전자무역연구, 제6권 제1호(2008.05.31)
E-Trade Review, Vol.6, No.1(May 31, 2008)
pp.1-37.

전자상거래 기업 환경에서의 시스템 사용자의 정보보안에 대한 인식 연구

The Study on the Information Security Awareness of Information System Users in the Electronic Commerce Environment

강성민*(Sung-Min Kang) · 송은수(Eun-Soo Song)**

Abstract

Due to the rapidly changing information technology(IT) and popularity of using the personal computer, we have been enjoying convenience in our life with fast growth in economy. But, it also provoked a series of problems such as hacking, malicious program distribution, illegal exposure of personal information, etc. At the same time, we are losing the sense of information security because we are caught up mostly on positive benefits of IT. In fact, modern society is encountered with adverse effects of information age that are caused by the serious infringement of confidentiality, integrity, and security. In this study, we examine the status quo of organizational IT environment with respect to security by conducting the study on main information system users, who are employed in the foreign companies and domestic companies separately. This study also makes suggestions in order to better protect the valuable information asset of an organization and emphasizes the importance of information awareness to common users, especially in electronic commerce environment.

Key Words: Information Security, Information System Users, Information Security Training Program

국문초록

우리는 정보통신 기술의 급속한 발전과 대중화로 생활의 편리함을 누릴 수 있게 되었고, 이를 바탕으로 경제적으로 빠른 성장을 하였으나 컴퓨터 시스템 해킹, 악의적인 프로그램 유포, 정보보안에 대한 인식 부족으로 인해 정보시스템의 비밀성, 무결성, 보안성이 손상되어 개인 및 기업에게 경제적 손실을 가져다주는 정보화의 역효과가 심각히 드러나고 있다. 이에 본 연구에서는 우리나라의 정보보안 현황 등에 대한 이론적 고찰을 통해 우리나라의 정보 침해 및 내부 사용자 보안의 중요성 등에 대하여 파악하고, 정보시스템을 다루고 있는 주요 주체인 정보 사용자들을 대상으로 설문 조사를 함으로서 전자상거래 환경에서의 정보보안 인식이 국내 기업 종사자와 외국기업 종사자 간 차이가 있는가를 확인함과 동시에 밝혀진 문제 내용에 대해 사용자들에게 정보보안에 대한 의식을 강조하는데 목적이 있다.

주제어: 정보보안, 정보이용자, 정보보안 교육

논문접수일: 2008. 04. 15. 심사완료일: 2008. 05. 20 게재확정일: 2008. 05. 26.

*중앙대학교 경영학부 부교수, 주저자
**중앙대학교 국제경영대학원 석사, 공동저자

목 차

Ⅰ. 서론

우리나라는 2007년 국가정보원, 정보통신부의 국가정보화백서에서 2005년 기준으로 국가정보화지수에서 3위로 평가되었는데 이는 초고속인터넷가입자수 1위, 인터넷 이용자 수 3위, CATV 가입자 수 3위를 함으로서 2004년 보다 전체 순위가 4계단이나 상승하였다.[1] 오늘날 정보통신시스템을 활용하여 인터넷 뱅킹이나 온라인 쇼핑몰에서의 거래, 그리고 인터넷을 이용해 우리가 원하는 정보를 손쉽게 사용함으로서 정보이용의 질적 향상을 가져온 것은 물론이거니와 우리가 사회생활을 해 나가는데 있어 필수적인 생활의 도구로 자리하였음을 부인할 수 없을 것이다. 분명 가정에서, 회사에서, 학교에서 그리고 놀이장소에서 이러한 편리한 혜택을 제공하는 정보시스템의 이면에는 일반 사용자들이 간과해 왔던 부정적이고 다소 위협스러운 부분이 존재하고 있으며, 그 위협이 위험으로 발전하여 우리의 일상을 침해하고 회사에는 막대한 경제적 손실을 입히고 있는 사례를 매체를 통하여 우리는 종종 듣는다. 컴퓨터 시스템의 해킹, 악의적인 프로그램의 유포, 정보보안에 대한 인식 부족으로 인해 정보시스템의 비밀성, 무결성, 보안성이 손상되어 개인 및 기업에게 경제적 손실을 안겨 줄 뿐 아니라, 스팸메일이나 허위 자료 등의 유포로 정보의 바다는 오염되거나 그 가치를 상실하게 됨으로서 원래의 그 취지에 역행하는 사례가 바로 그 예라 할 수 있겠다. 이런 사례들로 말미암아 정보시스템을 사용하는데 있어 사용자에게 직, 간접적으로 피해를 주고 정보화 사회의 발전을 심각히 저해하고 있는 것이다. 이에 본 연구에서는 전자상거래 환경에서 정보시스템을 다루고 있는 주요 주체인 사용자들을 대상으로 그들의 정보관리수준, 정보보안 의식과 정보보안교육에 대한 인식조사를 통해 현재의 상황을 알아보고자 하며, 연구 조사를 통해 밝혀진 내용을 가지고 사용자들에게 정보보안에 대한 의식을 강조하고, 중요한 정보자산의 보호에 대해 제안하고자 하였다.

이 연구는 기존의 정보보안 시스템 분석, 정책, 방법론 등 다양하고 많은 접근 방식 중 외국계 기업과 국내 기업의 정보 사용자의 정보관리에 대한 인식 수준, 정보보안 의식 그리

1) 한국전산원, 「2007 국가정보화백서」, 2007.

고 정보보안교육에 대한 인식의 차이가 있는가를 확인하는 것이다. 대한상공회의소에서 2002년에 발표된 연구보고서[2]에 따르면 국내 기업의 위기관리 수준이 90%가 초보단계인데 비해, 외국계 기업의 31%는 중급단계 이상으로 실질적인 위기관리에 있어 외국계 기업이 더 앞서는 것으로 조사 된 것과 삼성경제연구소(SERI) CEO Information 472호[3]에 반도체, 휴대폰 등 IT분야를 중심으로 외국기업에 의한 기술유출 시도가 급증하고 있으나 일부 대기업을 제외하고는 대부분의 국내 기업들이 보안의식 및 대응능력이 취약하다고 하였다. 이로 미뤄 볼 때 본 연구자는 외국계 기업의 종사자가 국내 기업의 종사자보다 연구문제 1, 2, 3에 대해 더 잘 수행하고 있다는 가정을 해 본다. 기업의 위기관리 실태에서 나온 결과와 우리나라의 정보보안의 역사보다 오래된 선진국가의 정보보호 기술과 정책을 현지 기업에 잘 접목하였으리라는 이유에서이다. 따라서 본 연구자는 두 그룹 간의 정보관리의 격차를 확인하고 연구 과제를 달성하기 위하여 다음과 같은 연구문제를 설정하였으며 또한 이 연구의 결과를 가지고 정보의 사용자들에게 그 방향을 제시하고자 한다.

연구문제 1. 정보이용자의 정보관리에 대한 인식 수준은 어떠하며 외국계 기업 종사자와 국내 기업 종사자간 차이가 있는가?

연구문제 2. 정보이용자의 정보보안의식은 어떠하며 외국계 기업 종사자와 국내 기업 종사자간 차이가 있는가?

연구문제 3. 정보이용자의 정보보안교육에 대한 인식은 어떠하며 외국계 기업 종사자와 국내 기업 종사자간 차이가 있는가?

본 논문은 제1장에서는 서론으로 연구의 필요성과 연구문제를 논의하며 본 연구의 방향을 제시하였다. 제2장에서는 이론적 배경으로 정보와 정보보안의 정의, 정보보안의 요소, 정보 침해 원인과 현황에 대해 확인하여 정보이용자들의 정보보안 인식에 대한 필요성을 제안하였다. 제3장에서는 위에 제시한 이론적 배경을 바탕으로 국내 기업 종사자와 외국 기업 종사자의 정보 이용자를 대상으로 한 실증분석의 연구 방법을 제시하였다. 제4장에서는 연구방법에 근거하여 파악된 실증 데이터를 빈도분석, 교차분석 등의 통계처리 기법을 이용하여 정보이용자의 개인정보관리, 정보보안의식 및 정보보안교육에 대한 인식을 파악하고 이러한 인식이 국내 기업 종사자와 외국기업 종사자간 차이가 있는가를 조사하였다. 마지막으로 제5장은 사용자들에게 정보보안에 대한 의식 및 중요한 정보 자산의 보호를 강조하며, 이를 위하여 정부와 개인 및 사업자들이 노력해야 할 사항에 대한 제안을 통해 결론을 맺었다.

2) 대한상공회의소, 「국내 기업과 외국계 기업의 위기관리 실태 및 대응방안 비교조사 , 2002.11.
3) 임영모 외 2인, “CEO Information”, 제472호, 삼성경제연구소(SERI), 2004.10.20.

II. 이론적 배경

1. 정보와 정보보안의 정의

정보란 무엇인가? 우리가 흔히 사용하는 정보화시대, 정보의 홍수 등등 정보가 들어가는 말은 흔한 일이 되어 버렸다. 이를테면 아침에 일어나면 뉴스를 통해 기상정보를 듣고, 출근하면서 교통정보를 접하며, 회사에서는 판매정보 또는 마케팅 정보를 가지고 계획을 실행에 옮긴다. 일과 후에는 증권정보를 통해 투자한 증권의 가격 상승과 판매 시점에 대해 알아보고, 피곤해지는 저녁 무렵이면 건강에 관련된 정보를 찾아 피로를 효과적으로 풀고 몸을 보할 수 있는 웰빙(Well-being) 정보를 인터넷이나 책 또는 다른 매체들을 통하여 접하고 있다. 이처럼 정보는 우리 주변을 구성하고 있는 의미 있는 사실 자료들이다. 연세 한국어 사전에 의하면 정보는 “어떤 사실에 대한 지식”, “어떤 비밀의 사실이나 상황에 관한 자세한 지식이나 보고나 자료”라고 한다. 또한 행정법-정보화촉진기본법(1995) 제 2조[4]에 의하면 “정보라 함은 자연인 또는 법인이 특정 목적을 위하여 광 또는 전자적 방식으로 처리하여 부호. 문자. 음성. 음향 및 영상 등으로 표현한 모든 종류의 자료 또는 지식을 말한다.” 라고 언급되어 있다. 이로 미루어 볼 때 정보는 요구되는 형태에 따라 처리될 수 있는 어떤 가치를 가지고 있는 사실 자료라 할 수 있겠다. 정보의 의미를 나타내는데 커다란 분기점으로 대두된 것은 정보산업이 사회를 주도함에 따라 정보통신 기기를 통해 전달되는 내용 모두가 정보라고 일컫는 것이 보편화 되었고 따라서 정보는 입력, 가공, 출력의 과정을 거치면서 새로운 아이디어나 전략을 창조하고 사업성과를 창출하게 된다.[5]

위에서 언급된 정보로 미뤄보아 정보보안은 “정보의 가치나 속성이 상실되거나 방해받지 않도록 위협으로부터 보호하고, 오용과 남용을 방지하기 위한 수단과 방책을 강구하는 행위” 라고 볼 수 있겠다. 여기서 위협(Threats)이란 자산에 피해를 줄 수 있는 위험의 원천이다.[6] 위협은 사용자의 부주의, 실수, 무관심, 오·남용과 같은 형태로 나타나는 내부적 위협과 시스템 밖에서 일어나는 해킹, 바이러스, 자연재해 등의 외부적 위협으로 나눠볼 수 있다.[7] (이종삼, 1995)[8]에 의한 형태별, 장소별, 의도별 위협의 분류를 아래의 <표 1>에 정리

4) 행정법, 정보화촉진기본법, 1995년 8월 4일, 법률 제4969호, 1995.
5) 배홍문, “정보보안에 대한 경제적 고찰과 정책방안에 관한 연구”, 서강대학교 경제대학원 석사학위논문, 1997.
6) 김기윤・나관식・김종석, “보안관리를 위한 위협, 자산, 취약성의 분류체계”, 「한국통신정보보호학회지」, 제5권 제2호, 한국통신정보보호학회, 1995.06.
7) 신용섭, “교사의 정보보호 및 보안의식에 대한 실태 분석”, 춘천교육대학교 춘천교육대학원 교육학석사학위논문, 2005.
8) 이종삼, “국내 기업 정보시스템 Security 위협 요소에 관한 연구”, 중앙대학교 국제경영대학원 석사학위논문, 1995.

