.6%의 근사치 결과를 제공하였다. 본 논문에서는 Chung 등[40]의 계산을 IT 사건에 적용하여 Tobin's q 값을 도출한 Bharadwaj 등[25]의 식을 다음과 같이 적용하였다.

$$Tobin's\ \ q = (MVE + PS + DEBT)/TA. \quad (7)$$

MVE = 시가총액 = (회계년 말의 보통주 시장가격) (보통 주식수),*
PS = 우선주 청산가치 = (우선주의 시장가격)(우선주의 발생주식수),*
DEBT = (유동부채 - 유동자산) + (재고자산) + (장기차입금),
TA = 총자산.

MVE와 PS는 각각 연말 회계기준의 보통주와 우선주의 시장가치이며, DEBT와 TA는 장부가격을 사용한다. PS는 우선주 발생주식수와 우선주 시장가격을 곱한 결과를 청산가치로 정의하였다. 총자산은 자기자본과 부채를 포함한 타인자본을 합하였으며, 순자산은 총자산에서 부채를 제외하였다. 자기자본은 자본금, 자본잉여금, 이익잉여금, 자본조정을 합한 비용이며, 자본금은 총발생주식수과 액면가를 곱하였다. Tobin's q 결과는 1을 기준으로 기업의 가치를 평가하나, 본 연구에서는 전체 사건의 q범위를 세분화하여 분석하였다. 즉, 1보다 큰 기업과 0과 1사이의 기업, 그리고 0보다 작은 기업의 세 그룹으로 분류하여 q비율에 따라 보안사고가 미치는 다양한 변화를 분석하였다.

IV. 분석결과

4.1 사건연구방법론과 평판손실 분석 결과

Table 3에서 정리한 52개 기업을 대상으로 사건연구방법론과 평판손실 및 Tobin's q를 적용하여 기업의 가치 변화를 분석하고자 한다. 이 전의 사건연구 문헌들은 언론보도일 중심으로 전과 후의 21일을 주 분석대상으로 지정하였다. 분석기간이 단기간으로 지정되면 보안사고가 주가에 제대로 반영되지 않을 수 있어 선호하지 않으며, 장기간으로 설정하면 보안사고가 미치는 영향만을 분석하는데 다른 사건의 영향이 주가에 개입될 수 있다[41]. 보안사고의 사건연구방법론을 적용한 선행연구들은 주로 2일에서 3일의 사건연구기간(event window)을 사용함을 Table 1에서 확인할 수 있다. 본 논문의 사건연구 분석기간은 기존 국내보안사고를 연구한 Kwon 등[26]과 보안사고와 평판분석을 시도한 Sinanaj 등[32]에 적용한 분석 결과의 비교를 위해 언론보도일 기준의 -5일부터 +5일까지로 정의하였다. AR을 예측하여 실제 주가와의 차이를 도출하기 위한 주가 거래일(estimation period)은 주로 100일에서 300일을 사용한다. 본 연구는 AR을 예측하여 실제 주가와의 차이를 도출하기 위해 가장 일반적으로 사용하는 200일을 주가거래일 기준으로 사고발생 이전의 주가를 추정한다. 보안사고의 영향이 없도록 언론보도일 30일 전부터 200일 전에 해당하는 총 -230일을 주가거래일로 적용하였다[13].

사건연구 분석기간에서 언론보도 하루 전 날인 t-1을 기준일로 함으로써 사고정보의 사전 노출 가능성을 고려하였고[29], 언론보도 당일 [-1, 0]부터 사건 후 5일 [-1, +5]까지를 대상으로 분석하였다. Tobin's q를 산출하기 위한 재무제표는 사건 발생일에 해당하는 분기 재무제표를 반영하였다. 단, 보안사고 발생 일이 해당 분기의 재무제표에 영향을 미치기 어려운 3월, 6월, 9월, 12월의 15일 이후에 해당하는 경우, 다음 분기 재무제표와의 평균값으로 하였다. 본 논문에 적용한 방법론의 분석 기간은 Fig 2에 표현하였다.

