Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.1, Feb. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.1.197

정보보호담당자의 역할이 조직의 정보보호수준에 미치는 영향

최 동 근,† 송 미 선, 임 종 인, 이 경 호‡
고려대학교 정보보호대학원

Study the role of information security personnel have on an organization's information security level

Dong-Keun Choi,† Mi-Sun Song, Jong In Im, Kyung-Ho Lee‡
Korea University

요 약

조직 내의 정보보호에 대한 이슈는 최근에 와서야 조직의 리스크로 인지되기 시작하였다. 정보보호 사고로 인하여 정보보호책임자 뿐만 아니라 대표, 임원 및 개인정보책임자까지 사임하거나, 기업에 커다란 금전적 피해와 회복하기 어려운 대고객 신뢰 등에 막대한 악영향을 초래하였다. 특히 개인정보 유출사고가 조직내 미치는 영향이 기업의 생존 문제로까지 인식되고 있는 이때에, 조직의 정보보호 수준을 향상시킬 수 있는 여러 가지 방안 중 정보보호 담당자의 역할과 업무수행이 어느 때보다 크게 부각되고 있으며, 이들 정보보호 담당자가 조직의 정보보호 수준에 얼마나 영향을 끼치는지 본 연구를 통하여 파악코자 한다. 본 연구에서는 기업내 정보보호 담당자들을 대상으로 조직 내 정보보호 담당자의 보안전담 업무수행 비중과 조직의 정보보호 수준 등 현상을 파악하고 이들 간의 상관관계를 분석하여 영향도를 분석하고자 한다. 이를 통해 기업내 정보보호 담당자의 보안업무비중을 전담 또는 크게 비중을 높임으로써 조직의 정보보호 수준을 향상시키고자 한다.

ABSTRACT

The issue of information security within an organization began to be recognized as risk of the organization. Because of this, not only ISO(Information Security Officer) but an executive or CEO were forced to resign. In addition, it brought about heavy financial damage to the company and made the company difficult to restore trust to customers. At a time when inadvertent disclosure of personal information has become accepted as a matter of survival because of having a bad effect within an organization, how the information security specialist causes influence on information protection level of the organization. For these reasons, targeting the information security specialists of various industry sectors, we'll analyse how task performance rate of the information security specialist within an organization cause influence to the information security level. The goal of this study is for the company to raise the task proportion of information security specialist and to improve the information protection level of the organization.
Keywords: Security organization, security level

I. 서 론

1.1 연구배경

한국의 정보보호는 지난 1960년대 산업화가 시작되었을 때에도, 1980년대 정보화가 시작되었을 때에도

접수일(2014년 11월 26일), 수정일(2014년 12월 17일), 게재확정일(2014년 12월 17일)
† 주저자, dkchoi@lottecard.co.kr
‡ 교신저자, kevinlee@korea.ac.kr (Corresponding author)

하드웨어나 시스템 소프트웨어와 같이 인프라로 인지되지 못하고 생산성 증대, 편리성, 신속성 등 비즈니스 측면이 먼저 고려되면서, 정보보호에 대한 정책과 구축 등이 고려하지 않고, 구현하지 않아도 되는 것으로 인식되어 조금도 관심의 대상이 되지 못하였다.
2000년 초반 인터넷이 상용화되고 전자상거래가 시작되면서부터 우리나라에도 정보보호에 대한 인식이 조금씩 달라지기 시작하였다. 정보보호가 보장되지 않는 한 전자상거래가 활성화될 수 없었기 때문이다. 초기에는 네트워크 위주의 보안대책을 구현하면 해결될 것으로 생각하고 네트워크 보안장비 개발과 구축으로 보안대책을 구현하였다. 하지만 IT의 급속한 발전으로 인해 보안사고가 증가하게 되었고, 그 피해액이나 대상도 크게 늘어나게 되었다.

2000년 초기, 대한민국에 벤처기업이 활성화되면서 보안 벤처기업에 대한 연구 및 투자가 시작되었으며, 보안에 대한 투자확산과 더불어 보안시장이 형성되기 시작하였다. 이때부터 보안 산업이 대한민국 산업의 한 분야로 자리 잡기 시작하였다.

우리나라의 보안 산업은 초기 미국이나 유럽, 이스라엘의 보안산업에 비해 매우 열악하였으나, 정부 정책지원과 벤처기업들이 보안산업에 뛰어들면서 우리나라의 보안기술도 성장을 거듭하여 지금은 세계시장으로 진출하는 등 가시적인 성과를 나타나고 있다. 그럼에도 불구하고, 우리나라의 정보보호 사고는 해를 거듭할수록 많은 폐해가 나타나고 있으며, 특히 개인정보 - 주민번호나 계좌번호 등 - 의 유출로 인한 피해가 날로 급증하고 있다.

2011년 옥션사태를 시작으로 대량의 개인정보가 유출되어 사회적 파장을 불러왔으며 2014년초 카드의 개인정보 유출은 건수만으로도 초유의 사건으로 기록되게 되었다[12].

기업 내의 보안리스크는 기업만의 문제가 아닌 사회적 문제로 부각되었으며, 최근 개인정보보호 유출로 인해 기업의 CEO 및 임원이 해임되고 이로 인한 금전적 피해 및 손해배상 등 기업 이미지에 심각한 타격을 주었다. 조직 내의 정보보호에 대한 이슈가 조직의 리스크로 인지되기 시작하였다.

그러나 조직 내의 정보보호 담당자는 여전히 정보보호 산업이 시작한 초기의 수준에서 조금도 나아진 것이 없이 기업의 고객정보를 관리하는 수준이 취약한 수준에 머무르고 있다. 기업의 정보보호 수준을 향상하기 위해서는 조직의 보안인식 수준이 높아져야 하며, 이를 위해 지속적인 투자 및 정보보호 인력이 양성되고 현장에 배치되어 정보보호 활동을 지속적으로 수행하여야 한다.

우리나라 기업이나 기관의 정보보호 담당자는 보안 전문 지식이 미흡할 뿐더러 보안활동을 전담하기보다 본인의 주 업무와 병행 또는 일부만 담당함으로써 정보보호 수준을 향상시키지 못하고 있다. 정보보호 담당자 역시 정보보호 역할의 중요성을 인지하지 못함으로써 정보보호 활동을 적극적으로 전개하지 못하고 있다.

1.2 목적

본 연구에서는 조직 내의 정보보호 담당자의 우리나라 기업 내에서 직급구조, 정보보호 활동의 전담비율의 변화에 따른 조직 내 정보보호 수준을 파악하고 분석하고자 한다.

