J. Soc. Korea Ind. Syst. Eng Vol. 38, No. 4 : 193-201, December 2015
http://dx.doi.org/10.11627/jkise.2015.38.4.193
ISSN : 2005-0461(print)
ISSN : 2287-7975(online)

A Study on Categorization of Accident Pattern for Organization's Information Security Strategy Establish

Hee-Ohl Kim* · Dong-Hyun Baek**†

*Graduate School of Management Consulting, Hanyang University
**Department of Business Administration, Hanyang University

기업 정보보안 전략 수립을 위한 보안 사고 유형 분류에 관한 연구

김희올* · 백동현**†

*한양대학교 일반대학원 경영컨설팅학과
**한양대학교 경상대학 경영학부

Corporation's valuable intelligent asset is being threatened from the skills of threatening subject that has been evolved along with the growth of the information system and the amount of the information asset. Domestically, attempts of various private information attacks, important information extortion, and information damage have been detected, and some of them have abused the vulnerability of security of information system, and have become a severe social problem that generates security incident. When accessing to the security, most of companies used to establish a strategy with a consistent manner and a solution plan. However, this is not a proper way. The order of priorities vary depending on the types of business. Also, the scale of damage varies significantly depending on the types of security incidents. And method of reaction and critical control point vary depending on the types of business and security incidents. In this study, I will define the security incidents by their types and preponderantly examine how one should react to those security incidents. In this study, analyzed many types of security accidents that can occur within a corporation and an organization considering various factors. Through this analysis, thought about factors that has to be considered by corporations and organizations when they intend to access to the information security. This study focuses on the response methodology based on the analysis of the case analysis of the leakage of industrial secret and private secret other than the conceptual response methodology that examines the way to prevent the leakage of the industry security systems and the industry information activities. And based on these factors, want to be of help for corporations to apply a reasonable approach when they establish a strategy to information security.

Keywords : Information Security, Security Incident, Accident Pattern, Categorization

Received 17 November 2015; Finally Revised 11 December 2015;
Accepted 14 December 2015
† Corresponding Author : estarbaek@hanyang.ac.kr

1. 서 론

갈수록 경쟁이 격화되는 오늘날 기업 환경 하에서 정보는 많은 조직들의 생명선과 같다. 그렇기 때문에 조직의 정보는 보호되어야 하고 알맞게 관리되어야 한다[4, 11, 32, 38]. 어떠한 이유에서든 만약 기업의 중요 정보가 손상된다면 기업은 시간을 낭비하게 되고 인력의 소모가 일어나며, 이에 따라 경제적인 손실과 함께 사업의 기회까지도 잃어버릴 수 있다[9, 47]. 이러한 정보를 보호하는 것을 일컫어 '정보보안'이라 한다. 정보보안의 주된 목적은 말 그대로 정보를 보호하는 것 이외에도 어떤 방식으로든 정보의 유용성, 기밀성, 무결성이 손상됨 없이 유지되어야 함에 있다[1, 11, 28, 31, 46]. 정보를 관리한다고 하는 것은 정보를 손상시킬 수 있는 위험이나 위협 그리고 취약성에 대해 사전에 대비하는 것을 말한다. 정보보안 업무는 기업에서 부가적인 업무로 다뤄질 것이 아니라 주 업무로써, 날마다 대비책을 세워야 하는 중요한 작업인 동시에 이제 경영상의 주요한 사안 중 하나가 되었다[5, 8, 25, 26, 33, 42, 48]. 이렇게 정보보안을 통해 기업 및 조직이 보유하고 있는 가치 있는 자산들을 보호함으로써 기업 및 조직이 받을 수 있는 피해는 최소화하고 이익과 비즈니스의 기회는 최대화 시킬 수 있다.

우리나라의 기업들 역시 정보보안의 중요성에 관한 인식이 점차 증가하면서 다양한 노력들을 기울이고 있다. 하지만, 그럼에도 불구하고 개인정보 유출 및 산업기밀 유출과 같은 정보보안 사고는 계속적으로 발생하고 있으며 그 빈도 또한 줄어들고 있지 않은 것이 현실이다. 방송통신위원회의 자료(2015)에 따르면 2011년 1월부터 2015년 7월까지 최근 4년 6개월 동안 개인정보 유출 사고가 신고된 정보통신 서비스 업체 107곳에서 최소 9,200만 건 이상의 개인정보가 유출된 것으로 나타났다. 이것은 우리나라 국민당 약 2번꼴로, 2011년 7월 홈페이지가 해킹된 SK커뮤니케이션즈가 3,500만 건, 게임 업체 넥슨코리아 1,300만 건, KT 1,170만 건 등이 포함된 수치이다. 또한 국가정보원 산업기밀 보호센터의 발표(2015)에 따르면 2010년부터 2014년까지 5년간 총 229건의 산업기밀 유출 피해가 발생했다. 기술 유출 예상 피해액수로는 30조 원 가까이가 추정되고 있는데 이는 2014년 국내 총생산(GDP)의 2%에 육박하는 수치이며, 2013년 중소기업 연평균 매출액인 107억으로 환산하면 2,800여 개의 중소기업 연 매출액과 비슷한 금액이다. 이와 같은 최근 조사결과는 우리나라 기업들의 취약한 정보보안 관리 현실을 적나라하게 보여주고 있다.