Fig.3a는 52개 보안사고 발생 기업을 대상으로 보안사고 발생일(t일) 기준 전 후 5일간의 평균 비

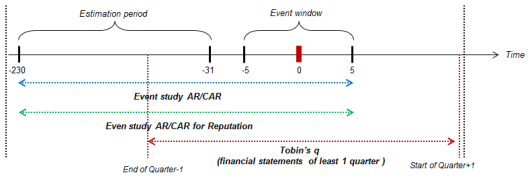

Fig. 2. Approaching windows for analysis of company's value

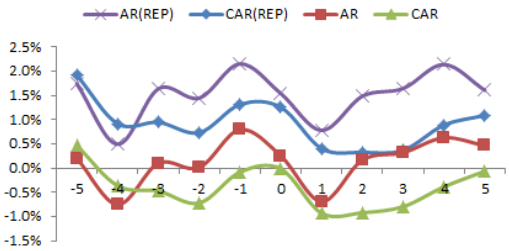

Fig. 3a. Analysis of AR, CAR and AR(RER), CAR(REP) of reputation loss on 52 events

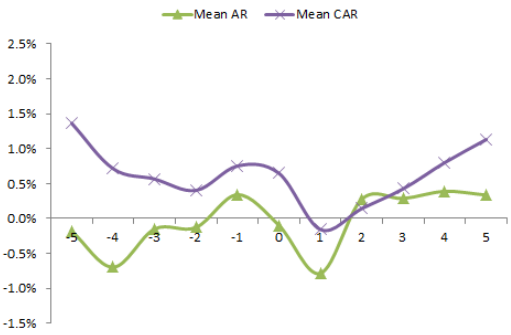

Fig. 3b. Analysis of Mean AR and Mean CAR of reputation loss on 37 events

정상 수익률(AR)과 평균 누적 비정상 수익률(CAR)을 분석하였다. AR은 사고의 언론보도 당일(t)부터 하락을 시작하여 +1일(t+1)에 가장 낮은 AR이며, +2일(t+2)부터 회복을 보였다. CAR은 AR의 누적값으로 AR과 유사하게 +1일(t+1)에 가장 낮으며 +5일(t+5)부터 회복하는 모습을 갖는다. 본 논문에서 분석한 AR과 CAR은 국내의 보안사고를 대상으로 한 Kwon 등[26]의 분석과 유사한 결과를 갖는다. Fig.3b는 평판손실을 분석하기 위해 보안사고 손실 비용이 확인된 37개 사건에 대한 Mean AR과 Mean CAR을 분석결과이다.

Fig.3a와 달리 Mean AR이 Mean CAR보다 높게 나타났고, Mean AR은 +1일(t+1)에 많은 하락이 발생하였다. Mean CAR은 Mean AR과 달리 +1일(t+1)에 잠시 하락했으나 +2일(t+2)부터 회복하였다. Sinanaj 등[32]의 분석결과는 AR(REP)는 +2일에 가장 많은 평판손실이 발생하였고 +5일까지 손실이 지속된 반면, 본 연구는 +1일에 가장 많은 손실이 발생한 후 +2일에 회복하는 차이를 보였다. 또한, CAR(REP)는 +5일까지 평판손실이 지속적으로 하락했으나, 국내의 보안사고로 인한 평판손실은 +1일에만 평판손실을 보인 후 바로 회복하는 차이를 확인할 수 있다.

Table 4는 보안사고의 언론보도 후 1일에 가장 많은 주가 하락이 발생함을 AR과 CAR에 대한 t검정통계량과 p-value를 통해 확인할 수 있다. Mean AR은 52개 기업별 -5일부터 +5일까지 도출한 각 날짜 별 평균 비정상수익률이며, Mean CAR은 52개 기업의 각 날짜 별 누적 AR의 평균을 의미한다. t검정통계량은 기업별 계산된 AR이 0인지를 검증하기 위한 통계량이다. Table 4에서 Mean AR과 Mean CAR은 사고발표일과 언론보도 후 1일에 낮은 값을 가지며, 2일후부터 조금씩 회복함을 확인할 수 있다. Mean AR과 Mean CAR은 전날 대비 변화의 크기를 비교하여 보안사고로 인한 주가의 변화를 파악할 수 있다. Mean AR의 경우 언론보도 5일 전과 4일 전의 경우 보안사고와 관련이 없으나 낮은 값을 갖는데, 이는 사고 이외의 다양한 요인이 주가에 영향을 미치기 시작함을 보인다. 특히, 보안사고의 언론발표 후 1일의 Mean AR은 -0.804, p-value는 0.001로 유의수준 0.05보다 낮으므로 보안사고가 기업가치에 통계적으