정보보호가 조직의 최상위 리스크로 대두된 현재의 상황에서 기업 내 정보보호 담당자의 위상을 재조명하여 조직의 정보보호 수준이 향상될 수 있는 방안을 연구하고자 한다.

이를 통하여 조직 내 정보보호 담당자에 대한 인식 수준을 강화하여 조직의 정보보호 수준을 높이는데 기여할 수 있으며, 또한 정부의 보안인력 정책에 변화를 가져오게 함으로써, 조직이나 정부의 보안 전담인력 채용이 확대되고 보안인력 수요에 대한 확산이 될 수 있다.

1.3 연구방법

본 연구의 목적을 달성하기 위하여 보안담당자의 보안전담 업무비중이 해당 기업의 정보보호 수준과 상관관계가 있을 것이라는 가설을 가지고 2012년 이후 3차례에 걸쳐 총 57개 기업의 관련 데이터를 수집하였다. 2012년 25개 기업, 2013년 17개 기업, 2014년 15개 기업의 보안담당자를 대상으로 조사하여 수집하였다.

수집된 데이터는 정보보호 담당자에게 있어 본인의 업무 중, 정보보호 직무 수행비율과 정보보호 담당자의 직급 및 성명, 소속, IT연관성 등의 조사를 통해 데이터를 수집하였으며, 3년 동안 일관되게 데이터를 수집하여 데이터의 정확도 및 신뢰도를 높였다. 정보보호 담당자의 보안전담 업무수행 비율을 기업의 정보보호 담당자가 자신의 업무 중 보안전담비율을 직접 기술하게 하였으며, 이를 토대로 기업의 정보보호 담당자의 보안전담 업무수행 데이터로 활용하였다.

또한 기업의 정보보호 수준을 메일 바이러스 훈련의 결과 값으로 얻어진 데이터를 분석하여 그 상관성을 도출하였다. 해당 기업의 메일 바이러스 훈련은 보안담당자를 조사한 동일 기업을 대상으로 매년 총 3회 실시한 데이터 결과 값을 가지고 분석하였다. 조사한 전체 인력은 45,060명의 직원들의 모의 메일바이러스 결과 데이타를 대상으로 수집하였다.

그리고 정보보호담당자의 IT유관 경험이나 직무를 가지고 있느냐가 조직의 정보보호 수준과 연관성이 있을 것이라는 생각을 가지고, 정보보호 담당자의 IT유관 업무수행을 하고 있는지를 조사하였다. 이는 IT유관 업무수행을 하는 정보보호담당자가 있는 조직이 Non-IT 업무수행을 하는 정보보호담당자가 있는 조직보다 정보보호 수준이 높을 것이라는 가설을 데이터의 상관성으로 확인코자 한다. IT유관 업무수행을 하는지에 대해서는 기업의 정보보호 담당자가 기술한 부서의 특성이나 역할을 분석하여 판단하였다. 즉, IT기획이나 정보보호 관련 역할을 수행하는 정보보호담당자는 IT유관 업무수행을 하는 것으로 보고, 그 나머지는 Non-IT 업무수행을 하는 것으로 분석하였다.

II. 관련연구

2.1 유사연구 사례 분석

기업에서의 가장 큰 정보보호 위협이 되는 사람은 보안위협이 미흡하거나 조심성이 없는 직원들이라고 1809명을 설문 조사한 결과 514명, 28.4%가 응답하였다[9].

조직 내부의 상황을 가장 잘 알고, 권한 있는 내부자가 보안솔루션을 우회하거나 일시적인 차단하는 방법을 아는 직원들에 의한 보안이 취약해 지는 상황을 만든다고 보안담당자들이 응답을 한 것으로, 최근 스마트 환경에서 직원의 절반 이상은 개인용 스마트기기 사용 제재에 관한 회사의 BYOD 정책에 강한 불만을 가지고 있으며, 정책을 위반할 생각도 있는 것으로 나타났다. 포티넷은 '2013 인터넷 보안 설문조사 (Fortinet 2013 Internet Security Survey)' 발표에서 일명 Y세대라 불리는 21-32세 직원들을 대상으로 자체 실시한 설문에서 스마트폰, 태블릿 PC 등 개인용 스마트 기기를 보유하고 있는 직원들을 대상으로 진행되었다[10].

개인 스마트기기 사용에 따른 회사의 방침을 위반할 생각이 있는가? 라는 질문에 '그렇다'라고 응답한

Table 1. Results of the survey of 1,809 staff of Information Security on October 14. 2014.

Who do you think is the person who imperils the security most?		
Item	%	Response Number
the staffs who are inadequate for the security consciousness or careless about it	28.43	514
the executives who don't care for the security	27.30	494
the staffs who are just to lazy to use the security procedures and system	26.28	475
the teenager or youth hackers who have no sense of morals He looks like he has no sense of morals	6.75	122
the organization of cyber warfare that is state sponsered or belong to a country	3.27	59
international hacker group	2.76	50
the hackers who belong to a criminal organization	5.01	91
Others	0.20	4
TOTAL	100	1,809

비율이 2012년 비교해 전세계적으로 42%가 증가했으며, 특히 한국은 90%나 증가한 수치를 보였다고 발표하였다. 또한 전체 응답자 중 51%(한국 57%)는 개인용 스마트기기를 회사에서 개인적 혹은 업무용도로 사용하는 행위를 금지하는 회사 정책을 위반할 생각이 있는 것으로 응답 하였다.

이처럼 보안위협이 미흡하거나 조심성 없는 임직원이 보안을 취약하게 하며, 스마트 환경에서 회사의 보안방침을 위반할 생각이 있다고 한 직원이 42% 로 나타난 것에서 볼 때, 조직에서의 임직원의 정보보호 인식은 스마트환경 이전과 비교해서도 매우 낮다고 볼 수 있다.

그럼에도 불구하고 기업에서의 정보보호 전문인력의 확보나 인력양성은 부족한 실정이다. 2014년 7월 조사된 개인정보보호, 정보보호담당자들을 대상으로 업무수행에 있어 가장 큰 애로사항이 무엇이냐는 설문에서 911명의 응답자 중 367명, 40%가 정보보호 전문인력이 부족하여 보안업무 부담이 증가하고 있다고 응답하였다[11].