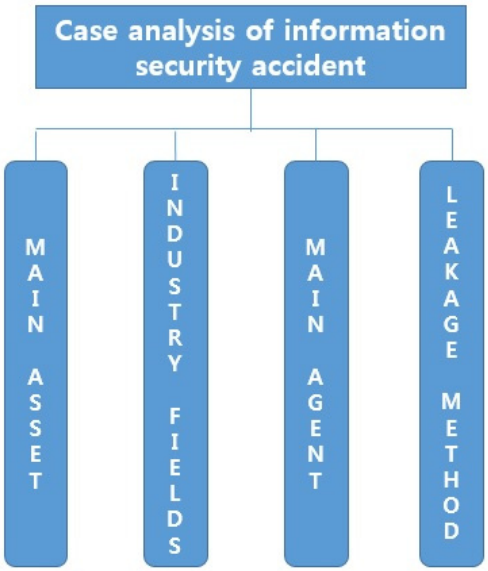
일반적으로 정보보안에 접근하고자 할 때 기업들은 기술 기반의 해결책에 의존하는 경향이 있다[7, 12, 29, 37, 40]. 이는 기업 내 정보시스템의 하드웨어, 소프트웨어, 네트워킹과 같은 기술적 자산에 대한 약점에 중점을 두고 있기 때문인데[13, 14, 15, 17, 28, 29, 36, 40, 45] 이러한 기술 중심의 정보보안은 해커나 바이러스와 같은 외부적인 위협에만 중점을 두고 있어 기업이 내부로부터의 위협이나 위험에 노출되도록 하고 있다[3, 6, 7, 10, 12, 22] 나날이 발전하고 있는 해킹, 바이러스와 같은 기술적 위협을 완벽하게 방어하는 것은 사실상 불가능하며, 이에 소모되는 비용 또한 우리나라의 기업 정서상 지속가능한 성장과 안정성에 대한 미래의 투자 개념이 아닌 소모성 비용으로 인식되고 있다[4, 12, 14, 18, 21, 23, 30, 34, 39, 44]. 이러한 소모성 비용이라는 인식을 바꾸려면 기업이 왜 보안에 투자를 해야 하고, 누가 집행할 것이며, 어디에 얼마나 투자해야 효과를 얻을 수 있는지에 대한 합리적인 데이터를 산출하기 위한 분석이 필요한데 이에 대한 연구는 거의 진행되지 않았을 뿐더러 개별 기업의 특성을 고려하지 않은 것들이 대부분이다[11, 15, 18, 21, 37, 40, 45].

정보보안이라고 해서 모든 기업들이 일관된 접근 방법을 사용하는 것은 효율적이지 않으며, 기본적으로 보안에 대한 인식자체가 턱없이 낮은 기업들이 대부분인 우리나라 기업 현실에서 개별 기업의 특성을 고려한 접근 방식과 해결 방안을 찾기 위한 이론적인 연구가 필요하다고 판단된다. 따라서 본 연구에서는 우선 2010년 1월부터 2015년 9월까지 최근 5년간 발생하여 기사화 되었던 정보보안 피해 사고 사례 131건을 수집하여 몇 가지의 분류 기준에 따라 분류하였고, 각각의 분류별로 어떤 특징을 보이는지 살펴보는 사례연구를 진행하였다. 그리고 사례연구를 통해 도출한 결과를 바탕으로 정보보안에 접근하고자 하는 기업의 상황에 맞는 전략 유형 틀을 제시하고자 하였다. 그리하여 기업들이 자사의 정보보안 전략을 수립할 때 의사결정을 지원할 수 있는 기반이 될 결과를 산출하는데 궁극적인 목적이 있다.

2. 정보보안 사고 사례 분석

정보보안 사고 사례 분석은 다음 <Figure 1>과 같이 4가지 분류 기준에 따라 진행하였으며, 각각의 분류 기준에 대한 근거와 자세한 사항은 각 항목별로 설명되어 있다.

2010년 1월부터 2015년 9월까지 수집된 131건의 정보보안 사고 관련 신문기사는 우리나라 최대 뉴스 포털인 네이버 뉴스에 기사화 되어있는 자료를 사용하였으며, 국가정보원 산업기밀보호센터의 통계 자료와 안랩, SK인포섹, 이글루시큐리티 등 IT정보보안 업체들의 리포트도 참고하였다.