Table 4. Mean AR and Mean CAR of security incidents on 52 events

Date	Mean AR	t-value	p-value	Mean CAR
-5	-0.150	-0.554	0.582	1.433
-4	-0.700	-2.135	0.038	0.743
-3	-0.227	-0.655	0.515	0.519
-2	-0.111	-0.293	0.771	0.373
-1	0.365	0.932	0.356	0.748
0	-0.073	-0.198	0.844	0.668
+1	-0.804	-3.673	0.001	-0.155
+2	0.232	0.695	0.491	0.101
+3	0.329	1.202	0.235	0.427
+4	0.361	1.079	0.286	0.776
+5	0.387	1.518	0.135	1.157

Table 5. Tobin's q group and mean expected loss

Tobin's q group	Manufacture	IT	Financial	Mean Expected Loss (Million Won)	Mean Debt (Million Won)
Group A (0 〉 q)	-	-	7	32,241	-275,000,000
Group B (0 ≦ q ≦ 1)	4	8	7	210,567	7,000,000
Group C (q 〉 1)	4	5	2	526,696	-6,800,000

로 유의미한 영향을 미치는 것으로 볼 수 있다. 이러한 결과는 Kwon 등[26]이 분석한 AR과 동일하게 언론보도 후 1일이 가장 낮은 수치를 갖으며 통계적으로 유의한 p-value를 갖는다.

4.2 Tobin's q 그룹별 분석 결과

평판손실 분석을 위해 총 52개의 사건 중 예상손실비용이 확인된 37개 사건을 대상으로 하였다. 기존 Tobin's q는 기업을 1보다 큰 기업과 1보다 작은 기업으로 분류하나, 본 논문에서는 1보다 작은 기업을 두 그룹으로 세분화하여 q가 제시한 그룹 별 보안사고의 영향을 상세히 분석하였다. 세 그룹으로 나눈 기업의 분포와 평판손실분석의 예상기대손실을 그룹 별 평균한 결과는 Table 5와 같다. q가 0보다 작은 기업은 금융기업만으로 분포되었고, q가 1보다 크거나 0과 1사이의 기업은 제조, 정보통신(IT), 금융기업이 각각 분포한 것으로 확인되었다.

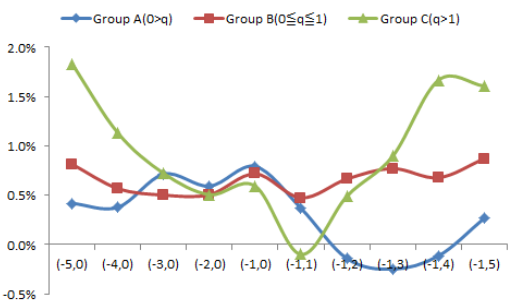

Fig. 4a. Mean CAR by Tobin's q group

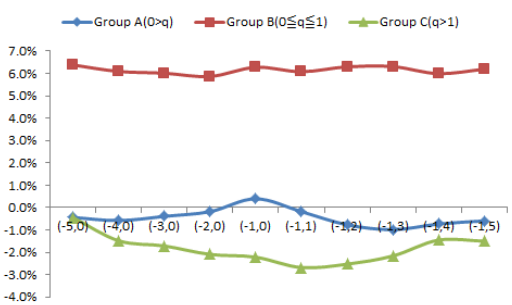

Fig. 4b. Mean CAR(REP) by Tobin's q group

특히, q에 따른 평균기대손실에서 많은 차이가 발생하는데, q가 1보다 큰 기업의 평균기대손실비용은 약 5,267억으로 q가 0보다 작은 기업의 322억과 비교시 약 16배에 해당함을 확인할 수 있다. 이러한 결과는 q가 높은 기업일수록 보안사고로 인한 평균기대손실이 q가 작은 기업보다 매우 높게 발생하는 것으로 볼 수 있다.

Tobin's q 그룹 별 평판손실 분석을 통해 각 q 그룹 기업의 피해규모와 평판손실을 확인할 수 있다. Fig.4a는 q 그룹 별 CAR을 비교한 것으로, Group A(0〉q)는 +1일부터 하락을 시작하여 +5일에는 회복하는 모습을 확인할 수 있다. Group B(0≦q≦1)는 큰 변화 없이 0.5%와 1% 사이를 유지하는 반면, Group C는 사건의 언론보도 당일(0)과 +1일에 가장 낮게 나타났으며 바로 회복하였다. Fig.4b는 q 그룹 별 평균 평판손실을 분석한 결과이다. Group A는 +1일부터 +2일에 주로 하락하여 +5일까지 하락상태를 유지하였고, Group C는 언론보도 당일부터 하락을 시작하여 +3일까지 하락을 유지하였고 +4일부터 회복하는 것을 확인할 수 있다. 반면 Group B는 보안사고로 인한 하락과 상관없이 6%~7%를 유지하였다. 이러한 현상은 Tobin's q의 각 변수들을 비교한 결과 Group B기업들의 평균부채(Mean Debt)가 약 7조원인 반면 Group A는 -27.5조, Group C는 -6.8조로 다른 변수와 비교하여 가장 많은 차이가 있음을 확인하였다.