Table 2. One of the biggest difficulties in the performance of security personnel?(2014-7-21)

Item	%	Response Number
Lack of security expertise	40.3	367
Security incidents: liability	27.3	248
CEO and management team expanded the investment through persuasion	18.5	168
A low level of remuneration	6.4	58
Frequent night shift and weekend work	4.7	43
Others	2.8	26
TOTAL	100.0	911

2.2 유사연구에서의 도출된 의미

Table 1.의 설문결과에서 나타난 바와 같이 기업에서의 가장 큰 정보보호 위협이 되는 사람이 보안위협이 미흡하거나 조심성이 없는 직원들이라고 응답하였고, Table 2.에서는 정보보호 담당자들이 업무수행에 있어 가장 큰 애로사항이 정보보호 전문인력이 부족하다고 응답함에서 임직원들을 교육시키고 정보보호 인식을 개선하기 위해서는 정보보호 전문인력이 필요하다는 의견에 동의하게 될 것이다. 또한 이를 개선하기 위해 지속적인 보안교육 및 보안활동을 전개되는 것이 필요하다고 볼 수 있다.

이상의 사례에서 살펴본바와 같이, 조직의 정보보호 수준향상을 위해 정보보호 담당자는 반드시 필요하며, 정보보호 교육 및 관련 보안활동을 통해 보안수준 향상을 꾀할 수 있으며, 이는 정보보호 담당자의 역할로 매우 중요한 것이라 할 수 있다.

또한 기존의 연구들에서는 조직의 정보보호 담당자의 보안전담 비중에 대해 논의된 연구논문들이 없으며, 더구나 수집된 데이터에 근거한 분석된 논문 또한 없는 것으로 파악된다. 따라서 본 연구를 통하여 조직의 정보보호 담당자의 IT관련 기능을 수행하는지에 따라 정보보호 수준이 달라지는지, 보안전담 조직의 유무에 따라 정보보호 수준이 달라지는지, 그리고 정보보호 담당자의 업무중 보안전담비중에 따라 정보보호 수준이 달라지는지를 연구, 분석해 보고자 한다.

III. 연구대상 및 가설설정

3.1 수집된 데이터와 가설

본 연구에서는 정보보호 담당자의 보안전담 업무비중과 IT유관 업무수행을 하는 담당자가 조직의 정보보호 수준과 관계가 있음을 수집된 데이터의 분석을 통해 도출하였고, 수집된 데이터는 조직의 정보보호 담당자의 현황 및 모의 메일 바이러스 훈련 결과값을 가지고 조사하였다.

본 연구에서는 다음과 같이 가설을 설정하였다.

가설1. 조직내 정보보호 담당자의 정보보호 업무비중에 따라 해당 조직의 정보보호 수준에 영향을 미치게 된다는 것이다. 이에 따라 정보보호 담당자의 업무비중이 보안업무를 전담으로 하거나 보안업무 비중이 높을수록 조직의 정보보호 수준이 높게 나타난다는 것이다.

가설2. 조직내 정보보호 담당자가 IT유관 업무수행을 하는 보안담당자가 속한 기업이 Non-IT 업무수행을 하는 보안담당자가 속한 기업보다 높은 정보보호 수준을 나타낸다는 것이다.

가설3. 조직내 정보보호 전담부서가 있음으로 해당 조직의 정보보호 담당자가 적극적 활동을 통하여 정보보호수준이 정보보호 전담부서가 없는 조직의 정보보호 수준과 차이가 있는지를 확인하여 전담부서가 있는 조직의 정보보호 수준이 높다는 것을 확인하고자 한다.

3.2 자료 수집 및 분석 방법

먼저 정보보호 담당자의 보안업무 수행비중이 정보보호 수준과의 상관성을 분석하기 위해, 수집된 데이터 군에 대해 정보보호 담당자의 본인 업무중 정보보호 비중을 백분율로 표시하도록 하여 데이터를 수집하였다.

두번째로 정보보호 담당자의 보안업무 수행이 IT유관업무를 수행하는가에 따른 정보보호 수준과의 상관성을 분석하기 위해, 수집된 데이터 군에 대해 정보보호 담당자의 IT유관부서 소속여부와 정보보호 비중을 백분율로 조사하였다.

세 번째, 정보보호 전담부서가 있어 정보보호 담당자가 보안역할 및 정보보호 관리활동이 적극 수행이 되어 전담부서가 없는 조직과 정보보호 수준 차이가 나타나는지 관련 데이터를 수집하고 조사하였다.

정보보호 수준은 정보보호 교육, 진단, 감사활동 등

전반적인 정보보호 활동에 대한 자료를 분석하여야 하나, 수집된 데이터는 메일 바이러스 훈련에 관한 결과값 만을 기준으로 조사하였다. 메일바이러스 훈련 역시 정보보호 담당자의 정보보호 활동 노력을 주체적으로 하였는지, 아니면 보안업무 중 일부만 수행한자로써 교육 등 보안활동을 등한시 하였는지에 따라 영향이 있을 것으로 보았다.

연구를 위한 자료는 정보보호 담당자의 업무현황을 조사하기 위해 3년간 데이터를 수집하였다. 정보보호 담당자의 회사, 성명, 직급, 부서, 주업무, 보안업무비중, 전담부서 유무, IT유관부서 소속 등을 각각 기술하게 하였다.

특히 보안업무비중은 0~100%로 기입하게 하였다. 비중에 따른 분석을 위해 비중범례를 5등급으로 분류하였으며, 조사된 보안비중에 대한 범례(remarks)는 다음과 같이 구분된다. 등급을 분류한 이유는 보안담당자의 보안업무 비중이 인사나 총무, 재무 등의 일을 하면서 일부 또는 한시적, 부가적인 업무로 0~20%, ~40%, ~60%, ~80% 미만의 보안업무를 하는 담당자와 자신의 주업무가 보안업무를 전담하는 보안담당자인 80%~ 에 해당하는 담당자를 비교하여, 보안전담역할이 80%~ 이상인 부서의 정보보호수준이 높다는 것을 보여주기 위해 등급별로 나누어서 분석 평가를 하였다.