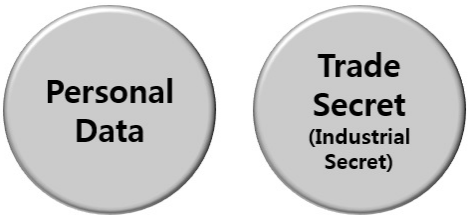


<Figure 1> Categorization of Accident Pattern

2.1 유출정보 유형별 분석 결과

기업 및 조직마다 핵심으로 여겨지는 자산의 종류는 다양하게 생각되어질 수 있다. 예를 들어 은행이나 카드사, 통신사와 같은 기업에서는 고객들의 신상정보가 중요한 자산으로 분류된다. 이름이나 휴대 전화번호는 물론이고 주민등록번호, 서명 등과 같은 식별 가능한 정보들이 여기에 포함된다. 공공기관의 경우에도 마찬가지이다. 최근 문제가 된 의료정보 유출사고의 경우 환자의 의료보험 정보 및 진료기록이 해커에 의해 공격 받았으며 결제에 사용된 카드정보와 비밀번호 또한 유출된 것으로 나타났다. 이 외에도 통계, 판례, 특허, 관세 등의 공공 개인정보가 위협 받을 수 있는 환경에 공공연히 노출되어 있다. 전자, 정보통신 분야의 경우 기업이 보유한 영업 비밀이나 설계도면, 첨단 기술 등이 중요한 자산으로 분류되어질 수 있다. 특히 반도체 기술이나 휴대폰의 주요 기술의 유출과 같은 경우 우리가 뉴스에서 빈번하게 접하는 정보보안 침해 사건 중의 하나이다. 실제 사고 사례에서 전자기업의 경우 첨단 휴대폰 혹은 반도체 기술이 유출되는 사례가 있었고, 자동차 제조 기업의 경우 자동차에 장착될 부품이나 첨단 기술이 해외로 유출된 사례가 있었다. 또한 2014년 말, 해커에 의해 원자력 발전소의 도면이 유출되는 사고도 발생 되었다. 이처럼 정보보안 사고는 산업의 구분, 규모를 가리지 않고 일어나고 있으며 공공기관 역시 피해에서 자유롭지 못하다.

본 연구에서는 이것을 <Figure 2>와 같이 크게 개인정보, 영업비밀(산업기밀)의 2가지로 사례들을 분류하였다.



<Figure 2> Type of Information

여기서 개인정보(Personal Data)라 함은 생존하는 개인에 관한 정보로서 성명·주민 등록 번호 등에 의하여 개인을 식별할 수 있는 정보(해당하는 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함)를 이야기 한다[27]. 영업비밀(Trade Secret)은 공유된 공공의 정보를 기반으로 하지 않은 제조법, 도안, 데이터 수집방법 등 비즈니스에 사용되는 지적 생산품을 의미하는데, 일반적으로 알려지지 않았고 비밀로서 유지하기 위한 합리적인 노력의 대상이 되는 것을 의미한다[43].

<Table 1>과 같이 131건 중 개인정보를 노린 피해 유형은 78건으로 절반을 넘는 비율을 차지하고 있었다. 그리고 첨단 핵심 기술이나 도면 등의 영업 비밀을 노린 유형은 53건으로 41% 정도였다.

<Table 1> Analysis Result by Main Asset

Accident Pattern	Number	Ratio
Personal data	78	59%
Trade secret	53	41%
Total	131	100%

2.2 산업 분야별 분석 결과

다음으로 표본이 된 131건의 보안 사고는 어떤 산업 분야에서 발생했는지 <Table 2>와 같이 분석해 보았다. 산업 분야 분류를 위한 기준은 통계청에서 발표한 제9차 한국표준산업분류(KSIC)에 근거하여 대분류 항목을 기준으로 살펴보았다. 가장 많은 정보보안 사고가 발생한 분야는 제조업으로, 50건의 보안 사고를 당한 것으로 나타났다. 특히 많이 알려진 대기업 보다는 중소기업에서 많은 피해가 발생한 것을 확인할 수 있었다. 대기업의 경우 기업 내 정보보안을 관리하는 부서가 별도로 존재하거나, 적어도 보안 시스템을 구축함에 있어서 예산을 책정하는데 중소기업보다 수월하다는 각종 분석을 통해 위와 같은 결과가 나온 것이 아닌가 예상해볼 수 있었다. 또한 정부에서 일정 수준 이상의 기업들에게 의무적으로 보안 관련 인증을 수행할 것을 강조하고 있는 추세이기

때문에 대기업들이 중소기업에 비해 피해를 줄일 수 있었을 것으로 생각된다. 하지만 특히 중소 제조기업의 경우 정보보안 분야에 투자가 인색할뿐더러 보안 인식 자체가 확립되지 않은 곳이 대부분이다. 특히 내부직원에 의한 피해 사례가 대부분을 차지했는데, 임직원들의 보안의식 부족이나 회사의 처우에 대한 불만, 금전적인 이득을 노리고 기업의 영업 비밀을 유출한 경우가 많았다.

<Table 2> Analysis Result by Industry Fields

Industry Fields	Number	Ratio
Manufacturing	50	38%
Information Service	22	17%
Financial and Insurance	19	15%
Wholesale and Retail	15	12%
Public Institution	12	9%
Facilities and Business Support Service	4	3%
Technology Service	2	1.5%
Private Service	2	1.5%
etc	3	2.3%
Total	131	100%