하여 본다.

<표 1> 위협에 대한 형태, 장소, 의도별 분류표

의도 / 장소	유		무
내부	범죄	프라이버시 침해	고장 및 오류
외부			재해

자료: 이종삼, “국내 기업 정보시스템 Security 위협 요소에 관한 연구”, 중앙대학교 국제경영대학원 석사학위 논문, 1995

아울러 정보화촉진기본법 제2조 정의에서 “정보보호라 함은 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손을 방지하기 위한 관리적. 기술적 수단을 강구하는 것을 말한다.”고 언급하고 있다. 다소 혼용되어 사용되고 있는 정보보안과 정보보호의 개념을 정리하자면 정보보안(Information Security)은 협의의 수단적 개념으로 정보 자체의 완전성, 즉 그 안전성(Safety)과 무결성(Integrity)의 보전을 의미하고, 정보보호(Information Protection)는 정보보안을 포함한 포괄적인 개념이라 볼 수 있다.[9] 정보보안과 정보보호의 비교를 한국정보센터의 비교를 빌어 다음의 <표 2>와 같이 정리하여 본다.

<표 2> 정보보안과 정보보호의 비교

구분	정보보안(Information Security)	정보보호(Information Protection)
적용	전산망 시스템 보안, 해킹방지 암호설정, 인증	국가정보보호, 개인정보보호, 기업단체정보보호
성격	완전성(안전성, 무결성) 보전	비밀성 보장
정의	정보의 가치가 상실되지 않도록 보호하기 위한 제반 수단과 대책을 강구하기 위한 행위	정보의 정상적인 유지를 위해 물리적, 기술적, 자연적인 장애기능을 사전예방, 사후 회복 조치

자료: 한국정보보호센터, 1997, 박주흠의 2002년 논문에서 재인용

2. 정보 보호의 요소

정보 보호의 일반화된 정의로 “정보시스템의 보안은 정보시스템의 자원의 무결성, 기밀성, 가용성을 관리하기 위해 수립되는 통제구조”라 한다. 또한 정보보호의 기본적인 목표는 내부 또는 외부의 침입에 의해 행해지는 각종 정보의 파괴, 변조 및 유출등과 같은 정보 범죄로부터 중요한 정보를 보호하는 것이다.[10] 무결성(Integrity)이란 자료가 정해진 절차에 의

9) 박주흠, “정보이용자들의 특성에 따른 정보보안의식에 관한 연구”, 계명대학교 경영대학원 석사학위 논문, 2002.

해 그리고 주어진 적절한 권한에 의해서만 변경이 되어야 하고 의도적이나 비의도적으로 변경 또는 파괴되지 않는 특성을 의미하는데 이를 방지하기 위해 물리적인 통제와 접근제어가 필요하고 또한 이런 변경이나 위험을 탐지하여 적발할 수 있는 수단이 필요하다. 기밀성(Confidentiality)은 보안성 또는 비밀성이라고도 표현되며 정보가 비 인가된 개인, 개체들에게 노출되거나 공개되지 않는 특성을 의미한다. 가용성(Availability)은 사용자가 관련된 정보를 요구할 때 자원에의 접근과 사용을 가능하게 해 주는 특성을 의미한다.[11] 무결성, 비밀성, 가용성 중에서의 우선순위는 조직의 특성과 업종에 따라 달라질 수 있으며 그 필요에 따라 달라질 것이다.

일반적으로 시스템들은 여러 가지 문제점(Computer Crime, Information Abuse, Natural Disaster, System Outrage, Malfunction, Destruction, Error, etc.) 에 노출되어 있으며 외부의 공격 및 내부인의 남용으로부터 취약하기 때문에 우리는 100% 정보 보안은 어렵다고 주장한다. 항상 정보 보안에 있어 가장 큰 문제는 사용자로부터 발생한다. 정보 보안은 관리적 보안, 시스템적 보안, 그리고 기술적 보안으로 크게 3개의 영역으로 나뉘어 구분된다. 관리적 보안은 보안 절차 및 프로세스의 정립 및 실행을 강조하며 시스템적 보안은 보안 문화 및 제도/교육의 중요성에 무게를 둔다. 또한 기술적 보안은 물리적/기계적 접근을 통한 기업의 자산 보호를 의미한다.[12] 시스템 사용에 있어서 사용자들이 많은 실수를 하기 때문에 기업의 보안 수준을 높이는데 있어 시스템적 보안은 중요한 부분을 차지한다. 아무리 기능적으로 우수한 시스템이 있어도 사용자의 인식 전환이 없으면 시스템의 활용도 및 업무 성과를 높이는데 있어 지속적인 어려움에 직면한다. 시스템 사용에 있어 일반 사용자는 무지 또는 관심 부족으로 인하여 실수를 하게 되며 단순한 실수 하나가 기업 측면에서는 큰 피해가 발생할 수 있는 원인이 된다. 개인의 무지 및 관심 부족으로 인하여 시스템 사용에 있어 준수되어야 하는 절차가 안 지켜지고 무시된다면 기업은 비즈니스 차원에서 큰 피해를 입을 수 있다.

따라서 기업의 입장에서는 최대한 효과적인 보안 체계를 수립하여야 하며 이를 위해서는 항상 시스템 취약점 및 남용에 대비하여야 하며 시스템 품질 유지 및 보증에 대한 지원을 하여야 한다. 또한, 효과적인 보안 통제 환경을 제공하기 위해서 기업들은 데이터 및 시스템의 관리 방법, 관리 절차, 관리 기준 및 관리 정의를 수립하여 구성원들에게 지속적인 보안 교육을 실시하여야 한다.

---

10) 호순근, “정보보호 인식제고 현황조사 및 시스템 구축방안 연구”, 동국대학교 국제정보대학원 석사학위논문, 2004.

11) 김현수, “정보보안수준 계량화 연구”, 「경영정보학연구」, 제9권 제4호, 한국경영정보학회, 1999.

12) Kenneth C. Laudon and Jane P. Laudon, *Management Information Systems: Managing the Digital Firm*, 10th edition, Pearson Education International: Upper Saddle River, NJ, 2007, pp.312-352.

3. 정보 침해 원인과 현황

정보통신 기술 발전으로 인터넷이 보편화되고 사용자가 증가함으로서 정보화 사회로 급진전하게 되었다. 이제는 전자상거래가 우리의 일상이 되었으며 그 잠재 가치는 무한하다고 할 수 있겠다. 그러나 인터넷이 가져다주는 익명성과 통제가 없는 공개된 환경 그리고 기술 발전에 따른 보안문제가 대두되고 그에 따른 법제나 침해 방지 기술이 미흡한 관계로 정보 침해 사례가 속출하게 되었다. 시스템에 대한 취약성도 문제이지만 급성장한 인터넷 환경에서의 사용자들의 윤리와 생활은 그 만큼 성장하지 못한 원인이 있다고 할 수 있겠다. 또한 최원혁(2005)[13]의 기업정보온라인유출, 유형 및 사례 분석에 의하면 그 근본적인 원천은 "인터넷이 가지고 있는 즉각성과 개방성에 기인 한다"고 하였다. 그로인해 개인정보 침해, 사이버 폭력, 해킹이나 바이러스 유포, 개인 사생활 감시(엿보기), 외계/통신언어의 사용으로 인한 언어오염, 청부살인, 동반자살 그리고 인터넷 중독 장애(IAD: Internet Addiction Disorder) 같은 정보사회의 역기능이 발생하게 되었다. 그 역기능 중 하나로 범죄로 발전된 유형별 사이버 범죄 현황을 보면 사이버범죄의 급증을 확인 할 수 있다.[14]

<표 3> 사이버 범죄 현황

구분	사이버 테러형 범죄			소계	일반 사이버 범죄
	계	해킹	바이러스		
2001년	33,325	10,562	112	10,674	22,651
2002년	60,068	14,065	94	14,159	45,909
2003년	68,445	14,159	82	14,241	54,204
2004년	77,099	15,348	42	15,390	61,709

자료: 국가정보원 · 정보통신부, 「2005 국가정보화백서」, 2005.

III. 연구 방법

1. 조사대상과 조사방법

본 연구는 외국계 기업 종사자와 국내 기업 종사자간 개인 정보관리, 정보 보안의식, 정보보안 교육에 차이가 있는가를 파악하는데 목적이 있다. 이를 위하여 외국계 기업 종사자와 국내 기업 종사자를 연구대상으로 선정하였다. 자료의 수집은 본 연구자가 직접 조사 및 수거하였으며 설문조사의 목적과 방법 등을 알려준 후 응답자가 설문항목에 대해 직접 기

13) 최원혁, 「기업정보온라인유출, 유형 및 사례 분석」, 국가사이버안전센터, 2005.
14) 한국전산원, 「2005 국가정보화백서」, 2005.

입하는 자기기입방법을 사용하였으며 응답자가 설문지에 응답하는 시간은 평균 10여분이 소요되었다.

설문조사 기간은 2006년 4월 3일부터 2006년 5월 4일까지 한 달간 이루어졌다. 배포된 200부의 설문지 중 회수된 설문지는 142부로서 응답률은 67%이며, 이 중 불성실하게 응답한 설문지 8을 제외한 134부(외국계 기업 종사자: 79부(59%), 국내 기업종사자: 55부(41%)가 유효 설문지였다.

2. 설문의 구성

본 연구의 목적을 달성하기 위하여 제작된 설문지는 선행연구[15) 16) 17)]를 참고로 본 연구자가 직접 수정하고 보완하여 작성하였다. 설문지는 크게 개인적인 사항, 정보이용자의 개인정보관리, 정보이용자의 정보보안의식, 정보 이용자의 정보보안교육에 대한 인식을 묻는 4개의 영역으로 구성되어 있으며 구체적인 설문문항 구성은 다음의 <표 4>와 같다.

<표 4> 설문지 문항구성

구 분	문항수	설문 내용
개인적인 사항	8	회사구분, 업종, 인원, 연령, 성별 및 근무연수, 학력, 직무분야, 컴퓨터 사용기간, 컴퓨터의 사용 장소
개인정보 관리	20	개인의 정보관리 상태, 해킹피해 경험, 바이러스 감염경험, 감염경로, 안티바이러스프로그램 설치/운용, 바이러스 프로그램의 갱신 주기, 기타 보안장치, 부팅 시 사용자 확인 유무, PC 암호변경주기, 자료 공유 시 폴더 암호 사용 여부, 바이러스정보 확인 여부(관심도), 온라인상 파일 다운로드 시 바이러스 점검 유무, 화면보호기의 사용, 사용 후 종료 여부, 개인 캐비닛/서랍 잠금장치 사용 여부, 개인정보 백업 여부, 백업본의 저장 장소, 백업을 받는 매체, 중요한 파일에 암호 사용 여부, 중요한 메일 송부 시 보안된 옵션이나 암호 사용 여부
정보보안 의식	15	규정과 절차 인지 여부, 정보보안에 대한 정보 취득 주기, 인터넷 회원 가입 시 조항 확인 여부, 회원 가입 시 주민번호의 필요성 여부, 주민번호를 요구하는 사이트에 대한 대처, 타인의 정보를 이용한 사이트 가입 방법, 스팸메일의 처리, 유출된 정보로부터의 피해 가능성 인지 여부, 정보 침해 사고 시 조치 방법, 신고기관 인지 여부, 자료의 위·변조 가능성 인지 여부, 개인정보의 유출 가능성 인지 여부, 개인정보 유출 경로, 해킹/무단복사/변조/열람 경험 여부
정보보안 교육에 대한 인식	7	조직 내 정보보안 인식 제고 프로그램의 존재 인지 여부, 정보 인식 제고 프로그램의 수행 주기, 정보보안 인식 제고 프로그램의 도움 여부, 도움이 되지 않는 이유, 인식 제고 방법, 정보보안 인식 제고 프로그램을 수행하는 부서

3. 분석 방법

15) 박주흠, 전게서.
16) 신용섭, 전게서.
17) 호순근, 전게서.