또한 수집된 데이터로부터 정보보호 담당자가 IT유관부서에 속해 있는지 아니면 Non-IT부서에 속해 있는지에 확인하기 위해 데이터를 수집하였고, 마지막으

Table 3. Security personnel form collected from data entry

Company	Name	Title	Department	Main Task	Security Business Portion (%)	Security Dept. Existence (Yes, No)	IT Related departments (Yes, No)

Table 4. Security Portion Remarks

Level	Security Portion (%)
1	0~19
2	20~39
3	40~59%
4	60~79%
5	80% ~ 100%

Table 5.Work status of information security staff

Year	Company	Security Level	Security Portion	Security Portion (remarks)	Security Dept.(o)	IT Related Dept.(o)
2012	1	3.5%	20.0%	2		O
	2	4.0%	10.0%	2		
	3	3.0%	30.0%	2		O
	4	3.0%	50.0%	3		
	5	3.8%	20.0%	2		
	6	1.3%	90.0%	5	O	O
	7	4.0%	20.0%	2		
	8	4.0%	50.0%	3		
	9	3.5%	30.0%	2		O
	10	2.9%	20.0%	2		O
	11	0.2%	100.0%	5	O	O
	12	3.3%	40.0%	3		
	13	2.4%	20.0%	2		
	14	6.3%	30.0%	2		
	15	4.0%	20.0%	2		
	16	1.6%	30.0%	2		O
	17	4.0%	30.0%	2		O
	18	6.0%	20.0%	2		
	19	2.6%	30.0%	2		O
	20	2.0%	70.0%	4		
	21	5.0%	30.0%	2		
	22	1.8%	100.0%	5	O	O
	23	7.5%	10.0%	1		
	24	0.4%	35.0%	3	O	O
	25	4.4%	10.0%	2		
2013	A	13.3%	5.0%	1		
	B	4.4%	100.0%	5	O	O
	C	13.3%	20.0%	2		
	D	0.0%	50.0%	3		O
	E	5.5%	40.0%	3	O	O
	F	4.6%	25.0%	2		O
	G	0.5%	100.0%	5	O	O
	H	9.8%	30.0%	2		O
	I	2.4%	15.0%	2		
	J	1.5%	20.0%	2		
	K	10.0%	10.0%	1		
	L	2.9%	15.0%	2		
	M	12.3%	20.0%	2		O
	N	4.5%	80.0%	5		
	O	14.0%	5.0%	1		
	P	4.2%	100.0%	5	O	O
	Q	6.3%	35.0%	3		O
2014	A1	15.2%	100.0%	5	O	O
	A2	23.0%	100.0%	5	O	O
	A3	17.9%	100.0%	5	O	O
	A4	35.3%	15.0%	2		
	A5	16.0%	100.0%	5	O	O
	A6	4.0%	100.0%	5	O	O
	A7	27.7%	20.0%	2		
	A8	21.9%	100.0%	5	O	O
	A9	5.6%	100.0%	5	O	O
	A10	32.1%	25.0%	2		O
	A11	45.2%	10.0%	1		
	A12	15.2%	100.0%	5	O	O
	A13	13.3%	100.0%	5	O	O
	A14	44.0%	5.0%	1		
	A15	17.8%	100.0%	5	O	O

로 수집된 데이터로부터 조직내 정보보호 담당자가 보안전담 부서에 속해 있는지, 아니면 보안전담 부서가 없는지에 따라 정보보호 수준을 파악하기 위하여 데이터를 수집, 분석하였다.

조직의 정보보호 수준은 2012년 이후 2014년까지 세 차례에 걸쳐 메일 바이러스모의 훈련을 실시하였으며, 이 훈련의 결과를 데이터로 수집하여 정보보호 수준으로 평가하였다. 즉, 해당 메일을 열어서 URL을 클릭하거나 첨부파일을 실행시킨 행위를 보안위반으로 간주하여 이를 데이터 처리하였으며 각 사별 보안수준으로 평가하였다.

메일 바이러스 모의훈련에서 사용된 메일은 다음과 같이 매년 수준을 높여서 훈련을 실시하였다.

먼저 기업의 직원들에게 무작위로 모의 바이러스 메일을 보내면 직원들이 해당 메일을 열어 보았는지, 그리고 받은 메일의 링크를 클릭하는지, 또는 첨부된 파일을 실행하는지를 피드백 받아, URL 링크를 클릭한 직원과 첨부를 실행한 직원의 인원수를 더한 수치가 전체 대상자 대비 몇%인지를 데이터를 집계하였다.

2012년에 실시한 모의 메일바이러스 훈련은 금융관련 정보로써, 최저이율 대출이란 제목으로 첨부파일을 링크하게끔 유도하였으며, 2013년에는 증권가 사설 정보지란 제목으로 직원들에게 호기심을 유발하는 메일로 훈련을 하였으며, 2014년에는 입사지원서를 발송케 함으로써 직원들에게 다른 사람의 정보를 보지 않도록 하는 것에 대한 모의훈련을 실시하였다.

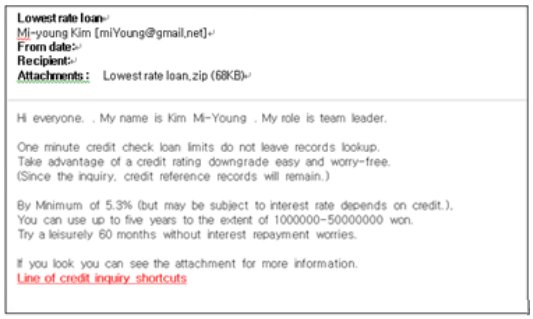
정보보호 담당자의 보안전담 업무비중과 정보보호 수준에 대하여, 수집된 데이터의 상관도 분석을 위하여 SPSS 21(Statistical Packages for Social Sciences)을 사용하였으며, 상관 분석시 적용된 상

Table 6. Mock-mail virus training data form

Company	Department	Name	Mail-ID	Open (Y/N)	URL click	ex-ecu-tion
XXX	기술담당	윤OO	**_yoon@**.net	O	O	X
		곽XX	oo.k-wak@*****.net	O	O	X

Table 7. Mock-mail virus training Aggregate data form

Company	Department	Open (Y/N)	URL click	ex-ecu-tion	Open (Y/N)	URL click	ex-ecu-tion	Total


Lowest rate loan
Mi-young Kim [miYoung@gmail.net]
From date:
Recipient:
Attachments : Lowest rate loan.zip (68KB)

Hi everyone. . My name is Kim Mi-Young . My role is team leader.

One minute credit check loan limits do not leave records lookup.
Take advantage of a credit rating downgrade easy and worry-free.
(Since the inquiry, credit reference records will remain.)

By Minimum of 5.3% (but may be subject to interest rate depends on credit.),
You can use up to five years to the extent of 1000000-50000000 won.
Try a leisurely 60 months without interest repayment worries.

If you look you can see the attachment for more information.
Line of credit inquiry shortcuts

Fig.1. 2012 Mock-mail virus training

관계수는 Pearson 상관계수이다.

또한 정보보호 전담부서 유무와 정보보호 담당자의 주 업무가 IT와 보안과 밀접한 관계가 있는지에 대해서는 상호 정보보호 수준 데이터를 비교분석하여 상관성을 확인하였다.