제조업 다음으로 보안 사고가 많이 발생한 분야는 정보서비스 분야로 22건이 발생하였다. 정보서비스 분야는 개인 정보와 첨단 산업 기술 두 가지 모두가 피해 대상이었다. 정보통신기술이 하루가 다르게 고도화, 첨단화되고 있고 글로벌하게 경쟁이 심화되다 보니 그만큼 보안을 위협하는 요소들이 많아진 것을 확인할 수 있었다. 정보서비스업의 경우 내부자의 소행이 대부분이었던 제조업과는 달리 해커의 기술적인 침입, 즉 해킹으로 피해를 입은 기업들이 대다수를 차지하였다. 다음으로는 19건이 발생한 금융 및 보험업으로 여기에는 은행, 카드사, 보험사 등이 해당되는데 미디어를 통해 우리가 자주 접하는 사건들이 대다수 포함되었다. 인터넷이 활성화 되고 개인정보는 이제 기업들의 중요한 자산으로서 인식되는 시대가 되었다. google, facebook, ebay 등 IT기업의 가치는 검색 알고리즘이나 특허 등 무형의 기술도 중요하지만 역시 사용자와 고객들로부터 수집한 개인 정보의 가치가 핵심이라고 볼 수 있다. 금융 및 보험업에는 이러한 개인 정보가 방대하게 쌓여있고, 개인의 경제적인 측면과 관련된 그래서 이를 노리는 이들이 크게 관심을 가지만한 정보들이 대부분이다. 15건이 발생한 도매 및 소매업의 경우 유통과정에서 발생하는 회원정보들이 해킹의 대상이 되었다. 그 외에 공공기관, 시설/사업지원 서비스업, 기술서비스업, 개인서비스업 등의 분야에서 보안사고가 발생하였다.

2.3 보안사고 주체별 분석 결과

그렇다면 보안 사고를 일으키는 주체는 어떤 이들인지 알아보았다. <Table 3>을 보면 해커에 의한 해킹 피해가 가장 많을 것이라는 예상과는 달리 가장 높은 비율을 차지한 것은 내부 직원에 의한 사고였다.

<Table 3> Analysis Result by Main agent of Security Accident

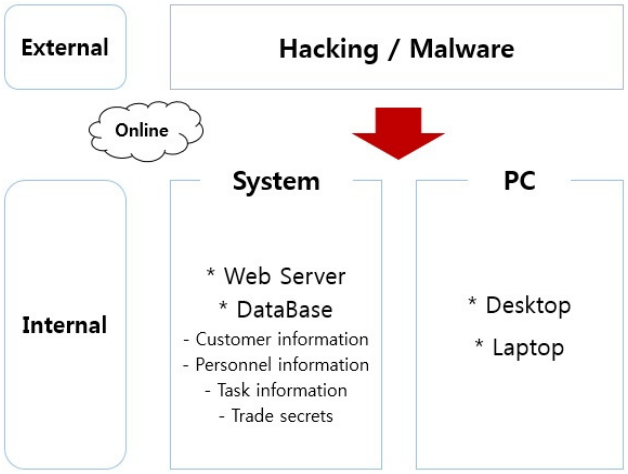
Industry Fields		Number	Ratio
Insider	Incumbent	34	26%
	Former	30	23%
Hacker		47	36%
Subcontractor		20	15%
Total		131	100%

131건 중 64건으로 거의 절반에 가까운 수치를 나타냈는데, 그 중 경쟁사로의 이직, 내부자 재 창업 등으로 사고 피해 기업을 퇴사한 전직 직원들의 경우 30건, 현재 피해 기업에 종사하고 있는 현직 직원에 의해 발생한 피해가 34건이었다. 전직 직원들의 경우 퇴사 이전부터 정보를 유출할 목적으로 기업 내의 정보자산들을 보조기억매체(USB, 외장하드 등)에 복사하거나 인쇄물로 출력하는 경우 또는 이메일로 전송하는 방식으로 개인정보 혹은 영업 비밀을 유출한 것으로 나타났다. 또한 경쟁사로 이직한 후에 전 직장동료였던 현직 직원들과 수시로 접촉하면서 직·간접적으로 기업 내 정보에 접근이 가능했기 때문에 고의적이든 무의식적이든 보안사고를 일으키는 경우가 많았다. 현직 직원들의 경우에도 정보를 유출하는 방법은 비슷했는데, 대부분의 경우가 금전적인 유혹과 같은 개인의 영리를 목적으로 이루어졌다. 이것은 기본적으로 임직원들의 보안에 대한 인식이 낮기 때문에 일어나는 것이라고 예상할 수 있었다. 최근 정보보안에 대한 연구들에서 첨단 기술 혹은 원천기술을 보유한 기업들의 인적 보안 노력의 중요성에 대해 지적하고 있는데 이번 연구에서도 역시 인적 보안의 중요성, 그리고 교육을 통한 임직원들의 보안 의식 함양에 대한 의지가 기업 내의 보안 사고를 감소시키는데 있어서 중요한 요소가 될 수 있음을 시사 하였다. 47건이 발생한 해킹 피해에서 해커들이 주로 노리는 것은 기업들이 가지고 있는 고객들의 개인정보였다. 개인정보의 경우 1차적으로 금융정보, 의료정보 등 금전적으로 이득을 취할 수 있는 고급 정보인 동시에 추가적으로 보이스 피싱, 스미싱, 파밍 등 최근 들어서 빈도가 높게 발생하고 있는 2차 사이버 범죄에 이용될 수 있는 정보이기 때문에 해커들의 좋은 먹잇감이 되고 있다고