본 조사에서 수집된 자료의 통계처리는 데이터 코딩(Data Coding)과 데이터 클리닝(Data Cleaning) 과정을 거쳐 SPSS 12.0 for Windows 통계 패키지 프로그램을 활용하여 다음과 같은 방법으로 분석하였다.

첫째, 표본의 일반적 특성을 파악하기 위하여 빈도분석(Frequency Analysis)을 실시하였다.

둘째, 외국계 기업 종사자와 국내 기업 종사자간 개인정보관리, 정보보안의식, 정보보안교육에 대한 인식 차이를 파악하기 위하여 교차분석(χ^2 검증)을 실시하였다.

IV. 분석 결과

1. 응답자의 일반적 사항

본 연구의 목적을 달성하기 위하여 외국계 기업 종사자 78명과 국내 기업 종사자 56명의 총 134명이 분석에 사용되었으며 이들의 일반적 사항은 아래 <표 5>와 같다.

<표 5> 응답자의 일반적 사항

구 분		빈도(명)	백분율(%)
회사 구분	외국계 기업 종사자	78	58.2
	국내 기업 종사자	56	41.8
업종	제조	10	7.5
	유통/서비스	62	46.3
	통신/전기/전자	62	46.3
인원	20명 이내	12	9.0
	50명 이내	58	43.3
	100명 이내	20	14.9
	100명 이상	44	32.8
연령	20대	38	28.4
	30대	82	61.2
	40대	14	10.4
성별	남성	94	70.1
	여성	40	29.9
근무연수	3년 미만	33	24.6
	5년 미만	32	23.9
	10년 미만	36	26.9
	15년 미만	26	19.4
	15년 이상	7	5.2

구 분		빈도(명)	백분율(%)
학력	중등	1	.7
	고등	11	8.2
	전문대	22	16.4
	대졸	78	58.2
	대학원	22	16.4
직무 분야	경리/회계	9	6.7
	구매/자재	9	6.7
	노무/인사	8	6.0
	마케팅/서비스	19	14.2
	생산/제조	26	19.4
	영업/판매	19	14.2
	총무/행정	5	3.7
	전산/정보통신	7	5.2
	정비/지원	18	13.4
	기타	14	10.4
컴퓨터 사용기간	3년 미만	11	8.2
	5년 미만	12	9.0
	10년 미만	30	22.4
	15년 미만	50	37.3
	15년 이상	31	23.1
컴퓨터 주 사용 장소	직장	109	81.3
	자택	22	16.4
	PC방	3	2.2
합계		134	100.0

분석 결과, 외국계 기업 종사자는 58.2%, 국내 기업 종사자가 41.8%로 나타났으며 업종은 유통/서비스업과 통신/전기/전자가 각 46.3%, 제조업이 7.5%로 조사되었다. 회사 인원 규모는 50명 이내가 43.3%, 100명 이상은 32.8%, 100명 이내가 14.9%로 조사되었다. 연령은 20대가 28.4%, 30대가 61.2%, 40대가 10.4%로 조사되었고 성별은 남성이 70.1%로 여성의 29.9%에 비하여 많았으며 근무연수는 3년 미만이 24.6%, 5년 미만이 23.9%, 10년 미만이 26.9%, 15년 미만이 19.4%, 15년 이상은 5.2%로 조사되었다. 학력은 대졸자가 58.2%, 전문대학교와 대학원 졸업자는 각각 16.4%로 조사되었다. 초 대졸 이상 비율로 보았을 때 91%의 비율로 고학력의 그룹이었다. 직무 분야는 생산/제조업이 19.4%로 가장 많았고 그 다음으로 마케팅/서비스와 영업/판매가 각 14.2%로 조사되었다.

컴퓨터 사용 기간은 15년 미만이 37.3%로 가장 많았고 15년 이상은 23.1%, 10년 미만은

22.4%로 조사되었다. PC보급이 대중화됨에 따라 컴퓨터의 사용기간이 5년 이상이 되는 사용자의 비율이 82.8%나 되었다. 컴퓨터 주사용 장소에 대하여 살펴보면 직장에서 사용하는 경우가 81.3%로 가장 많았고 자택에서 하는 경우가 16.4%로 조사되었다. 직장인들을 대상으로 하였고, 생활의 대부분을 직장에서 소비하는 생활 형태를 보았을 때 당연한 결과이나 귀가 후 자택에서 컴퓨터를 사용하는 사람들이 의외로 적었다. 업무시간이 끝난 후 여가시간은 컴퓨터가 아닌 다른 것이 차지하고 있음이 확실하다고 여겨진다.

2. 정보 이용자의 개인정보 관리

<표 6> 개인의 정보관리 상태

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	21 (26.9)	46 (59.0)	11 (14.1)	78 (100.0)
국내 기업 종사자	13 (23.2)	33 (58.9)	10 (17.9)	56 (100.0)
합계	34 (25.4)	79 (59.0)	21 (15.7)	134 (100.0)
통계량		χ^2 = .470	p = .791	

자신의 정보관리를 잘 하고 있는가에 대하여 살펴보면 전반적으로 보통이다가 59.0%로 가장 많았고 그렇다가 25.4%, 그렇지 않다가 15.7%로 개인의 정보관리 상태에 대하여 보통이라고 인식을 하고 있었다. 정보 보안에 관련해 국내 기업보다 앞선 외국계 기업의 선진 기술과 정책을 회사에 잘 반영하고 있고, 그 기업에 종사하는 종사자들 또한 잘 교육되고 구성과 실천이 잘 되고 있으리라는 본 연구자의 생각 “외국계 기업의 종사자가 국내 기업의 종사자보다 정보관리를 잘 한다”는 틀린 것으로 나타났다. IBM 2005 Global Business Security Index Report[18]에서 내부 종사자들이 주요 보안 취약 요인으로 이용될 것이라는 예측과 아울러 조직의 세계화 그리고 M&A나 매각, 구조조정 등으로 인해 내부 인력에 대한 보안 교육이나 관리가 더욱 어려워지고 있는 상황이라 언급한 내용과 고도화된 정보화 사회로 진입할수록 정보에 관련된 정보를 많이 접하고 있고, 이제는 일반인들에게 정보보안이라는 이슈가 일반화되었음은 물론이거니와, 매체를 통한 정보화에 대한 역작용에 대한 이슈들은 물론 사용자들의 관심 증가와 기업체에서의 교육 등으로 이런 결과가 나타난 것이리라 생각된다. 반대로 외국계 기업의 국내 행보에 있어 기업의 보안정책이나 교육이 내부 직원들에게 효과적으로 전파하지 못했을 가능성도 있다고 생각하였는데 이는 <표 41>의 조

18) IBM, “2005 Global Business Security Index Report,” 2005.

직 내 정보보안 인식제고 프로그램 존재 인지에서 외국계 기업의 종사자들이 55.1%가 모른다고 응답한 부분에서 그 해답을 찾을 수 있었다.

<표 7> 해킹피해 경험

구 분	1-2회	3회 이상	없다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	15 (19.2)	6 (7.7)	57 (73.1)	78 (100.0)
국내 기업 종사자	14 (25.0)	7 (12.5)	35 (62.5)	56 (100.0)
합계	29 (21.6)	13 (9.7)	92 (68.7)	134 (100.0)
통계량		χ^2 = 1.809	p = .405	

PC가 해커의 침입을 받은 경험에 대하여 살펴보면, 전반적으로 없다가 68.7%로 가장 많았고 1-2회의 해킹피해 경험이 있는 경우는 21.6%, 3회 이상 해킹 피해를 입은 경우도 9.7%로 총 31.3%의 사용자가 피해 경험이 있는 것으로 나타났다. 전 항목에 걸쳐 외국계 기업의 종사자들이 국내 기업 종사자보다 해킹피해 경험이 적은 것으로 조사 되었지만 두 그룹 간의 큰 편차를 보이지는 않았다.

<표 8> 바이러스 감염경험

구 분	없다	1-3회	4-6회	6회 이상	합계
	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	11 (14.1)	39 (50.0)	16 (20.5)	12 (15.4)	78 (100.0)
국내 기업 종사자	3 (5.4)	32 (57.1)	15 (26.8)	6 (10.7)	56 (100.0)
합계	14 (10.4)	71 (53.0)	31 (23.1)	18 (13.4)	134 (100.0)
통계량		χ^2 = 3.784		p = .286	

PC가 바이러스에 감염되어 피해를 본 경험에 대하여는 53.0%가 1-3회 감염을 경험한 것으로 나타났다. 그 다음으로 4-6회가 23.1%, 6회 이상 바이러스에 감염된 경우도 13.4%로 조사되었으며 바이러스 감염을 한번도 경험한 적이 없는 경우는 10.4%에 불과하였다. 다른 선행 연구에서의 감염비율은 강원지역 초등학교 교사를 중심으로 한 교사의 정보보호 및 보안 의식에 대한 신용섭(2005)[19]의 실태 연구결과와의 비교에서 66.1%, 박주흠(2002)[20]의

19) 신용섭, 전게서.
20) 박주흠, 전게서.

정보이용자들의 특성에 따른 정보보안의식에 관한 연구에서는 53.8%의 감염경험이 본 연구 결과와 다소 차이가 있지만 한정된 교사 집단 또는 지역적인 특성이나 연도 수 그리고 일반 직장인들을 비교 대상으로 한 결과를 고려 해 볼 때 89.5%의 높은 감염 경험은 비교 집단의 차이에서 온 것이라고 볼 수 있겠다.

<표 9> 감염경로

구 분	1순위	2순위	3순위
	N (%)	N (%)	N (%)
디스켓/USB 메모리	1 (.8)	1 (.8)	6 (5.0)
온라인상 파일 다운로드 시	64 (53.3)	42 (35.0)	11 (9.2)
전자우편	32 (26.7)	45 (37.5)	40 (33.3)
웹서핑	23 (19.2)	32 (26.7)	63 (52.5)
합계	120 (100.0)	120 (100.0)	120 (100.0)

바이러스에 감염된 경험이 있는 120명을 대상으로 감염경로에 대하여 살펴보면 1순위는 온라인상 파일 다운로드 시 감염이 된 경우가 53.3%로 가장 많았다 이는 파일 내부에 악의적인 코드가 포함되어 있는지 인지하지 못한 경우이며 파일을 다운로드한 후 바이러스 점검을 하지 않은 원인이라 파악된다. 2순위는 전자우편(37.5%) 이 또한 스팸메일 또는 바이러스에 감염된 메일을 클릭하거나 트로이목마와 같은 Spyware 프로그램이 첨부된 파일을 열어볼 때 이루어진다. Symantec사의 2005년 1월부터 6월까지 조사된 Internet Security Threat Report[21]에 의하면 전체 메일 트래픽의 61%가 스팸으로 분류된 것으로 볼 때 스팸메일을 통한 감염 비중이 높고, 본 조사의 결과에도 이를 뒷받침 해주고 있다. 3순위는 웹서핑(52.5%)으로 나타났다. 요즘엔 안티바이러스 프로그램이 최신으로 업데이트 되어 있지 않을 경우 인터넷을 하는 과정에서 사용자가 파일을 다운로드 하지 않았더라도 바이러스에 감염될 수 있다. 과거의 디스켓이나 PC통신에서 바이러스가 전파되던 예전과 비교하면 바이러스 감염의 주체는 인터넷을 이용한 통신라인이 그 전부라 해도 과언이 아니다.

21) Symantec(http://www.symanatec.com), “Symantec Internet Security Threat Report(Jan. 05 - Jan. 06),” Vol.VIII, 2005.09.