각 Group 간 통계분석을 비교한 결과는 Table 6, Table 7, Table 8에서 각각 확인할 수 있다. Group A와 Group B의 평균 평판손실에 대한 통계분석 결과는 Table 6에서 확인할 수 있고, Group B와 Group C의 평균 평판손실에 대한 통계분석 결과는 Table 7에서 유의한 p-value를 확인할 수 있다. 반면 Group A와 Group C의 평판

Table 6. Analysis of Mean CAR(REP) by Tobin's q group : 0 〉 q, 0 ≦ q ≦ 1

Classification		[-1,0]	[-1,1]	[-1,2]	[-1,3]	[-1,4]	[-1,5]
Group A(0 〉 q)	Mean CAR(REP)	0.004	-0.002	-0.008	-0.010	-0.007	-0.006
Group B(0 ≦ q ≦ 1)		0.063	0.061	0.063	0.063	0.060	0.062
t-statistics	Mean difference	-0.059	-0.063	-0.071	-0.073	-0.067	-0.068
	t-value	-1.826	-1.879	-2.131	-2.129	-1.923	-2.010
	p-value	0.080*	0.072*	0.044**	0.044**	0.066*	0.056*

Significance levels: * p〈0.10, ** p〈0.05

Table 7. Analysis of Mean CAR(REP) by Tobin's q group : 0 ≦ q ≦ 1, q 〉 1

Classification		[-1,0]	[-1,1]	[-1,2]	[-1,3]	[-1,4]	[-1,5]
Group B(0 ≦ q ≦ 1)	Mean CAR(REP)	0.063	0.061	0.063	0.063	0.060	0.062
Group C(q 〉 1)		-0.022	-0.027	-0.025	-0.022	-0.015	-0.015
t-statistics	Mean difference	0.085	0.088	0.088	0.085	0.074	0.077
	t-value	2.778	2.848	2.924	2.804	2.501	2.665
	p-value	0.010***	0.008***	0.007***	0.009***	0.018**	0.013**

Significance levels: ** p〈0.05, *** p〈0.01

Table 8. Analysis of Mean CAR(REP) by Tobin's q group : 0 〉 q, q 〉 1

Classification		[-1,0]	[-1,1]	[-1,2]	[-1,3]	[-1,4]	[-1,5]
Group A(0 〉 q)	Mean CAR(REP)	0.004	-0.002	-0.008	-0.010	-0.007	-0.006
Group C(q 〉 1)		-0.022	-0.027	-0.025	-0.022	-0.015	-0.015
t-statistics	Mean difference	0.026	0.025	0.017	0.011	-0.009	0.009
	t-value	0.663	0.623	0.432	0.290	0.188	0.238
	p-value	0.517	0.542	0.671	0.776	0.853	0.815

손실은 유의한 결과가 발생하지 않음을 Table 8에서 확인할 수 있다. 각 테이블에서 분석기준인 [-1,0]부터 [-1,5]는 언론보도 발표 하루 전인 -1일을 기준으로 언론보도일(0일)부터 보도 5일 후(+5일)까지 각각 계산된 CAR(REP)를 평균한 값이다. 이러한 방법으로 각 Group 간 분석한 결과 Table 6과 Table 7에서 Group B가 Group A와 C에 비해 평판손실 결과에 많은 차이가 발생함을 확인하였다. 이러한 결과는 Tobin's q값으로는 설명할 수 없지만, Tobin's q의 부채변수인 Debt의 차이에서 분석결과를 해석할 수 있었다. 기업의 평판은 재무성과로부터 영향 받음을 주장한 Roberts와 Dowling[42]의 연구결과와 부채비율은 기업성과와 관계가 있고[43], 사회적 성과에도 영향을 미치는 선행연구[44]를 통해 부채가 기업평판에 미치는 요인으로 고려될 수 있다. 이러한 연구결과는 보안사고로인한 평판손실이 Tobin's q의 Debt 변수에 정의 관계가 있을 것으로 판단하였다.