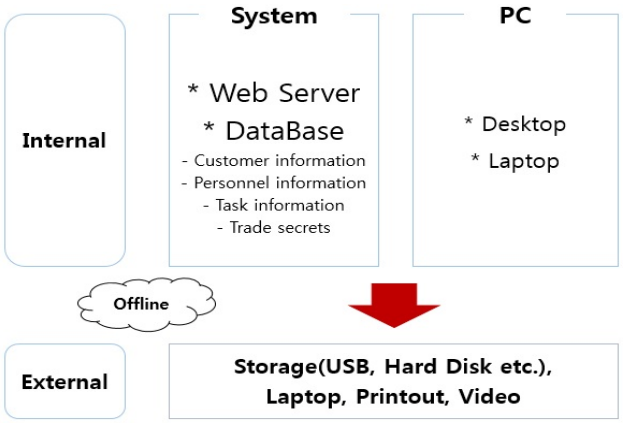
예상해볼 수 있다. 정부와 보안 관련 전문 업체에서 해킹 피해를 막기 위해 기술적으로 많은 노력을 기울이고 있지만, 해킹 기술은 하루가 다르게 발전하고 있고 점차 고도화 되고 있는 추세이다. 보안과 관련하여 가장 엄격한 규제를 적용하는 금융권에서 해킹 피해가 가장 빈번하게 발생하는 현실은 어떻게 막고, 어떻게 뚫어내는지에 대한 경쟁이라고 볼 수 있을 정도로 치밀하게 대비하지 않거나 '이정도면 괜찮겠지' 라는 마음가짐으로 접근한다면 보안사고가 발생할 수 있다는 점을 발견할 수 있었다. 그 외에 협력업체 혹은 외주업체로부터 사고가 발생한 경우가 20건으로 집계되었는데, 이 역시 금전적인 목적으로 계약 기간이 끝난 이후에 보조기억매체에 무단으로 복제하거나 이메일 등을 통해 아무런 제지 없이 정보를 유출한 경우였다.

2.4 정보유출 방법에 따른 분석 결과

정보를 유출하는 방법에는 여러 가지 방법이 있다. 앞서 언급한 해킹과 같은 방법으로 기업 내의 데이터베이스 혹은 네트워크 서버를 공격한 방법이 있을 것이고, 보조기억장치(USB, 외장하드 등)를 이용하는 방법, 이메일로 전송하거나 웹하드에 업로드 하는 방법 등이 있다. 본 연구에서는 <Figure 3>, <Figure 4>와 같이 이것을 크게 기술적인 방법(Technical method) 과 물리적인 방법(Physical method)으로 구분하였다. 기술적인 방법이라 하는 것은 기업 외부에서 내부로 연결된 망을 통해 기업 내 응용시스템, 서버, 네트워크, 데이터베이스 등을 공격하여 정보에 대한 위협을 가하는 것을 의미하고, 물리적인 방법이란 정보 시스템을 물리적인 방법, 즉 절도, 파괴, 화재 등과 같은 방법으로 정보에 위협을 가하는 것을 의미한다[16].



<Figure 3> Technical Method



<Figure 4> Physical Method

131건의 보안사고 사례를 분석한 결과 다음의 <Table 4>와 같이 분류되었다.

<Table 4> Analysis Result by Information Leakage Method

Leakage Method	Number	Ratio
Physical	84	64%
Technical	47	36%
Total	131	100%

47건이 발생한 기술적인 방법에 의한 보안사고는 온라인망을 통해 해커에 의해 기업 내 정보시스템 서버와 데이터베이스, 업무용 PC 등이 해킹을 당하거나 악성코드에 감염되어 보안 피해가 발생하는 유형이다. 이 같은 경우 기업 내부자의 도움 없이도 해커의 개인적인 능력에 의해 보안 피해가 발생할 수 있다는 특징이 있다. 기업 내의 시스템이나 업무용 PC가 온라인으로 외부와 연결되어 있기만 하다면 해커는 유출하고자 하는 정보에 무리 없이 접근이 가능했다. 47건의 기술적인 방법에 의한 보안사고 모두가 이에 해당 되었는데 금융정보, 게임관련 회원정보, 공인 인증서, 최근에는 국가 공공기관에서 관리하는 핵심 도면까지 유출되는 사례도 있었다. 또한 최초 피해를 당한 이후에 제대로 대비를 하지 않아 악성코드 등에 의한 2차 피해를 입은 기업들도 상당수 존재했다. 최근들어 금융 및 보험업계나 인터넷 정보통신 서비스 관련 기업들이 정보보호를 위해 기술적으로 많은 투자를 하고 있지만 해킹 기술 또한 나날이 발전하고 있기 때문에 정부와 기업 입장에서 좀 더 신중한 자세로 접근하는 것이 필요하다는 것을 확인할 수 있었다. 나머지 84건의 사고는 물리적인 방법에 의해서 사고가 발생한 경우였다. 현재 가장 광범위하게 발생하고 있는 보안 사고의 유형인데, 기업 내부에 있는 직원 혹은 외부 협력업체의 직원이 고의로 업무용 PC에서 보조기억장치(USB, 외장하드 등)