IV. 분석결과

4.1 상관분석

2012년 각 정보보호 담당자의 업무비중과 메일 바이러스 훈련의 데이터 값을 분석한 결과는 다음과 같다.

Table 8. 2012 Job portion of security staff : Organization of information security levels

Company	Level	Security Tasks Portion(%)
1	3.5%	20.0%
2	4.0%	10.0%
3	3.0%	30.0%
4	3.0%	50.0%
5	3.8%	20.0%
6	1.3%	90.0%
7	4.0%	20.0%
8	4.0%	50.0%
9	3.5%	30.0%
10	2.9%	20.0%
11	0.2%	100.0%
12	3.3%	40.0%
13	2.4%	20.0%
14	6.3%	30.0%
15	4.0%	20.0%
16	1.6%	30.0%
17	4.0%	30.0%
18	6.0%	20.0%
19	2.6%	30.0%
20	2.0%	70.0%

21	5.0%	30.0%
22	1.8%	100.0%
23	7.5%	10.0%
24	0.4%	35.0%
25	4.4%	10.0%

		VAR00001	VAR00002
VAR00001	Pearson correlation coefficient	1	-.613**
	Significant probability (both sides)		.001
	N	25	25
VAR00002	Pearson correlation coefficient	-.613**	1
	Significant probability (both sides)	.001	
	N	25	25

**. The correlation coefficient is significant at the 0.01 level (both sides).

Fig.2. 2012 Coefficient of Correlation : Security personnel of the specific gravity of security work and mock e-mail virus result.

pearson 상관계수: -0.613 (상관계수는 높을수록 관련성이 높은 것으로 보면 되고, (-)의 경우는 반비례의 관계를 나타내었다.)

유의확률: 0.001 (유의확률은 0.5이하가 되어야 의미 있는 상관계수라고 볼 수 있다.)

2012년의 분석결과 정보보호담당자의 보안업무 비중과 모의 메일바이러스 훈련 결과값의 상관계수는 0.613으로 유의수준 0.001에서 연구가설은 지지된다. 즉, 정보보호 수준은 정보보호담당자의 보안업무비중과 상관관계(-)가 있다고 할 수 있다.

2013년 각 정보보호 담당자의 업무비중과 메일 바이러스 훈련의 데이터값을 분석한 결과는 다음과 같다.

Table 9. 2013 Job portion of security staff : Organization of information security levels

Company	Level	Security Tasks Portion(%)
A	13.3%	5.0%
B	4.4%	100.0%
C	13.3%	20.0%
D	0.0%	50.0%
E	5.5%	40.0%
E	4.6%	25.0%
F	0.5%	100.0%
G	9.8%	30.0%
H	2.4%	15.0%
I	1.5%	20.0%
J	10.0%	10.0%
K	2.9%	15.0%
L	12.3%	20.0%
M	4.5%	80.0%
N	14.0%	5.0%
O	4.2%	100.0%
P	6.3%	35.0%

		VAR00001	VAR00002
VAR00001	Pearson correlation coefficient	1	-.519*
	Significant probability (both sides)		.033
	N	17	17
VAR00002	Pearson correlation coefficient	-.519*	1
	Significant probability (both sides)	.033	
	N	17	17

*. The correlation coefficient is significant at the 0.05 level (both sides).

Fig.3. 2013 Coefficient of Correlation : Security personnel of the specific gravity of security work and mock e-mail virus result.

pearson 상관계수: -0.519 (상관계수는 높을수록 관련성이 높은 것으로 보면 되고, (-)의 경우는 반비례의 관계를 나타내었다.)

유의확률: 0.039 (유의확률은 0.5이하가 되어야 의미 있는 상관계수라고 볼 수 있다.)

2013년의 분석결과 정보보호담당자의 보안업무 비중과 모의 메일바이러스 훈련 결과 값의 상관계수는 0.519 로 유의수준 0.033에서 연구가설은 지지된다. 즉, 정보보호 수준은 정보보호담당자의 보안업무비중과 상관관계(-)가 있다고 할 수 있다.

2014년 각 정보보호 담당자의 업무비중과 메일 바이러스 훈련의 데이터값을 분석한 결과는 다음과 같다.

Table 10. 2014 Job portion of security staff : Organization of information security levels

Company	Level	Security Tasks Portion(%)
A1	15.2%	100.0%
A2	23.0%	100.0%
A3	17.9%	100.0%
A4	35.3%	15.0%
A5	16.0%	100.0%
A6	4.0%	100.0%
A7	27.7%	20.0%
A8	21.9%	100.0%
A9	5.6%	100.0%
A10	32.1%	25.0%
A11	45.2%	10.0%
A12	15.2%	100.0%
A13	13.3%	100.0%
A14	44.0%	5.0%
A15	17.8%	100.0%

		VAR00001	VAR00002
VAR00001	Pearson correlation coefficient	1	-.882**
	Significant probability (both sides)		.000
	N	15	15
VAR00002	Pearson correlation coefficient	-.882**	1
	Significant probability (both sides)	.000	
	N	15	15

**. The correlation coefficient is significant at the 0.0 level (both sides).

Fig.4. 2014 Coefficient of Correlation : Security personnel of the specific gravity of security work and mock e-mail virus result.

pearson 상관계수: -0.882 (상관계수는 높을수록 관련성이 높은 것으로 보면 되고, (-)의 경우는 반비례의 관계를 나타내었다.)

유의확률: 0.000 (유의확률은 0.5이하가 되어야 의미 있는 상관계수라고 볼 수 있다.)

2014년의 분석결과 정보보호담당자의 보안업무 비중과 모의 메일바이러스 훈련 결과 값의 상관계수는 0.882 로 유의수준 0.000에서 연구가설은 지지된다. 즉, 정보보호 수준은 정보보호담당자의 보안업무비중과 상관관계(-)가 있다고 할 수 있다.

두 번째 수집된 데이터로부터 정보보호 담당자가 IT 유관부서에 속해 있는지 아니면 Non-IT부서에 속해 있는지에 따라 모의메일바이러스 훈련 결과값에 해당하는 정보보호수준과 상관관계가 있는지 분석하였다.

2012년 IT유관부서 정보보호 담당자의 업무비중과 메일 바이러스 훈련의 데이터 값을 분석한 결과는 다음과 같다.

		VAR00001	VAR00002
VAR00001	Pearson correlation coefficient	1	-.628*
	Significant probability (both sides)		.039
	N	11	11
VAR00002	Pearson correlation coefficient	-.628*	1
	Significant probability (both sides)	.039	
	N	11	11

*. The correlation coefficient is significant at the 0.05 level (both sides).