Table 9는 2회 이상의 보안사고를 경험한 기업가치의 변화를 Tobin's q로 분석한 결과이다. 총 12개 기업의 28개 보안사고를 대상으로 분석하여 보안사고가 반복 될수록 Mean Tobin's q가 감소함을 확인할 수 있다. 통계적으로 정규분포의 가정을 적용하기에는 사건의 회수가 부족하지만, 2회 이상의 보안사고는

Table 9. Tobin's q change by multiple security incidents

The number of security incidents	The number of event	Mean Tobin's q
1st security incident	12	1.98
2nd security incidents	12	0.92
3rd security incidents	4	0.44

Tobin's q로 평가한 기업가치가 감소함을 Mean Tobin's q의 변화로 확인할 수 있다. 이러한 결과를 통해 보안사고의 재발은 기업 가치에 부정적인 영향을 미치는 것으로 결론지을 수 있다.

V. 결 론

5.1 연구결과 요약 및 시사점

본 연구는 보안사고로 인한 기업의 시장가치 변화를 재무관점에서 정량분석하였다. 객관적인 분석을 위해 공시된 주가정보와 재무제표 기반의 방법론을 적용하였다. 사건연구방법론은 보안사고로 인한 단기적인 주가하락을 증명하였고, 평판손실 분석을 통해 예상기대손실비용의 발생과 평판에 미치는 손실을 분석하여 제시하였다. 이러한 분석결과를 Tobin's q가 제시한 기업가치 기준의 세 그룹으로 분류하여 각 그룹이 갖는 특징을 중심으로 분석하였다.

Tobin's q가 제시한 기업의 각 그룹에 따라 평판손실의 정도에 많은 차이가 있음을 확인하였다. q가 1보다 크거나 0보다 작은 기업의 경우 0과 1사이의 기업보다 많은 평판손실이 발생하며, 통계적으로 유의미한 결과를 확인할 수 있었다. 이러한 결과는 상세한 추가분석이 필요하지만, Tobin's q의 부채변수가 많은 차이를 갖는 점에서 원인을 유추해 볼 수 있다. 본 논문의 분석결과는 부채와 기업평판은 직접적인 관계인 관계를 갖는 것으로 보지만, 연구사례가 없어 간접적인 양의 관계인 것으로 밝혀졌다. 부채비율은 기업의 장기부채 상환능력과 타인자본의 의존성 정보로 활용 가능하나, 기업의 평판에 미치는 직접적인 영향을 분석한 사례가 없고 보안사고로 인한 기업가치의 변화와 다른 연구 분야이므로 선행연구의 결과를 참고하여 결론을 도출하였다. 즉, 기업의 평판은 재무성과에 큰 영향을 받으며, 부채비율은 기업의 재무성과와 관계가 있을 뿐 아니라 사회적 성과에도 영향을 미침을 분석한 선행연구 결과에 따라 부채비가 적은 그룹($0 \leq q \leq 1$)은 그렇지 않은 그룹보다 보안사고로 인한 평판손실이 낮은 것으로 결론을 도출하였다.

기존의 연구들은 보안사고 기업의 분석방법론의 보완과 응용을 통해 피해의 정량 분석이 갖는 결과에 집중하였다. 하지만 본 연구는 보안사고 기업의 시장가치 평가방법론인 Tobin's q의 분석 기준으로 보안사고 기업 별 주가손실과 평판손실을 분석함으로써 국내 상장기업의 피해를 정량화하는 시도를 하였다. 이러한 연구의 결과는 q에 해당하는 기업의 수준에 맞게 정보보호의 비용과 노력을 효율적으로 투입할 수 있고, 재무제표 상 부채가 높은 기업은 IT Risk를 기업경영의 핵심요소로 고려해야 함을 제시하였다. 또한, 보안사고로 인한 사회적 영향과 사회비용의 추정 및 관련 정책의 제언과 제도개선사항의 발굴에도 활용할 수 있을 것으로 본다.

본 연구의 분석결과가 갖는 의미는 다음 두 가지로 정리할 수 있다. 첫 번째는 보안사고 기업을 대상으로 평판손실의 정량분석을 시도하였다. 평판손실예측 분석은 고객의 신뢰도에 민감한 금융산업에서 주로 활용된 분석방법으로, 지속적이며 급속도로 발전하는 IT환경에서 보안사고의 언론보도는 금융산업의 매출에 직간접적으로 영향을 미친다. 특히 보안사고는 서비스의 신뢰도 하락에 따른 기업의 평판손실에 직결되므로 평판손실 분석결과는 보안사고 예방을 위한 비용투자와 리소스 운영의 효율 측면에서 유용한 정보로 활용 가능하다. 두 번째는 Tobin's q 가 제시하는 기업가치의 활용범위를 확대하였다. 기업가치 판단을 위해 주로 활용된 Tobin's q는 보안사고 기업의 가치를 Tobin's q로 분류하여 주가와 평판손실을 도출함으로써 Tobin's q에 따른 예상기대손실비용과 평판손실이 갖는 의미를 분석하였다. 또한, 기업이 갖는 부채의 정도가 미치는 영향에도 평판의 변화에 차이가 있음을 간접적으로 제시하였다. 이러한 시도는 보안사고 시 기업에 발생할 수 있는 피해기준을 고려하여 보안투자를 계획하는데 유용한 정보로 활용 가능할 것이다.