로의 자료를 이동시키거나 인쇄, 복사 그리고 촬영 등의 행동으로 외부로 반출하는 행위가 모두 포함된다. 휴대가 간편할뿐더러 과학 기술의 발달로 인해 조그만 장치에 엄청난 용량의 파일을 저장할 수 있는 USB와 외장하드(HDD)는 보안성에 끊임없는 문제에도 불구하고 가장 광범위하게 사용되고 있는 저장장치이다. 사고 사례 중에는 의도적으로 중요 정보를 유출한 경우는 물론이고 실수로 USB를 분실하였거나 USB 자체 내에 악성코드나 바이러스를 침투시켜 정보를 빼내는 경우도 있었다. 또한 업무용 노트북을 기업 밖으로 반출하는 경우 일부 대기업에서는 X-ray 검색기 등 통제수단을 사용하여 노트북 자체의 외부 반출을 막고 있지만 이것 역시 대다수의 기업들은 물리적인 환경 혹은 경제적인 요건 때문에 도입되지 못하고 있는 실정이다. 다만 업무상으로 불가피하게 자료를 이동하고 인쇄 등을 해야 하는 경우 중요한 정보에는 허가된 장비만이 접근할 수 있도록 시스템을 만들고 정보의 이동을 모니터링 할 수 있는 솔루션을 도입하여 보안 사고를 예방하는 전략이 필요할 것으로 보인다. USB와 노트북, 편리성과 효율성을 동시에 만족시켜주는 장치임에는 분명하지만 많은 보안사고 사례를 보면서 그만큼 정보보안의 중요성 또한 만족시키기 위해 많은 노력을 기울여야 할 것임을 시사하고 있다.

3. 산업 분야별 사고 사례 종합

지금까지 2010년 1월부터 2015년 9월까지 최근 5년간 발생하여 기사화 되었던 정보보안 피해 사고 사례 131건을 몇 가지 분류 기준에 따라 분류하였고, 각각의 분류별로 어떤 특징을 보이는지 살펴보았다. 그렇다면 사고가 가장 많이 발생했었던 상위 4개 산업분야(제조업, 정보서비스업, 금융 및 보험업, 도매 및 소매업)에 대한 사고의 유형을 종합적으로 알아보고자 한다.

제조업은 기업의 영업비밀(95%)을 내부직원(86%)이 물리적인 방법(98%)으로 피해를 입힌 경우가 가장 높게 나타났다.

정보서비스업은 기업 내의 개인정보 자산(95%)을 외부 해커(77%)가 해킹 등의 기술적인 방법(82%)으로 피해를 입힌 경우가 가장 높게 나타났다.

금융 및 보험업에서는 100%의 비율로 개인정보를 협력업체(36%) 직원이 물리적인 방법(53%)으로 피해를 입힌 경우가 가장 높게 나타났는데, 사고주체와 유출방법에 대해서 가장 높게 나타난 항목과 다른 항목들 간에 차이가 크지 않았다는 특징을 보였다.

도매 및 소매업의 경우 금융 및 보험업과 마찬가지로 개인정보(100%)를 협력업체 직원(80%)이 기술적인 방법(80%)을 이용해서 피해를 입힌 비율이 가장 높게 나타났다.

<Table 5> The Manufacturing Industry

Type of Information	Ratio	Main Agent	Ratio	Leakage Method	Ratio
Personal Data	4%	**Insider**	**86%**	Technical	2%
Trade Secret	**96%**	Hacker	2%	**Physical**	**98%**
		Subcontractor	12%		

<Table 6> The Information Services Industry

Type of Information	Ratio	Main Agent	Ratio	Leakage Method	Ratio
Personal Data	**95%**	Insider	18%	**Technical**	**82%**
Trade Secret	5%	**Hacker**	**77%**	Physical	18%
		Subcontractor	5%		

<Table 7> The Finance and Insurance Industry

Type of Information	Ratio	Main Agent	Ratio	Leakage Method	Ratio
Personal Data	**100%**	Insider	32%	Technical	47%
Trade Secret	0%	Hacker	32%	**Physical**	**53%**
		Subcontractor	**36%**		

<Table 8> The Wholesale and Retail Industry

Type of Information	Ratio	Main Agent	Ratio	Leakage Method	Ratio
Personal Data	**100%**	Insider	13%	**Technical**	**80%**
Trade Secret	0%	Hacker	7%	Physical	20%
		Subcontractor	**80%**		

정보보안 사고가 가장 많이 발생했던 4개 분야에 대해 종합적으로 알아본 결과 각각의 산업별로 발생 유형에서 조금씩 차이를 보이는 것을 확인할 수 있었다. 제조업의 경우 개인정보 보다는 영업비밀 혹은 산업기밀이 주요 타깃이 된다는 특징을 보였고, 나머지 3개 분야는 개인정보가 유출되는 유형이 가장 많았지만 유출되는 방법이나 주체가 각각 다르다는 특징이 나타났다. 종합한 결과로 보아, 기업 혹은 크게 봐서 산업별로 정보보안에 대한 전략을 수립하고자 할 때 각기 다른 전략을 가지고 접근해야 효과를 극대화 할 수 있음을 확인할 수 있었다.