<표 10> 감염경로 1순위에 대한 회사구분별 차이분석

구 분	디스켓/USB 메모리	온라인상 파일 다운로드 시	전자우편	웹서핑	합계
	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자		39 (58.2)	14 (20.9)	14 (20.9)	67 (100.0)
국내 기업 종사자	1 (1.9)	25 (47.2)	18 (34.0)	9 (17.0)	53 (100.0)
합계	1 (.8)	64 (53.3)	32 (26.7)	23 (19.2)	120 (100.0)
통계량		χ^2 = 4.072		p = .254	

감염경로의 1순위에 대하여 외국계 기업 종사자와 국내 기업 종사자간 차이분석을 실시한 결과 유의미한 차이를 보이지 않아 외국계나 국내 기업이나 별 차이가 없음이 확인 되었고, 2005년 한국정보보호진흥원(KISA) 정보보호 실태조사[22] 본문에서 컴퓨터 바이러스 감염 경로별 피해에서 다운로드받은 프로그램 87.1%, 전자우편 45.2%, 공유폴더/내부 네트워크 37%로 나란히 1 ,2, 3위를 차지한 것과 박주흠(2002)[23]의 연구에서의 감염순위를 볼 때 전체적으로 그 유형은 같다고 하겠다.

<표 11> 정품 안티바이러스 프로그램 설치/운영

구 분	있다	없다	정품 외의 제품 사용	테스트/무료 버전	합계
	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	45 (57.7)	15 (19.2)	2 (2.6)	16 (20.5)	78 (100.0)
국내 기업 종사자	40 (71.4)	5 (8.9)	2 (3.6)	9 (16.1)	56 (100.0)
합계	85 (63.4)	20 (14.9)	4 (3.0)	25 (18.7)	134 (100.0)
통계량		χ^2 = 3.743		p = .291	

PC에 바이러스 감염을 예방하기 위한 정품 안티 바이러스 프로그램을 설치하여 운영하고 있는가에 대하여 살펴보면 전반적으로 운영하고 있는 경우가 63.4%로 가장 많았다. 정품 소프트웨어, 정품 외의 제품 그리고 테스트/무료 버전까지 포함하여 운영되고 있는 경우가 85.1%로 조사되었는데 그 나머지 운영되고 있지 않은 14.9%에 대해선 본 연구자가 설명하기 어려운 부분이다. 요즈음 환경에서 안티바이러스 프로그램을 설치하지 않았을 경우 바이

22) 한국정보보호진흥원(http://www.kisa.or.kr), "2005년 정보보호 실태조사", 2005.
23) 박주흠, 전게서.

러스 감염확률은 100%에 가까운데 사용자들이 설치된 프로그램에 대해 인지하고 있지 못한 것인지 실제 설치되지 않은 것인지 의문이다. 본 연구자는 외국계 기업의 종사자의 경우 국내 안티바이러스백신 시장에서 점유율 1, 2위를 차지하고 있는 안철수 연구소와 하우리에 익숙하여 외산 백신 소프트웨어의 설치 유무를 파악하지 못한 이유라고 보며 후행 참고 조사에서 20명의 사용자에게 질문한 결과 무엇을 사용하는지 알지 못한다고 답변하였다. 그 다음으로 테스트 및 무료 버전을 이용하는 경우는 18.7%로 나타났다. 정품에 비해 다소 불편한 점은 있지만 경제적인 것을 추구하는 일반 유저들이 이 부류인 것으로 추정된다. 사용자들의 의식 개선으로 정품 외의 소프트웨어를 사용하는 비율은 3%에 그쳤으나 여전히 36.6%는 무료버전이나 정품이 아닌 복사/크랙된 프로그램을 사용하고 있는 것으로 드러나 PC사용자들의 정품소프트웨어 사용 환경 조성이 필요하다 하겠다.

<표 12> 바이러스 프로그램 갱신 주기

구 분	매일	1주 이내	1개월 이내	설치 후 그대로 사용	갱신 발생 시 자동으로	합계
	N (%)	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	5 (6.4)	13 (16.7)	8 (10.3)	15 (19.2)	37 (47.4)	78 (100.0)
국내 기업 종사자	5 (8.9)	13 (23.2)	9 (16.1)	7 (12.5)	22 (39.3)	56 (100.0)
합계	10 (7.5)	26 (19.4)	17 (12.7)	22 (16.4)	59 (44.0)	134 (100.0)
통계량		χ^2 = 3.257		p = .516		

최신 패치/안티 바이러스 프로그램의 업데이트(갱신)시기에 대하여 살펴보면 전반적으로 갱신 발생 시 자동으로 하는 경우가 44.0%로 가장 많았다. 그 다음으로 설치 후 그대로 사용하는 경우가 16.4%나 나왔고, 1주 이내로 갱신하는 경우는 19.4%로 나타났다. 매일 갱신 확인을 하는 경우는 7.5%에 불과하였으며 갱신 발생 시 자동으로와 매일 업데이트를 한다는 비율을 포함 하였을 때 52%인 것으로 봐서 아직도 많은 사용자들이 안티 바이러스 프로그램과 백신의 갱신에 대해 잘 이해하지 못하고 있는 것으로 보이며, 이런 이유로 백신 갱신을 제때에 하지 못하는 것으로 보인다. 사용자의 백신 업데이트에 대한 중요성 인식과 이를 개선할 교육이 요구된다고 생각되며, 파악된 이런 갱신주기의 문제점으로 인해 바이러스 감염 경험이 89.5%가 나온 것으로 판단된다.

<표 13> 기타 보안장치

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	49 (62.8)	16 (20.5)	13 (16.7)	78 (100.0)
국내 기업 종사자	34 (60.7)	6 (10.7)	16 (28.6)	56 (100.0)
합계	83 (61.9)	22 (16.4)	29 (21.6)	134 (100.0)
통계량		χ^2 = 4.064	p = .131	

PC에 안티 바이러스, 개인 방화벽 등 컴퓨터 및 자료보호를 위한 별도의 보안장치를 사용에 대한 분석 결과 전반적으로 그렇다는 응답이 61.9%로 가장 많았고 그렇지 않다가 21.6%, 보통이다가 16.4%로 기타 보안장치를 사용하는 비율이 높았다. 이는 정보 사용자가 해킹이나 바이러스 감염 등의 정보침해로부터 사용자의 자료와 컴퓨터를 보호하기 위한 인식에서 비롯된 가장 기본적이고 효과적인 예방 방법이란 것을 인식하고 있는 듯하다.

<표 14> 부팅 시 사용자 확인 유무

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	63 (80.8)	1 (1.3)	14 (17.9)	78 (100.0)
국내 기업 종사자	37 (66.1)	3 (5.4)	16 (28.6)	56 (100.0)
합계	100 (74.6)	4 (3.0)	30 (22.4)	134 (100.0)
통계량		χ^2 = 4.400	p = .111	

PC를 부팅 할 경우 사용자 확인을 실시하고 있는 경우가 74.6%로 조사되었고 그렇지 않다가 22.4%, 보통이다가 3.0%로 부팅 시 사용자 확인을 주로 하는 것으로 파악되었다. 전체적으로 국내 기업 종사자에 비해 외국계 기업 종사자가 부팅 시 사용자 확인을 잘 하고 있는 것으로 나타났지만 22%의 그렇지 않다는 답변의 원인에 업무 시작 시 부팅 시간을 줄일 수 있고, 사용자가 화면보호기를 암호로 보호함으로서 PC가 보호될 수 있다는 사용자의 의견을 들었다.

<표 15> PC 암호 변경 주기

구 분	한 달에 1번 이상	두 달에 1번 이상	석 달에 1번 이상	1년에 1번 이상	변경 안 함	합계
	N (%)	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	7 (9.0)	19 (24.4)	17 (21.8)	8 (10.3)	27 (34.6)	78 (100.0)
국내 기업 종사자	8 (14.3)	12 (21.4)	5 (8.9)	5 (8.9)	26 (46.4)	56 (100.0)
합계	15 (11.2)	31 (23.1)	22 (16.4)	13 (9.7)	53 (39.6)	134 (100.0)
통계량		χ^2 = 5.439		p = .245		

PC의 암호 변경 주기를 살펴보면 변경을 하지 않는 경우가 39.6%로 가장 많았고 그 다음으로 두 달에 1번 이상이 23.1%로 조사되었다. 석 달에 1번 이상은 16.4%로 조사되었으며 한 달에 1번 이상 PC의 암호를 변경하는 경우는 11.2%에 불과하였다. 여기서 암호를 변경하지 않는다는 의미에서 암호 변경시 이전 암호를 그대로 사용하는 것을 포함한다. 일반적으로 한 달에 1번 정도 암호 변경하는 것을 유효하다고 할 때 나머지 88.8%가 개선되어야 할 필요가 있다. 한 달에 한번이상 암호를 변경하는 부분에서 외국계 기업의 종사자보다 국내 기업에 종사하는 종사자의 비율이 더 높았으나 전혀 변경을 안 한다는 응답에선 외국계 종사자의 비율이 더 낮았다.

<표 16> 자료 공유 시 폴더 암호 사용 여부

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	28 (35.9)	20 (25.6)	30 (38.5)	78 (100.0)
국내 기업 종사자	31 (55.4)	10 (17.9)	15 (26.8)	56 (100.0)
합계	59 (44.0)	30 (22.4)	45 (33.6)	134 (100.0)
통계량		χ^2 = 5.009	p = .082	

사용 중인 PC가 네트워크 상에서 다른 사용자와 자료를 함께 공유하여 사용할 때 암호를 사용 여부에 대하여 살펴보면, 그렇다가 44.0%로 가장 많았고 그렇지 않다가 33.6%, 보통이다가 22.4%로 나타났다. 보통이다와 그렇지 않다를 포함했을 때 56%의 비율을 보인 것에는 사용자들이 공유폴더에 암호를 사용하지 않음에서 오는 위험을 간과하고 있는 것으로 판단된다. 그 이유는 직장에서 일하고 있는 동료가 정보를 빼돌려 업무 외에 활용하거나 다른 부정한 방법으로 활용할 수 있다는 기본 가정을 배제하였기 때문이라 생각되며 그 다음 가능성으로는 공유 폴더 암호를 사용하는 방법을 잘 모르거나 복잡하고 사용하기가 귀찮아서

그럴 수도 있다고 판단된다. 국내 기업의 사용자가 공유폴더에 대한 암호의 사용에 더 적극적인 것으로 파악되었다.

<표 17> 바이러스 정보 확인 여부

구 분	매일 확인	한 주에 1번 확인	한 달에 1번 확인	발생할 때마다	관심없다	합계
	N (%)	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	5 (6.4)	14 (17.9)	10 (12.8)	37 (47.4)	12 (15.4)	78 (100.0)
국내 기업 종사자	3 (5.4)	9 (16.1)	11 (19.6)	29 (51.8)	4 (7.1)	56 (100.0)
합계	8 (6.0)	23 (17.2)	21 (15.7)	66 (49.3)	16 (11.9)	134 (100.0)
통계량			χ^2 = 3.075		p = .545	

최신 바이러스와 관련한 정보에 대한 확인을 살펴보면 발생할 때마다 확인을 하는 경우가 49.3%로 가장 많은 것으로 나타났다. 이는 바이러스에 대한 사용자의 주의가 있다고 해석되어지는 부분이다. 그 다음으로 한 주에 1번 확인하는 경우는 17.2%, 한 달에 1번 확인하는 경우는 15.7%로 나타났다. 매일 확인하는 경우는 6.0%에 불과하였다. 이는 안티바이러스 회사에서 안내메일로 보내진 바이러스 정보에 대한 확인이 크다 하겠고 인터넷을 통해 알려지는 보안 뉴스 등에 의해 두 그룹간의 큰 차이가 없었다고 보여 진다. 바이러스 정보에 대해 발생할 때마다 또는 매일 확인 하는 사용자가 갱신도 잘하고 따라서 감염경험도 다른 사용자보다 낮다.

<표 18> 온라인상 파일 다운로드 시 바이러스 점검 유무

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	41 (52.6)	22 (28.2)	15 (19.2)	78 (100.0)
국내 기업 종사자	35 (62.5)	17 (30.4)	4 (7.1)	56 (100.0)
합계	76 (56.7)	39 (29.1)	19 (14.2)	134 (100.0)
통계량		χ^2 = 3.798	p = .137	

온라인상에서 자료를 다운로드 받을 경우 바이러스 체크에 대하여 살펴보면 그렇다가 56.7%로 바이러스 체크를 대체적으로 잘 하고 있는 것으로 나타났다. 파일 다운로드 시 바이러스 감염에 대한 위험성을 인지하고 있으며 대체로 실천에 옮기고 있다고 간주된다. 보통이다는 29.1%, 그렇지 않다는 14.2%로 조사되었다.