5.2 향후연구의 방향

본 연구에서는 다음 네 가지 측면에서 연구의 한계점이 존재한다. 첫 번째는 평판분석에 이용된 보안사고 예상손실비용 산정방식의 정확성 부족이다. 언론보도에 언급된 피해비용은 해당기업의 주관성이 반영될 수 있으며, 이를 보완하기 위해 포네몬 연구소의 직/간접비용 방식을 적용한 DataLossDB의 유출정보 건 별 일괄비용 산정방식은 보안사고 기업별 정교한 피해비용의 반영에 부족함이 있다. 그러나 정교한 피해비용의 산정은 아니더라도 피해수준에 근거한 평판의 손실분석 시도는 보안사고로 인한 피해의 정도를 이해하는데 유용한 정보로 볼 수 있다. 두 번째는 보안사고 기업을 Tobin's q가 제시한 기준에

따라 그룹화하여 특성을 분석했으나, q가 0보다 크고 1보다 작은 기업이 갖는 평판손실의 직접적인 원인을 선행연구를 통한 객관적 사실로만 접근한 점이다. 해당 그룹들은 1년 이상의 장기간 동안 발생된 기업가치의 변화를 측정하기 위한 Tobin's q 변화 분석, 기업복원력 결정요인, 부채가 기업의 재무성과와 평판에 미치는 영향, 위험분석을 통한 피해복구 및 예방비용 산정 등 보다 상세한 추가 분석과 새로운 연구방법의 접근이 필요하다. 세 번째는 보안사고 분석 대상이 상장기업 뿐 아니라 비상장기업과 공공기관, 외국계기업이 많아 상대적으로 적은 상장기업만을 대상으로 다양한 통계적 접근과 분석의 시도에 제약이 따랐다. 하지만 현재의 연구방법론으로는 비상장기업, 공공기관, 외국계기업 등에 대해 기업의 가치를 평가하는 방법이 부족한 것이 현실이다. 마지막으로 각 산업별 보안사고로 인한 시사점으로 도출하는데 제한이 따랐다. 상장기업을 대상으로 하여 산업과 보안사고 등을 세분화하여 분석하기엔 분석대상이 부족하였으나, 금융기업과 제조업 등 각 산업이 갖는 특징에 따라 정보보호의 접근 방법의 차이를 분석한다면 이 또한 기업입장에서 도움이 될 수 있을 것으로 판단하였다.

IT강국인 대한민국에서 IT선진화에 따른 보안사고의 특징을 이해하고 대처하기 위해 학술연구의 지속적인 발전이 필요하다. 하지만 보안사고의 특성상 언론보도가 되지 않거나 사실의 왜곡이 가능하고 국내 사례의 부족으로 통계적인 접근의 한계가 있어 국외 사례를 보완하여 분석결과를 견고히 할 필요가 있다. 향후 연구에서는 이러한 예상기대손실비용 도출의 이론적 기반을 마련하고, 국내외 추가적인 사례발굴을 통하여 연구의 일반화와 함께 정보보호 예방에 관한 기준을 제시할 수 있을 것으로 본다. 또한, 본 연구에서 시도한 정량분석을 기반으로 정성분석을 추가하여 분석결과의 완성도를 높일 수 있을 것으로 예상한다. 본 연구에서 분석한 보안사고의 언론보도 기사의 내용이 기업가치에 미치는 피해를 근거이론(grounded theory)으로 분석한다면 정량분석 결과를 보완할 수 있을 것으로 기대한다.

References

[1] S.W. Chai, "Economic effects of personal information protection," Korea Consumer Agency, vol. 33, pp. 43-64, Apr. 2008.

[2] D.B. Parker, "The strategic values of information security in business," Computers & Security, pp. 572-582, Jun. 1997.

[3] L.A. Gordon and M.P.Loeb, "Economics of information security investment," ACM Transactions on Information and System Security, vol. 5, no. 4, pp. 438-457, Nov. 2002.