4. 결 론

본 연구는 기업 및 조직 내에서 발생할 수 있는 보안사고 유형에 대해 여러 가지 요인들을 고려하여 사고 사례를 분석하였다. 서두에 밝혔듯 정보보안에 대해 모든 기업들이 일관적인 접근 방법과 해결 방안을 가지고 전략을 세우는 것은 올바른 방법이 아니다. 각각의 기업이 어떤 분야에서 활동하고 있고, 현재 가장 중요하게 여기고 있는 자산은 어떤 것들이 있는지, 또한 그 중에서 핵심적으로 지켜내야 하는 자산은 어떤 것인지 등을 전반적으로 살펴서 기업의 특성과 유형에 따라 정보보안 전략을 수립하는 것이 필요하다. 그간 기술적인 대책 위주의 많은 연구와 노력에도 불구하고 정보보안 사고는 끊임없이 발생했으며, 기업이 경제활동을 멈추지 않는 한 계속해서 발생할 것으로 예상된다. 다양하고 지능화 되고 있는 각종 공격을 기술적인 방법으로만 막아내기에는 한계가 분명 존재하므로 향후에는 피해를 막아낼 수 있는 현실적인 대응 역량을 높이는 데 집중할 필요가 있다. 본 연구에서 수행한 보안사고 분석에서 나타난 특징을 고려하여 정보보안을 위한 다양한 대응 전략과 방안을 지속적으로 탐구하는 것이 요구된다. 분석 결과 대부분의 기업들은 기업 내의 중요한 정보들을 보호하기 위해 많은 노력을 기울이지 않는 모습을 보였다. 또한 정부의 규제만을 피해서 최소한의 보안에만 신경을 쓰고 피해가 발생할 경우 피해를 축소시키기에만 급급한 모습이었다. 어차피 보안에 대한 투자를 투자가 아닌 비용으로 인식한다면, 그래서 많은 비용을 책정할 것이 아니라면 보안에 대해 정확히 알고 각자의 기업의 특성에 대해 정확히 분석하여 가장 효율적인 방안으로 보안에 접근하는 것이 필요하다.

기업이 경제적인 활동을 계속하고 보호하고자 하는 자산이 존재하는 한 정보보안에 대한 이슈는 끊임없이 지속될 것이다. 향후 연구에서는 본 연구에서 분류한 보안사고 유형에 따라 최적의 대응 방법을 연구하여 정보보안에 접근하고자 하는 기업이 가장 효율적인 전략을 세울 수 있도록 도움을 주고자 한다.

References

[1] Aljifri, H. and Navarro, D.S., International Legal Aspects of Cryptography. *Computers and Security*, 2003, Vol. 22, No. 3, pp. 196-203.

[2] Announcement on National Industrial Security Center, NISC, 2015.

[3] Besnard, D. and Arief, B., Computer security impaired by legitimate user. *Computers and Security*, 2004, pp. 253-264.

[4] Bharadwaj, A. and Keil, M. and Mahring, M., Effects of Information Technology Failures on the Market Value of Firms. *The Journal of Strategic Information Systems archive*, 2009, Vol. 18, No. 2, pp. 66-79.

[5] Brancheau, J.C., Janz, B.D., and Wetherbe, J.C., Key Issues in Information Systems Management : 1994-95 SIM Delphi Results. *MIS Quarterly*, 1996, Vol. 20, No. 2, pp. 225-242.

[6] Broderick, J.S., Information Security Risk Management-When should it be Managed?. *Information Security Technical Report*, 2001, Vol. 6, No. 3, pp. 12-18.

[7] Calder, A. and Van Bom, J., Implementing Information Security Based on ISO 27001/ISO 17799. Van Haren Publishing, 2006.

[8] Cavusoglu, H. and Raghunathan, S., Economics of IT Security Management : Four Improvements to Current Security Practices. *Communications of the Association for Information Systems*, 2004, Vol. 14, No. 3.

[9] Deloitte, Touche and Tohmatsu (2005). Global Security Survey, Available at : www.deloitte.com.

[10] Dhillon, G. and Moores, S., Computer Crimes : Theorizing about the Enemy within. *Computers and Security*, 2001, Vol. 20, No. 8, pp. 715-723.

[11] Doherty, N.F. and Fulford, H., Do Information Security Policies Reduce the Incidence of Security Breaches : An Exploratory Analysis. *Information Resources Management Journal*, 2005, Vol. 4, pp. 21-38.

[12] Ettredge, M. and Richardson, V.J., Information Transfer among Internet Firms: the Case of Hacker Attacks. *Journal of Information Systems*, 2003, Vol. 17, No. 2, pp. 71-82.

[13] Finne, T., Information Systems Risk Management : Key Concepts and Business Processes. *Computer and Security*; 2000, Vol. 19, No. 3, pp. 234-42.

[14] Flint, D.J., Woodruff, R.B. and Gardial, S.F., Exploring the Phenomenon of Customers Desired Value Change in a Business-to-Business Context. *Journal of Marketing*, 2002, Vol. 66, pp. 102-117.

[15] Hagen, J.M. and Albrechtsen et al., Implementation and Effectiveness of Organizational Information Security Measures. *Information Management and Computer Security*, 2008, Vol. 16, No. 4, pp. 377-397.

[16] Halliday, S., Badenhorst, K., and von Solms, R., A Business Approach to Effective Information Technology Risk Analysis and Management. *Information Management and Computer Security*, 1996, Vol. 4, No. 1, pp. 19-31.

[17] Hawkins, S. and Yen, D.C., Awareness and Challenges of Internet Security. *Information Management and Computer Security*, 2000, Vol. 8, No. 3, pp. 131-143.

[18] Hu, Q., Hart, P., and Cooke, D., The Role of External and Internal Influences on Information Systems Security Practices : An Institutional Perspective. *The Journal of Strategic Information Systems Archive*, 2006, Vol. 16, No. 2, pp. 153-172.

[19] Information Security Specialist's CISSP Note, 2012.

[20] Jahner, S. and Krcmar, H., Beyond Technical Aspects of Information Security : Risk Culture as a Success Factor for IT Risk Management, AMCIS 2005 Proceedings, 2005, p. 462.