<표 19> 화면보호기의 사용

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	43 (55.1)	8 (10.3)	27 (34.6)	78 (100.0)
국내 기업 종사자	24 (42.9)	5 (8.9)	27 (48.2)	56 (100.0)
합계	67 (50.0)	13 (9.7)	54 (40.3)	134 (100.0)
통계량		χ^2 = 2.537	p = .281	

PC를 사용하여 작업하던 자리를 이동할 경우 암호로 보호된 화면보호기를 사용하는 경우는 50.0%로 나타났으며 사용하지 않는 경우는 40.3%, 보통이다는 9.7%로 조사되었으며 신용섭(2005)[24]의 선행연구에서는 사용하는 경우가 36.7%, 사용하지 않는 경우가 46.3% 그리고 방법을 모르는 경우도 16.9%로 조사되어 일반 직장인들을 대상으로 한 그룹과는 다소 차이가 있었다. 그렇지 않다의 응답에는 화면보호기를 사용하지만 암호로 보호하지 않았을 때의 경우를 포함한다.

<표 20> 사용 후 종료 여부

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	66 (84.6)	6 (7.7)	6 (7.7)	78 (100.0)
국내 기업 종사자	43 (76.8)	10 (17.9)	3 (5.4)	56 (100.0)
합계	109 (81.3)	16 (11.9)	9 (6.7)	134 (100.0)
통계량		χ^2 = 3.331	p = .189	

퇴근 시 PC의 전원을 off(종료)하는 가에 대하여 81.3%가 그렇다고 응답하여 대부분의 사용자가 PC의 전원을 끄는 것으로 나타났다. 이 항목과 함께 개인 컴퓨터에 부팅, 로그인, 화면보호기의 패스워드를 설정하여 사용하라는 권고가 국가사이버안전센터에서 나온 정보보호 생활수칙(2005)[25]에 들어있다.

24) 신용섭, 전게서.
25) 국가사이버안전센터, “인터넷시대 정보보호 생활수칙”, 2005.01.13.

<표 21> 개인 캐비닛/서랍 잠금장치 사용 여부

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	40 (51.3)	21 (26.9)	17 (21.8)	78 (100.0)
국내 기업 종사자	27 (48.2)	14 (25.0)	15 (26.8)	56 (100.0)
합계	67 (50.0)	35 (26.1)	32 (23.9)	134 (100.0)
통계량		χ^2 = .448	p = .800	

이 질문은 전자정보 외의 출력된 인쇄물에 대한 보호 상태를 알아보고자 한 부분이다. 퇴근 시 본인의 캐비닛과 서랍에 잠금장치를 하는 경우는 50.0%, 그렇지 않은 경우는 23.9%, 보통이다는 26.1%로 절반가량이 잠금장치를 하고 있는 것으로 나타났다. 전자정보뿐만 아니라 출력된 인쇄물의 보호에 사용자의 관심과 실천이 요구되는 부분이다. 각 항목에 있어 두 그룹 간이 아주 유사한 비율을 보였다.

<표 22> 개인정보 백업 여부

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	39 (50.0)	26 (33.3)	13 (16.7)	78 (100.0)
국내 기업 종사자	40 (71.4)	10 (17.9)	6 (10.7)	56 (100.0)
합계	79 (59.0)	36 (26.9)	19 (14.2)	134 (100.0)
통계량		χ^2 = 6.259	p = .044*	

*p<.05

중요한 자료에 대하여 사본(Backup)을 따로 작성하여 관리하고 있는 경우는 59.0%로 나타났다. 백업을 하지 않는 경우는 14.2%로 나타났는데 이를 외국계 기업 종사자와 국내 기업 종사자간 차이분석을 실시한 결과 중요한 자료에 대해 백업을 하는 비율이 외국계 기업 종사자(50.0%)에 비하여 국내 기업 종사자(71.4%)가 많은 것으로 나타나 국내 기업 종사자가 중요한 자료에 대한 사본을 작성하여 관리하고 있는 수준이 높은 것으로 나타났다(p<.05). 이는 <표 41>의 정보보안 인식제고 프로그램의 존재 인지 수준에서 국내 기업의 종사자 37.5%가 모른다는 답변을 한 결과에 비해 외국계 기업의 종사자는 55.1%가 모른다는 답변을 한 점과 그 프로그램을 수행하는 부서가 외국계 기업의 종사자 답변에서는 IT부서가 92%를 차지한 것에 비해 국내 기업의 종사자 답변에서는 IT, 보안부서나, 정보보안부

서, 경영기획부, 등 다양하고 세분화된 부서에서 교육을 실시하였다. 이 부분에서 사용자에 대한 인식제고 교육이 외국계 기업보다 국내 기업이 좀 더 유효했던 것으로 보인다.

<표 23> 백업본의 저장 장소

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	26 (33.3)	37 (47.4)	15 (19.2)	78 (100.0)
국내 기업 종사자	20 (35.7)	21 (37.5)	15 (26.8)	56 (100.0)
합계	46 (34.3)	58 (43.3)	30 (22.4)	134 (100.0)
통계량		χ^2 = 1.628	p = .443	

백업 본은 금고, 캐비닛, 사내 백업 저장소 등 보안된 장소에 보관하는 수준에 대하여 살펴보면 전반적으로 보통이다가 43.3%, 그렇다가 34.3%, 그렇지 않다가 22.4%로 보안된 장소에 대한 보관 수준은 보통인 것으로 나타났다. 문제는 백업 받은 자료들을 보안된 장소에 보관하지 않음으로서 정보 유출의 높은 가능성을 나타내고 있는데 이는 해킹보다도 훨씬 쉬운 보안 사고를 야기 할 수 있고 그 원인은 정보관리의 1차적 백업 이후 2차적 보관 문제에 대해 간과하고 있음이다. 아울러 <표 21>의 개인 캐비닛/서랍 잠금장치 사용 여부의 결과와 비교해 볼 때 백업본의 저장장소 보다 개인 캐비닛/서랍의 잠금장치에 더 주의를 하고 있는 것으로 보인다. 이 또한 사용자가 백업된 사본의 보호의 중요성에 대해 간과하고 있다는 증거이며 기업에서 정보보안 교육 시 백업된 사본의 보관과 개인 캐비닛/서랍의 잠금장치의 중요성에 대해서 강조할 필요가 있는 대목이다.

<표 24> 백업을 받는 매체

구 분	CD/DVD ROM	파일 서버	외장 하드디스크/ USB Memory	웹 하드/ 디스크	기타	합계
	N (%)	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	18 (23.1)	16 (20.5)	32 (41.0)	7 (9.0)	5 (6.4)	78 (100.0)
국내 기업 종사자	23 (41.1)	8 (14.3)	23 (41.1)	2 (3.6)		56 (100.0)
합계	41 (30.6)	24 (17.9)	55 (41.0)	9 (6.7)	5 (3.7)	134 (100.0)
통계량			χ^2 = 9.162	p = .057		

중요한 자료를 백업할 경우 매체에 대하여는 41.0%가 외장 하드디스크 및 USB Memory였으며 그 다음으로 30.6%가 CD/DVD ROM으로 응답하였다. 이 경우 하드디스크의 가격이 하락하면서 사용자들이 대용량의 자료들을 손쉽게 외장형 하드디스크에 백업을 하는 것으로 보이며 최근 간편하게 들고 다닐 수 있고 용량 또한 적지 않은 USB Memory를 선호하는 것으로 나타났다. 예전의 백업방식이던 플로피 디스켓에 백업을 받는 다는 응답은 단 한 건도 나오지 않았으며 대용량의 자료들을 백업받을 수 있고 가격도 저렴한 CD/DVD ROM 또한 사용자가 선호하는 백업매체였다. 그러나 CD/DVD ROM의 경우 시간이 지날 경우 손상의 가능성이나 인식이 잘 되지 않은 위험성을 가지고 있다. 파일 서버를 이용하는 경우는 17.9%, 웹 하드 및 디스크를 이용하는 경우는 6.7%로 나타났다. 기업에서 문서관리를 하고 있다면 파일서버를 이용하는 비율이 높을 것으로 생각되는데 이 비율이 낮은 것으로 보아 중앙 문서 관리가 잘 이루어지지 않을 가능성과 구축이 미비하여 활용도가 떨어지는 가능성, 마지막으로 사용자가 자신이 만든 자료 공유의 거부감 또는 저항감이 파일 서버를 백업 매체로 사용하는 비율을 떨어뜨릴 수 있다고 본다. 기업에서 문서 보안이 어떤 단계에 있는지 모르지만 중요한 자료들의 백업 장소가 파일 서버(File Server) 가 아닌 외장 하드디스크나 USB Memory 또는 CD/DVD ROM이란 얘기는 내부 문서 보안이 잘 이루어지고 있지 않음을 반증하는 자료이다. 이에 기업들은 문서관리 솔루션을 도입할 필요가 있다 하겠으나 경기 침체에 따른 비용 문제가 대두되어 많은 기업에서 도입할 시기를 기다리고 있거나 도입 의사를 포기하는 문제가 있다 하겠다.

<표 25> 중요한 파일에 암호 사용 여부

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	21 (26.9)	16 (20.5)	41 (52.6)	78 (100.0)
국내 기업 종사자	13 (23.2)	17 (30.4)	26 (46.4)	56 (100.0)
합계	34 (25.4)	33 (24.6)	67 (50.0)	134 (100.0)
통계량		χ^2 = 1.705	p = .426	

중요한 자료를 작성하여 파일로 저장할 대 파일에 읽기 쓰기용 암호를 사용하는 수준에 대하여 살펴보면 그렇지 않다가 50.0%로 파일에 대한 암호는 잘 사용하지 않는 것으로 나타났고 신용섭(2005)[26]의 선행연구에서도 암호 없이 컴퓨터에 저장하는 비율이 51.8%로 조사된 것으로 볼 때 사용자들이 중요 문서 관리 수준이 낮은 것으로 파악된다. 중요 파일에 암호를 사용하는 경우는 25.4%로 나타났으며 앞서 언급한 신용섭의 연구에서도 27.7%의 비

26) 신용섭, 전게서.

슷한 비율을 보였다. 자료가 노출되었을 때 이를 마지막에서 보호할 수 있는 수단이 암호화를 시키거나 파일에 암호를 사용하는 것인데 아직까지 사용자들이 이 부분에 대한 인식과 실천이 많이 떨어지는 것으로 보인다. 응답자의 일반적인 사항에서 PC 사용자의 사용기간이 5년 이상 되는 비율이 82.8%인 것으로 볼 때 사용자가 엑셀이나 워드 같은 문서에 암호를 사용하는 옵션을 몰라 중요한 파일에 암호 사용 여부가 떨어지는 가능성은 낮다고 평가된다.

<표 26> 중요한 메일 송부 시 보안된 옵션이나 암호 사용 여부

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	12 (15.4)	21 (26.9)	45 (57.7)	78 (100.0)
국내 기업 종사자	9 (16.1)	17 (30.4)	30 (53.6)	56 (100.0)
합계	21 (15.7)	38 (28.4)	75 (56.0)	134 (100.0)
통계량		χ^2 = .244	p = .885	

중요한 자료를 작성하여 메일로 보낼 때 보안된 옵션이나 첨부된 파일에 암호를 사용하는 경우는 15.7%에 불과하였으며 사용하지 않는 경우가 56.0%로 디지털 서명과 암호 사용 수준은 낮은 것으로 나타났다. 이 또한 <표 25> 중요한 파일에 암호 사용 여부의 내용과 마찬가지로 정보 사용자들의 사용율이 낮았으며 파일에 암호를 사용하는 비율보다도 메일에 보안된 옵션이나 암호를 사용하는 비율이 더 낮게 나왔다. 이메일은 네트워크를 통해 전송이 되고, 그 과정에서 타인에게 의도적 방법으로 노출이 되거나 또는 정보의 복제/변조 위험의 가능성 그리고 비의도적인 개인의 실수로 잘못된 수신자에게 배달되거나 시스템의 오류로 잘못 전달될 위험이 큰 관계로 중요한 정보일 경우 암호화를 사용하는 것이 권고된다. 또한 이메일 전송 시 disclaimer(책임제한)를 넣어두어 향후 발생할 수 있는 정보누출 사고에 대해 법적으로 대응할 수 있는 방법을 사용하는 것도 바람직하다.