Fig.5. 2012 Coefficient of Correlation : IT-related to the security personnel of the specific gravity of security work and mock e-mail virus result

pearson 상관계수: -0.628 (상관계수는 높을수록 관련성이 높은 것으로 보면 되고, (-)의 경우는 반비례의 관계를 나타내었다.)

유의확률: 0.039 (유의확률은 0.5이하가 되어야 의미 있는 상관계수라고 볼 수 있다.)

2012년의 분석결과 IT유관부서 정보보호담당자의 보안업무 비중과 모의 메일바이러스 훈련 결과 값의 상관계수는 0.628으로 유의수준 0.039에서 연구가설은 지지된다. 즉, 정보보호 수준은 IT유관부서 정보보호담당자의 보안업무비중과 상관관계(-)가 있다고 할 수 있다.

2013년 IT유관부서 정보보호 담당자의 업무비중과 메일 바이러스 훈련의 데이터값을 분석한 결과는 다음과 같다.

		VAR00001	VAR00002
VAR00001	Pearson correlation coefficient	1	-.590*
	Significant probability (both sides)		.095
	N	9	9
VAR00002	Pearson correlation coefficient	-.590*	1
	Significant probability (both sides)	.095	
	N	9	9

Fig.6. 2013 Coefficient of Correlation : IT-related to the security personnel of the specific gravity of security work and mock e-mail virus result

pearson 상관계수: -0.590 (상관계수는 높을수록 관련성이 높은 것으로 보면 되고, (-)의 경우는 반비례의 관계를 나타내었다.)

유의확률: 0.095 (유의확률은 0.5이하가 되어야 의미 있는 상관계수라고 볼 수 있다.)

2013년의 분석결과 IT유관부서 정보보호담당자의 보안업무 비중과 모의 메일바이러스 훈련 결과 값의 상관계수는 0.590으로 유의수준 0.095에서 연구가설은 지지된다. 즉, 정보보호 수준은 IT유관부서 정보보호담당자의 보안업무비중과 상관관계(-)가 있다고 할 수 있다.

2014년 IT유관부서 정보보호 담당자의 업무비중은 대상 10개사 정보보호 담당자 업무비중이 모두 동일하게 100%로 산정되어 있어서 상관성을 비교하는 것이 무의미하다고 볼 수 있다.

Table 11. 2012-2014 Information security levels for IT related Dept. vs. Non-IT related Dept.

Year	IT related Dept.		Non-IT Dept.		IT vs. Non-IT
	Security Level (%)	Company Number	Security Level (%)	Company Number	
2012	2.3	11	4.3	14	**1.87**
2013	4.4	9	7.7	8	**1.75**
2014	15.0	10	36.9	5	**2.46**
Total	21.7		48.9		
Avg.	7.23		16.30		**2.25**

Table 10.에서 나타난 바와 같이, 연도별로 IT유관부서에 속한 정보보호 담당자의 보안수준 평균값이 Non-IT에 속한 정보보호 담당자의 보안수준 평균값보다 2배 차이가 나는 것을 알 수 있다. 이는 IT유관부서에 속한 정보보호 담당자가 있는 조직의 정보보호 수준이 2배나 높게 나타나는 것을 의미한다.

Fig.7., Fig.8.의 그래프에서 보는 바와 같이 IT유관부서의 정보보호 수준 값이 IT조직이 아닌 부서의 정보보호 수준 값보다 그래프가 낮게 분포되어 있다. 이는 IT유관부서의 정보보호 수준이 높다는 것을 의미한다.

세 번째로는 정보보호 담당자가 조직내 정보보호 전담부서에 속해 있는지 아니면 일반부서에 속해 있는지에 따라 정보보호 수준이 차이가 있는지를 연구하였다.

Table 12.에서 나타난 바와 같이, 정보보호 전담부서에 속해 있는 정보보호담당자 조직의 보안수준 평균값이 일반부서에 속한 정보보호 담당자의 보안수준 평균값보다 2배 차이가 나는 것을 알 수 있다. 이는 정보보호 전담부서에 속한 정보보호 담당자가 있는 조직의 보안 수준이 2배나 높게 나타나는 것을 의미한다.

Table 12. 2012-2014 Information security levels for Security Dept. vs. General Dept.

Year	Security Department		General Department		Security Dept. vs. General Dept.
	Security Level (%)	Company Number	Security Level (%)	Company Number	
2012	0.9	4	3.8	21	**4.22**
2013	3.7	4	6.9	13	**1.86**
2014	15.0	10	36.9	5	**2.46**
Total	19.6		47.6		
Avg.	6.53		15.87		**2.43**

Fig.9., Fig.10.의 그래프에서 보는 바와 같이 정보보호 전담부서의 정보보호 수준 값이 일반부서의 정보보호 수준 값보다 그래프가 낮게 분포되어 있다. 이는 정보보호 전담부서가 있는 조직이 정보보호 수준이 높다는 것을 의미한다.