[21] Karyda, M., Kiountouzis, E., and Kokolakis, S., Information security policies : a contextual perspective. *Computers and Security*, 2005, pp. 246-260.

[22] Kim et al., Implication of Industrial Security Capacity Based on Level Evaluation. *Journal of the Korean Society for Quality Management*, 2013, Vol. 41, No. 4, pp. 649-658.

[23] Korea Communications Commission Report, A Fact-Finding on Leak Out of Personal Data, KCC, 2015.

[24] Kotulic, A.J. and J.G. Clark, Why There aren't more Information Security Research Studies. *Information and Management*, 2004, Vol. 41, No. 5, pp. 597-607.

[25] Lebek, B., Degirmenci, K., and Breitner, M.H., Investigating the Influence of Security, Privacy, and Legal Concerns on Employees Intention to Use BYOD Mobile Devices, Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, Illinois, 2005, pp. 15-17.

[26] Lee, A.S., Retrospect and Prospect : Information Systems Research in the Last and Next Twenty-Five Years. *Journal of Information Technology*, 2010, Vol. 25, No. 4, pp. 336-348.

[27] Lee, J.H., Shin, W.S., and Park, H.J., A Study on Improvement Plans for Technology Protection of SMEs in Korea. *Journal of Society of Korea Industrial and Systems Engineering*, 2014, Vol. 37, No. 2, pp. 77-84.

[28] Lewis, A., Time to Elevate IT Security to the Boardroom. *e Secure*, 2000, Vol. 1, No. 1, p. 28.

[29] Lohmeyer, D.F., McCrory, J., and Pogreb, S., *Managing Information Security*, The McKinsey Quarterly, Special Edition : Risk and Resilience, 2002, Vol. 2, pp. 12-16.

[30] National Defense Science and Technology Vocabulary, 2011.

[31] National Institute of Standards and Technology, An Introduction to Computer Security : The NIST Handbook, Special Publication, 2000, pp. 800-12.

[32] NIST, Information Security Handbook : A Guide for Managers, 2006.

[33] Peppard, J., The Conundrum of IT Management. *European Journal of Information Systems*, 2007, pp. 336-345.

[34] Pfhleeger, C.P., Security in Computing, Second edn, Prentice Hall, United States of America, 1997.

[35] Posthumus, S. and Von Solms, R., A Framework for the Governance of Information Security. *Computers and Security*, 2004, Vol. 23, No. 8, pp. 638-646.

[36] Ransbotham, S. and Mitra, S., Choice and Chance : A Conceptual Model of Paths to Information Security Compromise. *Information Systems Research*, 2009, Vol. 20, No. 1, pp. 121-139.

[37] Sarker, S., Lau, F., and Sahay, S., Using an Adapted Grounded Theory Approach for Inductive Theory Building About Virtual Team Development. *DATA BASE for Advances in Information Systems*, 2001, Vol. 2, No. 1, pp. 38-56.

[38] Smith, E., Kritzinger, E., Oosthuizen, H.J., and Von Solms, S.H., Information Security Education, in Proceedings of the WISE 4 Conference, Moscow, Russia, 2004.

[39] Son, J.Y. and Benbasat, I., Organizational Buyer's Adoption and Use of B2B Electronic Marketplace : Efficiency and Legitimacy-Oriented Perspectives. *Journal of Management Information Systems*, 2007, Vol. 24, No. 1, pp. 55-99.

[40] Spears, J.L. and Barki, H., User Participation in Information Systems Security Risk Management. *MIS Quarterly*, 2010, pp. 503-522.

[41] Squara, D., LAN Security will become a Priority in the Networks of Tomorrow. Available at: http://itweb.co.za. 29, 2000.

[42] Stiles, P. and Taylor, B., *Boards at work : How directors view their roles and responsibilities*. Oxford : Oxford University Press, 2001.

[43] Straub, D. and Welke, R., Coping with Systems Risk : Security Planning Models for Management Decision Making. *MIS Quarterly*, 1998, Vol. 22, No. 4, pp. 441-469.

[44] The 9th Korean Standard Industrial Classification, 2007.
[45] Thomson, M.E. and Von Solms, R., Information Security Awareness : Educating Your Users Effectively. *Information Management and Computer Security*, 1998, Vol. 6, No. 4, pp. 167-173.
[46] Unfair Competition Prevention and Business Secret Protection Law, 2007.
[47] Vidgen, R. and Wang, X., Coevolving Systems and the Organization of Agile Software Development. *Information Systems Research*, 2009, Vol. 20, No. 3, pp. 355-376.
[48] Von Solms, R. and Von Solms, S.H., From policies to culture. *Computers and Security*, 2004, Vol. 23, No. 4, pp. 275-279.
[49] Von Solms, S.H., Information Security Management through Measurement, in Prodeedings of the SEC99 conference, Johannesburg, South-Africa, 1999.
[50] Whiteman, W. and Mattord, H.J., Principles of Information Security, Thomson-Course Technology, Canada, 2003.
[51] Wood, C.C., Why Information Security is Now Multi-Disciplinary, Multi-Departmental, and Multi-Organizational in Nature. *Computer Fraud and Security*, 2004, No. 1, pp. 16-17.

ORCID

Dong-Hyun Baek | http://orcid.org/0000-0002-3107-9511
Hee-Ohl Kim | http://orcid.org/0000-0001-8600-4528