[4] R. Bojanc and B. Jerman-Blazic, "An economic modeling approach to information security risk management," International Journal of Information Management, vol. 28, pp. 413 - 422, Oct. 2008.

[5] S.W. Nam and J.I. Lim, "An empirical study on the impact of security events to the stock price in the analysis method of enterprise security investment effect," Ph.D. Thesis, Korea University, Feb. 2006.

[6] A. Bharadwaj, M. Keil and M. Mahring, "Effects of information technology failures on the market value of firms," Journal of Strategic Information Systems, vol. 18. pp. 66-79, Jun. 2009.

[7] K. Campbell, L.A. Gordon, M.P Loeb and L. Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," Journal of Computer Security, vol. 11, pp. 431-448. Mar. 2003.

[8] H. Cavusoglu, B. Mishra and S. Raghunathan, "The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers," International Journal of Electronic Commerce 9, pp. 69-104, Feb. 2002.

[9] K. Kannan, J. Rees and S. Sridhar, "Market reactions to information security breach announcements: an empirical analysis," International Journal of

Electronic Commerce, vol. 12, no. 1, pp. 69-91, Fall 2007.
[10] A. Hovav and J. D'Arcy, "The impact of denial-of-service attack announcements on the market value of firms," Risk Management and Insurance Review, vol. 6, pp. 97-121. Oct. 2003.
[11] A. Hovav and J. D'Arcy, "The impact of virus attack announcements on the market value of firms," Information System Security, vol. 13, no. 3, pp. 46-156. Dec. 2004.
[12] A. Hovav and J. D'Arcy, "Capital market reaction to defective IT products: the Case of Computer Viruses," Computers & Security, vol. 24, pp. 409-424. Aug. 2005.
[13] I. Bose and A.C.M. Leung, "The impact of adoption of identity theft countermeasures on firm value," Decision Support Systems, vol. 55, pp. 753-763, Jun. 2013.
[14] S. Goel and H.A. Shawky, "Estimating the Market Impact of Security Breach Announcements on Firm Values," Information & Management, vol. 46, pp. 404-410, Oct. 2009.
[15] M. Ko and C. Dorantes, "The impact of information security breaches on financial performance of the breached firms: an empirical investigation," Journal of Information Technology Management, vol. 17, pp. 3-29, Nov. 2006.
[16] A. Grag, J. Curtis and H. Halper, "Quantifying the financial impact of IT security breaches," Information Management and Computer Security, vol. 11, pp. 74-83. 2003.
[17] B. Jerlod and J.Stephen, "Using daily stock returns: the case of event studies," Journal of Financial Economics, vol. 14, pp. 3-31, Mar. 1985.
[18] A.G. Kotulic and J.G. Clark, "Why there aren't more information security research studies," Information and Management, vol. 41, pp. 597-607, May 2004.
[19] J. Perry and P.De. Fontnouvelle, "Measuring reputational risk: the market reaction to operational loss announcements," Federal Reserve Bank of Boston, Oct. 2005.
[20] Basel Committee on Banking Supervision, International convergence of capital measurement and capital standards. A Revised Framework. Comprehensive Version, Jun. 2006.
[21] Basel Committee on Banking Supervision, Proposed enhancements to the Basel II rramework, Consultative Document, Jan. 2009.
[22] F. Fiordelisi, M-G. Soana and P. Schwizer, "Reputational Losses and Operational Risk in Banking," The European Journal of Finance, vol. 20, pp. 1-20, Mar. 2011.
[23] Y. Konchitchki and D.E. O'Leary, "Event study methodologies in information systems research," International Journal of Account Information Systems 12, pp. 99-115, Jan. 2011.
[24] E.B. Lindenberg and S.A. Ross, "Tobin's q and industrial organization," The Journal of Business, vol. 54, no. 1, pp. 1-32, Jan. 1981.
[25] A.S. Bharadwaj, S.G. Bharadwaj and B.R. Konsynski, "Information technology effects on firm performance as measured by Tobin's q," Management Science, vol. 45, no. 6, pp. 1008-1024, Jun. 1999.
[26] Y.O. Kwon and B.D. Kim, "The effect of information security breach and security investment announcement on the market value of korean firms," Information System Review, 9(1), pp. 105-120, Apr. 2007.
[27] The Economist Intelligence Unit, Sharing the blame how companies are collaborating on data security breaches,