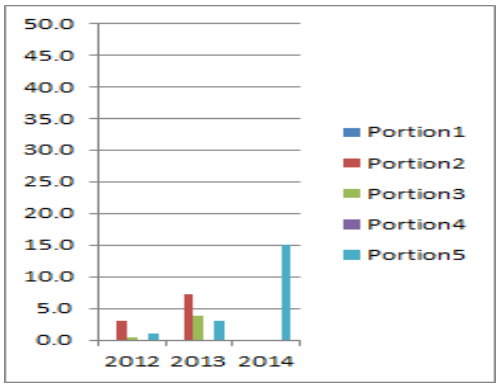


Fig.7. Year(2012-2014) IT related Dept. Security portion

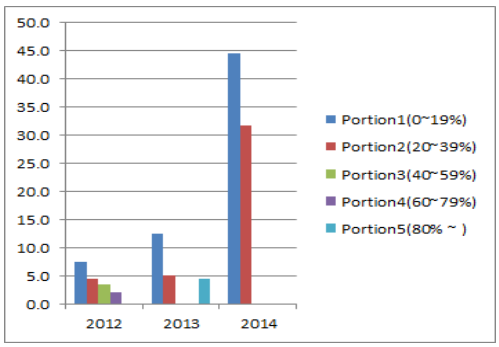


Fig.8. Year(2012-2014) Non-IT Dept. Security portion

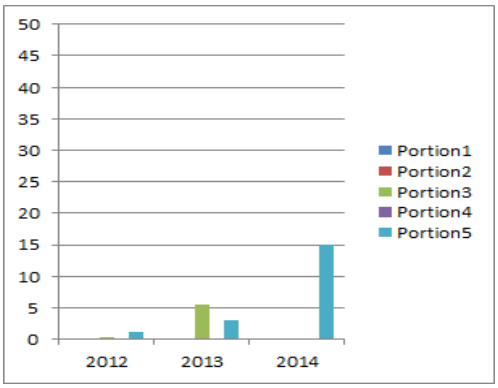


Fig.9. Year(2012-2014) Security Dept. security portion

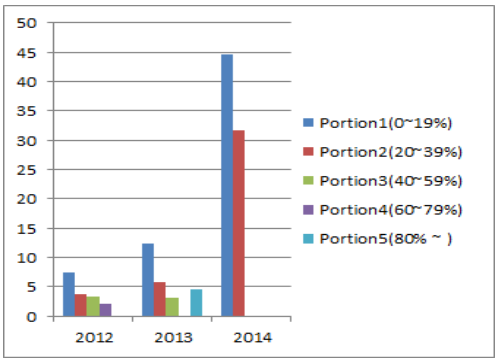


Fig.10. Year(2012-2014) General Dept. security portion

4.2 상관분석 모델

기업의 정보보호 담당자의 보안업무비중과 IT유관부서 보안담당자와의 정보보호 수준에 대한 일반적인 기준은 상관분석의 결과인 상관계수의 크기를 가중치로 사용하여 나타내면 Table 11.과 같다.

Model 1

$$Y = (0.613\ x1 + 0.519\ x2) / 2 + C$$

Y: 정보보호 수준
x1: 정보보호 전담업무 비중 (변수, 2012년)
x2: 정보보호 전담업무 비중 (변수, 2013년)
C: 상수

Model 2

$$Y = 0.882\ x3 + C$$

Y: 정보보호 수준
x3: 정보보호 전담업무 비중 (변수, 2014년)
C: 상수

기업내 각 부서의 정보보호 담당자가 보안전담 비중이 20%미만 일 때에는 2012년 및 2013년의 상관계수를 반영하는 것이 일반적이며(Model 1), 각 부서의 정보보호 담당자의 보안전담 비중이 75%를 넘으면 2014년 상관계수를 반영하는 것(Model 2.)이 일반적인 기준으로 사용될 수 있다.

이는 2012년 보안전담 비중이 80% 이상인 조직이 전체25개 기업중 3개 기업만 해당하므로 12%이고, 2013년은 전체 17개 기업중 4개 기업으로 18%로 나타나므로, 20%미만인 조직에서는 2012년, 2013년 상관계수를 사용하고, 2014년은 전체15개 기업중 10개 기업이 보안담당자의 보안전담 업무비중이 67%로 나타나므로 그 이상의 조직에서는 2014년 상관계수를 사용될 수 있다.

이상과 같이 정보보호 담당자의 보안업무 비중이 높을수록 해당 조직의 정보보호 수준이 높은 것을 상관관계를 통해서도 볼 수 있다.

3개년 데이터를 정보보호 담당자의 보안업무 비중과 메일 바이러스 모의훈련 데이터를 분석하여 상관성을 확인한 결과 유의미한 상관도를 찾을 수 있었으며, 이는 정보보호 담당자의 보안업무 비중이 높을수록 기업의 정보보호 수준이 높아진다는 것을 알 수 있게 되었다.

또한 보안전담 부서가 있는 경우의 정보보호 수준이 보안전담부서가 없는 경우와 비교할 때, 평균 2배 이상의 정보보호 수준이 차이가 나므로 기업의 정보보호 수준을 향상시키기 위해서는 보안전담부서를 두는 것이 필요하다. 상수 C 는 연도별 편차를 반영한 것이다.

$$Y1 \equiv 2.43\ ^{*}\ x1 + C$$

Y1: 정보보호 전담조직의 정보보호 수준
x1: 일반부서 조직의 정보보호 수준(변수)
C : 상수 (-1.8 〈 C 〈 0.6)

Table 13. Numbers of security staff for Security Job portion

	2012	2013	2014
Portion1(0~19%)	1	3	2
Portion2(20~39%)	16	7	3
Portion3(40~59%)	4	3	
Portion4(60~79%)	1		
Portion5(80% ~)	3	4	10

Table 14. Three Years(2012-2014) Information Security Level for Information Security Portion

Portion	2012	2013	2014
Portion1(0~19%)	7.5	12.4	44.6
Portion2(20~39%)	3.8	5.8	31.7
Portion3(40~59%)	2.7	3.9	
Portion4(60~79%)	2.0		
Portion5(80% ~)	1.1	3.4	15.0

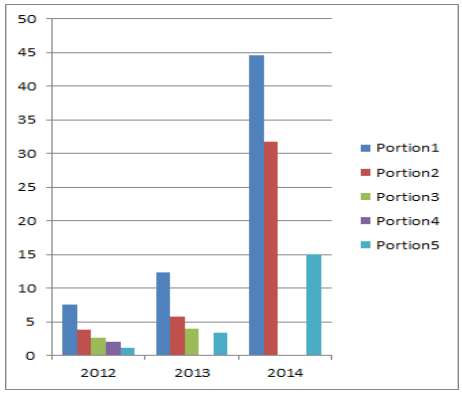


Fig.11. Year-mail virus-specific simulation training results

그리고 IT나 보안과 연관 있는 부서의 정보보호담당자가 있는 조직의 정보보호 수준이 일반부서에 속한 정보보호담당자가 있는 조직의 정보보호 수준보다 약 2배 가량 높게 나타났다. 상수 C 는 연도별 편차를 반영한 것이다.

$$Y2 = 2.25 * x2 + C$$

Y2: IT 및 보안이 주 업무인 보안담당자가 속한 조직의 정보보호 수준
x2: IT&보안 유관조직 정보보호 수준(변수)
C: 상수 (-0.2 〈 C 〈 0.5)

따라서 정보보호 수준을 향상시키기 위해서는 정보보호 전담조직을 갖추고, IT 또는 정보보호 경험이나 스킬이 있는 정보보호 담당자를 전담보안인력으로 활용하는 것이 매우 큰 영향을 끼칠 수 있을 것으로 나타났다.