3. 정보 이용자의 정보보안 의식

정보보안에 관한 규정이나 절차에 대한 인지도를 살펴보면 알고 있다는 응답은 19.4%에 불과하였고 모르고 있다는 41.0%, 보통이다는 39.6%로 정보보안관련 규정과 절차에 대한인지 수준이 낮았다. 이는 아직도 기업이 사용자에 대한 정보보안교육이 효과적으로 전달되지 못하거나 제대로 된 정보보안 교육이 아닌 형식적인 전달, 그리고 양방향 communication이 아닌 단방향(기업이 종사자에게 일방적으로)으로 전달함에 따른 부작용이 존재하고 있음으로 파악된다. 또한 외국계 기업의 경우 정보보안 전담부서가 아닌 IT부서에만 의존한 결과

전문성의 부족이나 형식적인 교육을 시행함으로서 별 관심이 없는 사용자에게 다가서지 못한 이유가 있다고 하겠다.

<표 27> 규정과 절차 인지 여부

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	17 (21.8)	33 (42.3)	28 (35.9)	78 (100.0)
국내 기업 종사자	9 (16.1)	20 (35.7)	27 (48.2)	56 (100.0)
합계	26 (19.4)	53 (39.6)	55 (41.0)	134 (100.0)
통계량		χ^2 = 2.113	p = .348	

특이한 점은 <표 46> 정보보안 인식 제고프로그램을 수행하는 부서에서 국내 기업이 정보전담부서나 IT가 아닌 다른 전담 부서에서 인식 제고 프로그램을 수행을 하는 경우 좀 더 전문성이 있을 것이라 생각이 되어 인지도가 높을 것으로 예상되었는데 실제 사용자들의 규정과 절차에 대한 인지여부는 외국계 기업보다 떨어지는 결과를 보였다.

<표 28> 정보보안/정보윤리에 대한 정보 취득 주기

구 분	매일 함	1주에 수회	한달에 수회	일년에 수회	하지 않는다	합계
	N (%)	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	2 (2.6)	2 (2.6)	6 (7.7)	31 (39.7)	37 (47.4)	78 (100.0)
국내 기업 종사자		6 (10.7)	4 (7.1)	22 (39.3)	24 (42.9)	56 (100.0)
합계	2 (1.5)	8 (6.0)	10 (7.5)	53 (39.6)	61 (45.5)	134 (100.0)
통계량			χ^2 = 5.227	p = .265		

정보보안 또는 정보윤리에 대한 세미나, 유인물 혹은 교육에 대하여 정보 취득 주기를 살펴보면 하지 않는다가 45.5%로 가장 많아 정보보안에 정보 취득에 소홀한 것으로 나타났다. 일 년에 수회 정보를 취득하는 경우는 39.6%로 조사되었다. 이처럼 사용자들이 정보보안이나 정보윤리에 대한 정보를 적극적으로 취득하지 않고 있음으로서 정보침해에 대한 사고가 발생하거나 윤리의식 부족으로 인한 정보의 오·남용이 이루어지게 되고 더 확대되어 사이버 범죄로 까지 이어지는 결과를 가져온다고 할 수 있겠다.

<표 29> 인터넷 회원 가입 시 조항 확인 여부

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	8 (10.3)	27 (34.6)	43 (55.1)	78 (100.0)
국내 기업 종사자	10 (17.9)	18 (32.1)	28 (50.0)	56 (100.0)
합계	18 (13.4)	45 (33.6)	71 (53.0)	134 (100.0)
통계량		χ^2 = 1.623	p = .444	

인터넷 웹사이트 회원으로 가입할 때 개인 신상정보공개(약관) 동의서의 내용을 꼼꼼히 읽어보는 경우는 13.4%에 불과하였고 잘 읽어보지 않는 경우는 53.0%, 보통이다가 33.6%로 인터넷 회원 가입 시 약관에 대해 꼼꼼히 읽지 않는 것으로 나타났다. 회원 가입 시 조항이 너무 길고 법률적 용어를 포함하는 어려운 내용들이 포함되어 있어 사용자들이 대충 읽어보고 가입을 하는 경우가 많은데 그 항목 속에는 계열사와 협력업체에도 마케팅에 정보를 활용할 수 있다는 내용이 있을 수 있음을 사이트 이용자들은 유념해야 한다. 또한 자기 개인 정보의 가치가 얼마나 되는지 사용자 스스로가 신중히 판단해야할 것임은 물론 불필요한 사이트에의 가입을 자제해야 할 것이다. 참고로 Asite(asiate.dreamwiz.com)와 크레딧뱅크(www.creditbank.co.kr) 등이 주민번호 도용을 확인할 수 있는 웹 사이트이다.

<표 30> 회원 가입 시 주민번호의 필요성 여부

구 분	반드시 필요	경우에 따라 필요	필요 없다	전혀 필요 없다	합계
	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	7 (9.0)	29 (37.2)	33 (42.3)	9 (11.5)	78 (100.0)
국내 기업 종사자	1 (1.8)	30 (53.6)	21 (37.5)	4 (7.1)	56 (100.0)
합계	8 (6.0)	59 (44.0)	54 (40.3)	13 (9.7)	134 (100.0)
통계량		χ^2 = 5.647		p = .130	

온라인 회원 가입 시 주민번호의 필요성에 대하여 살펴보면 경우에 따라 필요하다는 의견이 44.0%로 가장 많았고 그 다음으로 필요 없다는 의견이 40.3%로 조사되었으며 전혀 필요 없다는 의견은 9.7%로 나타났다. 반드시 필요하다와 경우에 따라 필요하다를 필요하다고 간주하여 묶었을 때 50% 그리고 필요 없다와 전혀 필요 없다를 필요 없다고 간주하여 묶었을 때 역시 50%의 비율을 보였다. 그러나 경우에 따라 필요하다는 견해에 대해 주민번호의 대체수단을 제공할 경우에 반드시 주민번호가 필요하다고 보지 않음으로 결과적으로 94%의

비율이 인터넷 회원가입 시 주민번호가 불필요하다고 보여 진다. 사용자들 역시 주민번호를 본인 확인 수단으로 필요에 따라 인정하는 부분이나 주민번호를 대체할 수 있는 대안이 개발된다면 인터넷 회원 가입에 있어 주민번호는 무의미 해 질 것이고 주민번호의 노출/도용에 대한 위험이 낮아질 것으로 예상된다.

<표 31> 주민번호를 요구하는 사이트에 대한 대처

구 분	반드시 필요한 경우만 가입	그냥 가입	남의 것을 사용하여 가입	가입 안 함	합계
	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	51 (65.4)	17 (21.8)		10 (12.8)	78 (100.0)
국내 기업 종사자	43 (76.8)	12 (21.4)	1 (1.8)		56 (100.0)
합계	94 (70.1)	29 (21.6)	1 (.7)	10 (7.5)	134 (100.0)
통계량		χ^2 = 9.178		p = .027*	

*p<.05

주민번호를 묻는 온라인 회원 사이트에 대한 대처를 살펴보면 반드시 필요한 경우에만 가입하는 경우가 70.1%로 나타났고 그냥 가입하는 경우는 21.6%로 조사되었다. 가입을 하지 않는 경우는 7.5%로 조사되었다. 이를 외국계 기업 종사자와 국내 기업 종사자간 차이분석을 실시한 결과 외국계 기업 종사자는 12.8%가 가입을 하지 않는다고 응답하였고 국내 기업 종사자 중 가입을 하지 않는다고 응답한 경우는 없어 주민번호를 묻는 온라인 사이트에 대하여 외국계 기업 종사자의 거부감이 훨씬 더 큰 것으로 나타났다(p<.05). 또한 주민번호를 요구하는 사이트에 대한 대처에서 의문스러운 점은 타인의 정보를 사용해 사이트에 가입했다는 사용자가 유효설문지의 57%를 차지하는데도 불구하고 <표 31>에 나타난 남의 것을 사용하여 가입이라는 질문에선 단지 1명의 사용자만 나온 것이다.

<표 32> 타인의 정보를 이용한 사이트 가입 방법

구 분	직계/비 직계 가족	친구	모르는 사람의 것	주민번호 생성기	합계
	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	32 (68.1)	2 (4.3)	11 (23.4)	2 (4.3)	47 (100.0)
국내 기업 종사자	20 (66.7)	3 (10.0)	4 (13.3)	3 (10.0)	30 (100.0)
합계	52 (67.5)	5 (6.5)	15 (19.5)	5 (6.5)	77 (100.0)
통계량		χ^2 = 2.820		p = .420	

주민번호를 남의 것을 사용하여 한번이라도 가입을 한 경험이 있는 77명을 대상으로-이는 유효한 설문지의 무려 57%나 되는 비율이다- 그 가입 방법에 대하여 살펴보면 직계/비직계 가족의 것을 이용한 경우가 67.5%로 가장 많았고 모르는 사람의 것을 이용한 경우도 19.5%로 조사되었다. 직계/비 직계의 경우 둘 다 비슷한 비율이었으나 친구의 정보를 도용한 경우와 인터넷에서 주민번호 생성기를 다운로드 받아 웹사이트에 가입한 경우에는 국내 기업 종사자가 외국계 기업 종사자보다 높은 비율을 나타내었다. 반면 모르는 사람의 정보를 이용하여 사이트에 가입한 경우 국내 기업 종사자보다 외국계 기업의 종사자가 더 많은 비율을 보였다. 전반적으로 친구나 모르는 사람보다 신고나 적발 시 처벌의 위험부담이나 죄의식이 덜 드는 직계/비 직계 가족의 정보를 도용한 경우가 많은 것 같지만 어찌되었든 이 경우도 개인 정보의 침해/도용이고 이런 친족 간의 죄책감 없는 정보도용에 대해 정보윤리 교육의 필요성이 절실히 요구된다. 이 사례 조사의 경우 매체에 공개되지 않아 실제 비율은 훨씬 더 클 것이라 생각된다.

<표 33> 스팸메일의 처리

구 분	열어본다	바로 지운다	확인하고 지운다	스팸 거부 설정을 한다	합계
	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	5 (6.4)	38 (48.7)	17 (21.8)	18 (23.1)	78 (100.0)
국내 기업 종사자		30 (53.6)	15 (26.8)	11 (19.6)	56 (100.0)
합계	5 (3.7)	68 (50.7)	32 (23.9)	29 (21.6)	134 (100.0)
통계량		χ^2 = 4.259		p = .235	

알지 못하는 곳으로부터 전자메일이 온 경우 메일처리에 대하여 살펴보면 바로 지우는 경우가 50.7%로 가장 많았고 확인하고 지우는 경우는 23.9%, 스팸 거부 설정을 하는 경우는 21.6%로 나타났다. 그러나 그냥 열어보는 경우가 3.7%나 나왔다는 것은 아직도 스팸메일의 위험성을 인지하지 못한 결과라 생각된다. 주로 바로 지우고 스팸 거부 설정을 하는 것이 일반적인 케이스로 나타났고, 이 또한 외국계 기업 종사자와 국내 기업 종사자 모두 비슷한 패턴을 보였다.

유출된 개인정보가 악용되어 본인도 경제적 손실을 입을 수 가능성에대한 인지 여부를 살펴보면 그렇다가 87.3%로 피해 가능성에대한 인지 수준이 높은 것으로 나타났다. 아이러니 한 것은 이처럼 피해 가능성을 인지하고 있지만 백업과 캐비닛/서랍 관리 부분에서는 사용율이 낮은 것은 실천이 뒷받침이 되지 않은 이유일 것이다.