Jun. 2014.
[28] Juniper Networks, Juniper networks third annual mobile threats report, Jun. 2013.
[29] A. Hovav and J.Y. Han, "The impact of security breach announcements on the stock value of companies in south Korea," Korea Internet e-Commerce Association, vol. 13, pp. 43-67, Sep. 2013.
[30] S.H. Jeong, J.S. Yoon, J.I. Lim and K.H. Lee, "Study on the effect of information security investment executive," Journal of The Korea Institute of Information Security & Cryptology, 24(6), pp. 1271-1284, Dec. 2014.
[31] R. Gillet, G. Hubner and S.Plunus, "Operational risk and reputation in the financial industry," Journal of Banking and Finance, vol. 34, pp. 224-235, Jan. 2009.
[32] G. Sinanaj and J. Muntermann, "Assessing corporate reputational damage of data breaches: an empirical analysis," Association for Information System BLED 2013 Proceedings Paper 29, Jun. 2013.
[33] Ponemon Institute LLC, 2011 cost of data breach study, Traverse City, Mar. 2011.
[34] S. Bond, A. Klemm, R. Newton-Smith, M. Syed and G. Vllieghe, "The roles of expected profitability, Tobin's q and cash flow in econometric models of company investment," Bank of England Working Paper, vol. 43, Jun. 2004.
[35] H. Zafar, M. Ko and K. Osei-Bryson, "Does a CIO matter? Investigating the impact of IT security breaches on firm performance using Tobin's q," System Sciences, pp. 1-7, Jan. 2011.
[36] D.Y. Jeong, K.B. Lee and T.H. Park, "A study on improving the electronic financial fraud prevention service: focusing on an analysis of electronic financial fraud cases in 2013," Journal of The Korea Institute of Information Security & Cryptology, 24(6), pp. 1243-1261, Dec. 2014.
[37] C.L. Choi, J.H. Yun and K.H. Lee, "A study on IT outsourcing policy based on operational risks of financial industries," Journal of The Korea Institute of Information Security & Cryptology, 24(4), pp. 681-694, Aug. 2014.
[38] E.F. Fama, L. Fisher, M.C. Jensen and R. Roll, "The adjustment of stock price to new information," International Economic Review, vol. 10, no. 1, pp. 1-21, Feb. 1969.
[39] Korea Online Privacy Association, Social cost analysis of the personal information infringement and valuation, Nov. 2013.
[40] K.H. Chung and S.W. Pruitt, "A simple approximation of Tobin's q," Financial Management, vol. 23, no. 3, pp. 70-74, 1994.
[41] A. McWilliams and D. Siegel, "Event studies in management research: theoretical and empirical issues," Academy of Management Journal, vol. 40, no. 3, pp. 626 - 657, Jun. 1997.
[42] P.W. Roberts and G.R. Dowling, "Corporate reputation and sustained superior financial performance," Strategic Management Journal, vol. 23, pp. 1077-1093, Sep. 2002.
[43] J.B. McGuire, T. Schneeweis and B. Branch, "Perceptions of firm quality: a cause or result of firm performance," Journal of Management, vol. 16, no. 1, pp. 167-180, Mar. 1990.
[44] W.G. Simpson and T. Kohers, "The link between corporate social and financial performance: evidence from the banking industry," Journal of Business Ethics, vol. 35, pp. 97-109, Jan. 2002.

〈저자소개〉

황 해 수 (Haesu Hwang) 정회원
2001년 2월: 청주대학교 컴퓨터정보공학과 학사
2010년 2월: 성균관대학교 이동통신공학과 석사
2011년 3월~현재: 성균관대학교 기술경영학과 박사과정
〈관심분야〉 정보보호, 기업가치분석, 빅데이터보안

이 희 상 (Heesang Lee) 정회원
1985년 2월 서울대학교 공학사 (산업공학)
1985년 2월 서울대학교 대학원 공학석사 (산업공학)
1991년 Ph.D in Industrial and Systems Engineering,
Georgia Institute of Technology, Atlanta, GA, USA
현재) 성균관대학교 기술경영학과 교수, 시스템경영공학과 교수, 제약산업학과 겸임교수
1991년~1995년: KT, 선임연구원 (통신망연구소, 연구개발단)
1995년~2004년: 한국외국어대학교 산업공학과 조교수, 부교수
1999년~2000년: Visiting Scholar at DIMACS, NJ, USA
2002년~2003년: Editor of Int. Journal of Management Science
2004년~현재: 성균관대학교 기술경영학과 교수
〈관심분야〉 오픈 이노베이션, 기술전략, 기술경영 모델링