<표 34> 유출된 정보로부터의 피해 가능성 인지 여부

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	69 (88.5)	6 (7.7)	3 (3.8)	78 (100.0)
국내 기업 종사자	48 (85.7)	6 (10.7)	2 (3.6)	56 (100.0)
합계	117 (87.3)	12 (9.0)	5 (3.7)	134 (100.0)
통계량		χ^2 = .367	p = .832	

외국계 기업 종사자와 국내 기업 종사자간 극히 비슷한 비율을 보였고 두 집단 간 비교에서 유의미한 차이를 보이지는 않은 이유는 유출된 정보의 피해 사례를 각종 매체나 사내 교육을 통해 인지하고 있음으로 파악된다. 그러나 어떤 정보의 원천이 그들에게 더 가깝게 다가가는지는 향후 추가 조사를 통해 연구해야 하겠다.

<표 35> 정보 침해 사고 시 조치 방법

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	10 (12.8)	9 (11.5)	59 (75.6)	78 (100.0)
국내 기업 종사자	5 (8.9)	1 (1.8)	50 (89.3)	56 (100.0)
합계	15 (11.2)	10 (7.5)	109 (81.3)	134 (100.0)
통계량		χ^2 = 5.342	p = .069	

주민등록번호와 신용카드 등이 타인으로부터 도용되어 피해를 본 경험에 대하여는 81.3%가 없는 것으로 나타났다. 자료에서 나타나듯이 외국계 기업 종사자와 국내 기업 종사자간 차이분석에 유의미한 차이를 보이지 않지만 외국계 기업 종사자가 국내 기업 종사자보다 침해를 당한 비율이 더 높았다. 정보 침해를 당했는지도 모르는 비율을 따지면 실제보다 더 많을 거라 생각되는데, 여기서 외국계 기업의 종사자가 국내 기업의 종사자보다 인지율이 더 높았을 수 있다는 가정도 배제할 수 없다.

<표 36> 신고기관 인지 여부

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	9 (11.5)	24 (30.8)	45 (57.7)	78 (100.0)
국내 기업 종사자	8 (14.3)	23 (41.1)	25 (44.6)	56 (100.0)
합계	17 (12.7)	47 (35.1)	70 (52.2)	134 (100.0)
통계량		χ^2 = 2.243	p = .326	

정보도용 피해를 입었을 경우 조치 방법에 대하여 살펴보면, 알고 있는 경우는 12.7%로 매우 적었으며 모르는 경우가 52.2%, 보통이다가 35.1%로 신고기관에 대한 인지수준이 낮았다. 실제 본인이 정보침해 사례를 겪지 않거나 그 수준이 경미하여 간과했을 가능성도 있고, 정부나 기업 등을 포함한 각 매체에서 이런 정보를 일반 사용자들에게 효과적으로 전달하지 못한 이유인 듯하다. 침해사고 대응기관으로는 경찰청 사이버테러대응센터, 대검찰청 인터넷범죄수사센터 그리고 인터넷침해사고대응센터 등이 있다.

<표 37> 개인정보의 유출 가능성 인지 여부

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	50 (64.1)	21 (26.9)	7 (9.0)	78 (100.0)
국내 기업 종사자	32 (57.1)	19 (33.9)	5 (8.9)	56 (100.0)
합계	82 (61.2)	40 (29.9)	12 (9.0)	134 (100.0)
통계량		χ^2 = .794	p = .672	

개인정보의 유출 가능성에대한 인지 수준을 살펴보면, 그렇다가 61.2%로 나타나 개인정보가 모르는 사이에 유출되어 사용되어 있다고 생각하는 수준이 높은 것으로 나타났다. 보통이다는 29.9%로 나타났으며 그렇지 않다는 응답은 9.0%에 불과하였다. 이는 두 그룹 간 정보 사용자의 우려가 나타난 결과이나 9%의 사용자는 아직도 그 가능성에 대해 인지하고 있지 않음이다.

네트워크상에서 다른 사용자와 자료를 공유할 경우, 공유 목적 외에 자료를 열람, 복사, 변조 등을 할 수 있다고 생각하는가에 대하여 64.2%가 그렇다고 응답하였고 22.4%는 보통이다고 응답하였으며 그렇지 않다고 응답한 경우는 13.4%에 불과하였다. 즉, 네트워크상에서 자료의 위 · 변조 가능성에 대한 불안감이 높은 것으로 나타났다.

<표 38> 자료의 위·변조 가능성 인지 여부

구 분	그렇다	보통이다	그렇지 않다	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	49 (62.8)	16 (20.5)	13 (16.7)	78 (100.0)
국내 기업 종사자	37 (66.1)	14 (25.0)	5 (8.9)	56 (100.0)
합계	86 (64.2)	30 (22.4)	18 (13.4)	134 (100.0)
통계량		χ^2 = 1.800	p = .407	

<표 39> 개인정보 유출 경로

구 분	정부부서 담당자	임원/인사 담당자	고객관리 회사의 종사자	해커 또는 외부 침입자	기타	합계
	N (%)	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	4 (5.1)	2 (2.6)	38 (48.7)	27 (34.6)	7 (9.0)	78 (100.0)
국내 기업 종사자	4 (7.1)	2 (3.6)	26 (46.4)	22 (39.3)	2 (3.6)	56 (100.0)
합계	8 (6.0)	4 (3.0)	64 (47.8)	49 (36.6)	9 (6.7)	134 (100.0)
통계량			χ^2 = 1.979	p = .740		

개인정보 유출의 경로는 누구로부터 이루어진다고 생각하는가에 대하여 살펴보면 절반에 가까운 47.8%가 고객관리 회사의 종사자라고 응답하였다. 이는 매체를 통하여 고객의 정보를 다른 업체에 팔아넘긴 사례라던가 고객의 정보 관리를 못하여 침해 사건이 발생한 사건 사례, 텔레마케팅을 통해 원하지 않은 전화를 받은 경험 등이 이 항목을 선택한 이유로 생각된다. 36.6%는 해커 또는 외부 침입자라고 응답하였다. 전반적으로 두 그룹이 이 문제에 대해 공통된 생각을 가지고 있는 것으로 파악되었다.

타인의 정보를 해킹/무단복사/변조/열람한 경험이 있는가를 살펴보면 88.1%가 그런 적 없다고 응답하였으며 1-5회의 경험이 있는 경우는 4.5%, 6회 이상과 시도만 해보고 실패한 경우는 각 3.7%로 나타났다. 국내 기업 종사자가 해킹/무단복사/변조/열람 빈도수와 성공확률에서 더 높은 것으로 미세한 차이가 파악되었고, 그런 적 없다의 답변이 88.1%가 나온 이유를 조사 대상 일부 사용자들에게 직접 문의한 결과 우연히 열람하게 된 경우는 제외하였고, 해킹과 연결하여 자료를 열람한 것으로 생각하였다는 추가적인 답변을 받았다. 이는 해킹과 연관되지 않고 우연히 또는 의도적으로 타인이 자료를 무단 열람한 경우 그 비율이 더 높아질 수도 있다고 파악된다.

<표 40> 해킹/무단복사/변조/열람 경험 여부

구 분	1-5회	6회 이상	시도만 해보고 실패	그런 적 없다	합계
	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	2 (2.6)	2 (2.6)	4 (5.1)	70 (89.7)	78 (100.0)
국내 기업 종사자	4 (7.1)	3 (5.4)	1 (1.8)	48 (85.7)	56 (100.0)
합계	6 (4.5)	5 (3.7)	5 (3.7)	118 (88.1)	134 (100.0)
통계량		χ^2 = 3.244		p = .356	

4. 정보 이용자의 정보보안교육에 대한 인식

<표 41> 조직 내 정보보안 인식 제고 프로그램의 존재 인지

구 분	운영되고 있음	계획중임	준비단계임	모름	고려하고 있지 않음	합계
	N (%)	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	25 (32.1)	5 (6.4)	1 (1.3)	43 (55.1)	4 (5.1)	78 (100.0)
국내 기업 종사자	13 (23.2)	7 (12.5)	8 (14.3)	21 (37.5)	7 (12.5)	56 (100.0)
합계	38 (28.4)	12 (9.0)	9 (6.7)	64 (47.8)	11 (8.2)	134 (100.0)
통계량		χ^2 = 14.733		p = .005**		

**p<.01

회사 내에 정보보안 인식 제고 프로그램의 수립 또는 시행에 대한 인지수준을 살펴보면 전반적으로 모르고 있다는 응답이 47.8%로 가장 많아 프로그램 존재에 대한 인지도가 매우 낮았다. 정보보안 인식 제고 프로그램이 운영되고 있는 경우는 28.4%로 나타났으며 계획 중인 경우는 9.0%, 준비단계에 있는 경우는 겨우 6.7%로 나타났다. 정보보안 인식제고 프로그램이 운영되고 있다고 응답한 내용에선 외국계 기업의 종사자가 인지도가 높았고, 모른다는 답변에서는 외국계 기업의 종사자가 낮은 인지 비율을 보였다. 계획 중이거나 준비단계에 있는 경우 과거 기업의 정보보안 우선순위가 기술적인 부분에 치우쳐 정책이나 사용자의 교육을 등한시 하였던 것과 2005년 국가정보원-정보통신부의 국가정보보호백서[27]에 정보보호 교육의 문제점으로 교육기회 부족 26%, 전문교육프로그램의 부족 23%, 전문교육프로그램의 부족 23%, 예산부족 14% 그리고 관리자의 인식부족이 16%를 보인 것에 그 해답을

27) 국가정보원 · 정보통신부, "2005 국가정보보호백서", 2005; 국가정보원 · 정보통신부, "2006 국가정보보호백서", 2006.

찾을 수 있겠다. 전체적으로 이 부분은 지속된 정보보안 교육을 통해 사용자들의 정보보안 인식 제고를 향상시킬 수 있는 시간을 가져야 한다는 것을 의미한다. 이를 두 그룹 간 차이 분석을 실시한 결과 외국계 기업 종사자(55.1%)가 국내 기업 종사자(37.5%)에 비하여 모르고 있다는 응답이 많아 프로그램 존재에 대한 인지도가 낮았다($p<.01$).

<표 42> 정보 인식 제고 프로그램의 수행 주기

구 분	1-2회	3-4회	5회 이상	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	7 (28.0)	9 (36.0)	9 (36.0)	25 (100.0)
국내 기업 종사자	5 (38.5)	6 (46.2)	2 (15.4)	13 (100.0)
합계	12 (31.6)	15 (39.5)	11 (28.9)	38 (100.0)
통계량		χ^2 = 1.775	p = .412	

정보보안 인식 제고 프로그램이 운영되고 있는 회사 종사자 38명을 대상으로 정보보안 인식 제고 프로그램의 수행 주기에 대하여 살펴보면 1-2회가 31.6%, 3-5회는 39.5%, 5회 이상은 28.9%로 나타났다. 정보사용자의 인식 제고 프로그램에 대한 인지율이 낮음에 따라 다양한 정보 인식 제고 프로그램을 제대로 이해하지 못했을 수도 있고 관심 있게 지켜보지 않을 경우 그 범위나 방법에 대해 과소평가 할 수도 있을 것이다. 그 수행 주기가 일 년에 5회 미만 정도인 비율이 71.1%라는 것은 앞으로 기업과 정부가 좀 더 자주 그리고 효과적으로 정보 사용자의 인식 제고를 위해 비용을 투자하고 시간을 할애해야 한다는 것을 의미한다. 아래 <표 43> 정보보안 인식 제고 프로그램의 도움 여부의 내용을 보았을 때 도움이 된다는 비율이 65.8%인 것을 감안하면 의미 있는 내용이라 할 수 있다.

<표 43> 정보보안 인식 제고 프로그램의 도움 여부

구 분	도움이 됨	보통이다	도움이 안 됨	합계
	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	17 (68.0)	7 (28.0)	1 (4.0)	25 (100.0)
국내 기업 종사자	8 (61.5)	5 (38.5)		13 (100.0)
합계	25 (65.8)	12 (31.6)	1 (2.6)	38 (100.0)
통계량		χ^2 = .871	p = .647	

정보보안 인식 제고 프로그램의 도움 정도에 대하여 살펴보면, 도움이 된다는 의견이

65.8%로 도움이 많이 되는 것으로 나타났다. 앞서 <표 42> 정보인식 제고 프로그램의 수행 주기에서 언급한 내용과 같이 사용자는 정보보안 인식 제고 프로그램이 도움이 된다고 하였지만, 기업에서 그 수행 주기가 많지 않음은 개선되어야 할 과제라 생각한다.

<표 44> 도움이 되지 않는 이유

구 분	형식적 이어서	관심부족	지루해서	전문성 부족	합계
	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	5 (20.0)	14 (56.0)		6 (24.0)	25 (100.0)
국내 기업 종사자	2 (15.4)	7 (53.8)	1 (7.7)	3 (23.1)	13 (100.0)
합계	7 (18.4)	21 (55.3)	1 (2.6)	9 (23.7)	38 (100.0)
통계량		χ^2 = 2.032		p = .566	

도움이 되지 않는다면 그 이유에 대하여 살펴보면 관심이 부족하기 때문에가 55.3%로 가장 많았고 전문성이 부족하기 때문에 도움이 되지 않는다는 의견은 23.7%, 형식적 이어서 도움이 되지 않는다고 응답한 경우는 18.4%로 나타났다. 기업에서는 좀 더 다양한 방법으로 사용자의 관심을 유도해 낼 수 있는 방법을 개발하고 더 전문적인 교육 방법으로 효과적인 교육으로 사용자에게 다가설 수 있어야 한다는 결과라 할 수 있겠다.

<표 45> 인식 제고 방법

구 분	뉴스레터/ 포스터	사내 게시판	사내잡지	기타	합계
	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	10 (40.0)	9 (36.0)	3 (12.0)	3 (12.0)	25 (100.0)
국내 기업 종사자	7 (53.8)	4 (30.8)		2 (15.4)	13 (100.0)
합계	17 (44.7)	13 (34.2)	3 (7.9)	5 (13.2)	38 (100.0)
통계량		χ^2 = 2.069		p = .558	

정보보안 인식 제고 프로그램의 인식 제고 방법에 대하여 살펴보면 뉴스레터와 포스터를 이용하는 경우가 44.7%로 가장 많았고 사내 게시판을 이용하는 경우는 34.2%로 나타났다. 이는 사용자의 눈에 가장 많이 띄고 비용이 제일 저렴한 방법을 선택한 결과로 호순근(2004)[28]의 정보보호 인식제고 현황조사 및 시스템 구축방안 연구에서도 보안의 날 행사나

28) 호순근, 전게서.

그룹웨어 게시판 공고 등의 비용이 들어가지 않는 항목에 대해서만 시행된 연구 결과를 보였다. 기타의 답변에는 이메일을 통하거나 정보보안 캠페인 또는 정보보안의 날을 기업자체에서 정하여 사용자를 계도하는 기업도 있었는데 예산이 책정되어 있다면 기업 전사 차원에서 캠페인이나 사내 자체 보안의 날 등의 지정은 사용자에게 정보보호를 인식시키는데 매우 효과적이고 바람직한 방법이라 판단한다.

<표 46> 정보보안 인식 제고 프로그램을 수행하는 부서

구 분	IT부서	보안부서	정보보안 부서	기타	합계
	N (%)	N (%)	N (%)	N (%)	N (%)
외국계 기업 종사자	23 (92.0)		2 (8.0)		25 (100.0)
국내 기업 종사자	5 (38.5)	3 (23.1)	1 (7.7)	4 (30.8)	13 (100.0)
합계	28 (73.7)	3 (7.9)	3 (7.9)	4 (10.5)	38 (100.0)
통계량		χ^2 = 16.790		p = .001**	

**p<.01

정보보안 인식 제고 프로그램을 수행하는 부서는 IT가 73.7%로 가장 많았고 보안부서와 정보보안 부서에서 수행하고 있는 경우는 각 7.9%로 나타났다. 이를 외국계 기업 종사자와 국내 기업 종사자간 차이분석을 실시한 결과 외국계 기업은 92.0%가 IT에서 정보보안 인식 제고 프로그램을 수행하였으나 국내 기업은 기타 부서에서 수행하는 경우가 30.8%로 나타나 유의미한 차이를 보였다(p<.01). 외국계 기업은 보통 IT에서 정보보안 인식 제고 프로그램을 수행하였고 국내 기업은 IT를 포함한 기타 부서에서 수행하는 경우가 많았다. 기타의 답변에는 경영기획부, 관리부 등이 있었는데 조직적인 구조상 이 부서들이 정보보안 부서나 IT부서보다 상위에 있는 상황일 수도 있고 기업에서 비용이나 인력 부족 또는 주체부서에 대한 중요성의 인식 비율이 낮아 관리부나 경영기획 부서에 그 책임을 맡기고 일반적인 정보보안 인식 제고 프로그램을 수행하는 경우도 있다 하겠다. 실제 본 연구자의 주변에는 이와 같은 경우를 많이 보아왔고, 그에 대한 해답을 <표 44> 정보보안교육이 도움이 되지 않는 이유에서 그 해답을 찾을 수 있는데 이는 정보보안을 수행하는 부서가 전문적이지 않고 사용자의 요구를 충족시키지 못함으로서 형식적이게 되고 사용자는 이를 어렵게 받아들여 관심부족을 낳은 악순환이 이루어 진 결과라 파악된다. IT부서에서 정보보안 인식을 수행하고 있는 경우 기업에서 정보보안을 전담할 부서가 없고, 비용과 관련 인력이 많지 않음이 크다고 하겠다.

V. 결론

오늘날 우리나라는 언제 어디서나 인터넷에 접속하여 정보를 신속하게 얻을 수 있으며 세계최고 수준의 IT 인프라와 기술적 우위를 가지고 있다. 그러나 급속한 정보화 환경의 변화 속에 정보침해사고라는 심각한 역기능이 등장하였고, 이 역기능의 중심은 사람이라고 판단된다. 이에 본 연구에서는 외국계 기업 종사자와 국내 기업 종사자간 정보관리에 대한 인식, 정보보안의식, 정보보안교육에 대한 인식 차이를 파악하여 회사의 특성에 따른 인식 차이가 있는가를 알아보고 이를 분석하여 정보사용자들의 정보보안 인식을 고취하고 중요성에 대해 강조하고자 하였다.

전반적으로 정보이용자들의 정보보안 인식은 외국계 기업 종사자와 국내 기업 종사자간 차이는 거의 없었다. 정보보안이라는 주제는 다양한 매체들로부터 알려지고 강조되어 이미 보편적인 이슈가 되었으며, 이러한 수준은 국내·외 기업 간 차이보다는 진행되고 있는 사회적 현상이라고 볼 수 있다. 한국전산원이 2006년에 발표한 '2005년 정보화통계조사'[29] 결과에 의하면, 2004년 7월부터 2005년 6월까지 PC 보유사업체 중 바이러스 피해를 경험한 사업체가 28.9%로 전년의 같은 기간과 비교 하였을 때 9.9%가 감소한 것으로 나타났고, 해킹 피해 현황 역시 전년의 같은 기간보다 0.6% 감소한 것은 물론 정보보호 제품을 사용한 업체는 3.3% 증가 하였으며 이는 대부분의 기업들이 정보보안의 중요성에 대해 인지하고 정보보안에 능동적으로 대처하였다는 것을 보여준다. 또한, 전체적인 결과는 단지 그들의 개인적 상황(학력, 직종, 업무, 경력)에 따라 다소 유의한 차이가 있을 뿐이지 기업형태에 따른 차이는 없다고 판단되며, 조사에서 정보이용자들의 개인정보관리 수준과 정보보안 의식 수준은 낮은 것으로 나타나 개인정보관리와 정보보안 의식을 함양시키기 위한 교육과 홍보가 필요할 것으로 판단된다. 조사에서 해당 기업이 정보보안교육에 얼마나 많은 예산을 할당하고 있으며 집행하였는지 조사가 가능하였다면 좀 더 정확한 결과를 얻을 수 있었는데 일반 사용자를 대상으로 한 조사이다보니 정보보안 예산과 관련된 정보를 취득하기 어려웠고, 사용자들이 그런 자료에 대한 공개를 꺼리는 이유로 인하여 이번 조사영역에 포함하지 못하였다. 주목할 만 한 점은 정보이용자들이 개인정보 유출에 대한 우려와 불안감 수준이 아주 높다는 것이다. 비록 사용자들이 정보관리를 잘못하고 있더라도, 정보 유출에 대한 불안이 높기 때문에 기업이나 정부에서는 이와 같은 우려를 잘 활용한다면 일반 정보 사용자들의 정보보안 실천에 큰 도움이 될 것이다. 또한 정보사용자들의 정보 유출에 대한 높은 불안감이나 신용 거래 사고 등에 대한 국민의 불신감 증대가 정보화 사회의 기반을 깊숙이 흔드는 원인이 되며 이는 곧 국가 대외 신인도에 있어서 영향을 미치게 되므로 이를 해소

29) 정보통신부 · 한국전산원, "2005년 정보화통계조사", 2006.03.24.

할 수 있는 대처 방안이 국가 차원에서 마련되고 조속한 시일 내에 실행되어야 할 것이다.

조직 내에서의 정보보안 교육의 인지도 및 그 수준 역시 아직은 낮은 수준으로 파악되기 때문에, 각 기업들은 직원들을 대상으로 내실 있고 전문성 있는 정보보안 교육을 실시하여 일반 사용자의 정보보안 이해와 실천을 독려함으로서 정보 보호 수준을 높일 수 있어야 할 것이다.

참고문헌

국가사이버안전센터, “인터넷시대 정보보호 생활수칙”, 2005.01.13.

국가정보원・정보통신부, “2005 국가정보보호백서”, 2005.

국가정보원・정보통신부, “2006 국가정보보호백서”, 2006.

김기윤・나관식・김종석, “보안관리를 위한 위협, 자산, 취약성의 분류체계”, 「통신정보보호학회지」, 제5권 제2호, 한국통신정보보호학회, 1995.06.

김현수, “정보보안수준 계량화 연구”, 「경영정보학연구」, 제9권 제4호, 한국경영정보학회, 1999.

대한상공회의소, 「국내 기업과 외국계 기업의 위기관리 실태 및 대응방안 비교조사」, 2002.11.

박주흠, “정보이용자들의 특성에 따른 정보보안의식에 관한 연구”, 계명대학교 경영대학원 석사학위논문, 2002.

배홍문, “정보보안에 대한 경제적 고찰과 정책방안에 관한 연구”, 서강대학교 경제대학원 석사학위논문, 1997.

신용섭, “교사의 정보보호 및 보안의식에 대한 실태 분석”, 춘천교육대학교 춘천교육대학원 석사학위논문, 2005.

이종삼, “국내 기업 정보시스템 Security 위협 요소에 관한 연구”, 중앙대학교 국제경영대학원 석사학위논문, 1995.

임영모 외 2인, “CEO Information”, 삼성경제연구소(SERI), 제472호, 2004.10.20.

정보통신부, “개인정보보호지침”, 2002.01 고시(http://www.mic.go.kr).

정보통신부・한국전산원, “2005년 정보화통계조사”, 2006.03.24.

정보통신부, “개인정보 보호를 위한 종합대책(안)”, 2005.09.27.

최원혁, 「기업정보온라인유출, 유형 및 사례 분석」, 국가사이버안전센터, 2005.

호순근, “정보보호 인식제고 현황조사 및 시스템 구축방안 연구”, 동국대학교 국제정보대학원, 석사학위논문, 2004.

한국전산원, 「2005 국가정보화백서」, 2005.

한국전산원, 「2007 국가정보화백서」, 2007.

한국정보보호진흥원(http://www.kisa.or.kr), “2005년 정보보호 실태조사”, 2005.

IBM, “2005 Global Business Security Index Report,” 2005.

ITU, “ITU Internet Reports 2004,” 2004.09.

Laudon, Kenneth C., and Jane P. Laudon, *Management Information Systems: Managing the Digital Firm*, 10th edition, Pearson Education International: Upper Saddle River, NJ, 2007.

Symantec, “Symantec Internet Security Threat Report(Jan. 05 - Jan. 06),” Vol.VIII, 2005.09(http://www.symanatec.com).