V. 결 론

5.1 결론

본 연구를 통하여, 정보보호 담당자의 보안업무 비중이 높은 조직이 보안업무 비중이 낮은 조직보다 정보보호 수준이 높다는 것을 분석을 통하여 밝혔다. 이는 정보보호 담당자의 보안업무 비중이 높을수록 정보보호 수준이 높게 나타났으며, 특히, 보안업무를 전담으로 하는 정보보호 담당자의 경우 매우 높은 정보보호 수준을 나타내는 것으로 분석되어 향후 정보보호 조직구성 및 운영관리에 좋은 연구 자료로 활용될 수 있으리라 기대한다.

따라서 조직 내 정보보호 수준을 향상하기 위해서는 기업이나 조직은 정보보호 담당자를 임명하고 보안업무 비중이 80%이상 높게 업무를 부여하거나 보안업무를 전담하게 하여 정보보호 활동을 수행하도록 하여야 한다. 또한 정보보호 전담부서를 두거나 정보보호 담당자를 IT유관부서에서 활용하도록 역할과 책임을 부여함으로써, 조직의 정보보호 수준을 극대화 할 수 있을 것이다. 이는 보안 전담부서가 없거나, IT와 관련 없는 부서에서 정보보호 담당자 역할을 수행하는 경우보다 두 배의 정보보호 수준을 높일 수 있다고 분석되었기 때문이다.

결론적으로 조직이나 기업의 정보보호 수준을 높이는 활동으로 정보보호 담당자의 역할은 매우 중요하고 크다고 할 수 있으며, 이를 위해 정보보호 전담조직 및 정보보호 전담 인력을 배정하는 것이 조직의 정보보호수준을 향상시키는 가장 중요한 요인들 중 하나라는 사실을 깊이 인지하여야 한다. 마치 기업이 직원의 복리후생 차원에서 식당을 운영할 때, 임직원의 인원수에 비례하여 영양사를 두는 것과 마찬가지로, 임직원의 인원수나 보유한 개인정보 회원수 및 운영하는 일일 처리 개인정보 건수 등에 비례하여 정보보호 전담인력을 배정하는 매우 중요한 일이라 하겠다. 그러므로 기업의 정보보호 수준이 향상될 수 있도록 보안전담 조직 및 전담 보안인력을 운영하여야 한다.

법.제도적인 측면에서도 기업이나 산하 기관들이 정보보호 조직을 현실성 있게 구성하도록 정부 및 상급기관들도 정보보호 전담조직이나 보안전담 인력이 현장에 배치될 수 있도록 법.제도를 개선함으로써, 정보보호 활동이 지속적으로 발전될 수 있도록 지원하여야 한다. 정부 및 공공기관의 정보보호 전담조직과 정보보호 실무담당자가 보안업무만 전담할 수 있도록 제도가 개선되어야 하며, 일반 기업들도 정보보호 문제를 제기만 하지 말고, 정보보호 전담조직 및 정보보호 전담인력이 조직내 양성되고 배치될 수 있도록 시급히 개선되어야 한다. 나아가 영양사 제도처럼 의무화되는 것이 바람직하다.

5.2 한계 및 향후 발전방향

본 연구에서 제시한 정보보호 수준 데이터는 협의의 범주에서 수집한 데이터라 할 수 있다. 정보보호 활동이 다양하고 여러 계층의 직원들에서 보안평가에 대한 결과 값이 나타나므로 보다 폭 넓게 데이터를 수집하여 비교 평가하는 것이 필요하다. 즉 다양한 방법으로 정보보호 수준을 수치화하고 계량화하는 것이 필요하다. 또한 정보보호 전담자의 근속년수와 정보보호 수준과의 상관성 분석도 병행하여 분석하는 것도 매우 의미 있는 결과를 도출할 수 있을 것이다.

또 다른 입장에서, 기업의 산업군별 정보보호 수준을 분석하는 것도 향후 발전방향으로 매우 중요한 의미가 있을 것이다.

References

〔1〕 SangSoo Jang, BongNam Noh, and SangJoon Lee, "The Effects of the Operation of an Information Security Management System on the Performance of Information Security" Journal of Korean Institute of information scientists and engineers, IT-40(1), pp. 58-69, Feb. 2013.

〔2〕 ConCERT," FORECAST 2014 Enterprise information security issues prospect," Dec. 2014.

〔3〕 Tae-Sung Kim, and kihwan Kim, "Analysis on a Turnover Process of Information Security Professionals," Journal of the Korea Institute of Information Security and Cryptology, 21(6). Dec. 2011.

〔4〕 Kim, Ji-Soo, Kim, Jong-Bae, and Shin, Yongtae, "A Study on the Effect of CISO's Recognition of the Role to the Information Security Performance," The Korean Society of Management Consulting, 12(4). pp. 21-34, Dec. 2012.

〔5〕 KISIA, "Survey for Information Security Industry in Korea : Year 2013," Dec. 2013.

〔6〕 sang-hyun, Shim, "A Syudy on Personal Information Protection Knowledge Level System," KISA-WP-2013-0027, Korea CPO Forum, Dec. 2013.

〔7〕 Tae-Sung Kim, "A Study on Mid- and Long-term Forecast for Demand for and Supply of Manpower in Knowledge Information Security Sector," KISA-WP-2010-0034, KIISC, Oct. 2010.

〔8〕 "Currently, the biggest security threat is who?" Boannews, Oct. 14. 2014.

〔9〕 "More than half the company's employees are willing to violate policy, BYOD." Boannews, Oct. 31. 2013.

〔10〕 1 ranking security staff complaints, "I can not wait no manpower," Boannews, July. 21. 2014.

〔11〕 Electronic Times Internet. http://www.etnews.com/201402020138 , Feb. 2. 2014.

〈저자소개〉

최 동 근(Dong-Keun Choi) 일반회원
1987년 2월: 경북대학교 통계학과 이학사
2011년 9월~현재: 고려대 정보보호대학원 석사과정
1988년 8월~2014년 3월: LGCNS, 시큐어소프트, 이니텍, 롯데정보통신 등 근무
2014년 3월~현재: 롯데카드 CISO
〈관심분야〉 정보보호 컨설팅, 개인정보보호 정책, 융합보안

송 미 선(Mi-sun Song) 학생회원
2010년 2월: 서울여자대학교 정보보호학과 학사
2009년 11월~2012년 12월: NHN NTS/I&S 서비스보안팀 근무
2013년 9월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 정보보호 관리체계, 개인정보보호 및 정보보호 정책

임 종 인 (Jong In Im) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월:고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
현재: 고려대학교 정보보호대학원 원장, 고려대학교 사이버국방학과 교수,
개인정보보호 위원회 위원, 대검찰청 디지털수사자문위원회 위원장,
금융보안 연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원,
국방부 정보화책임관 자문위원, 한국저작권위원회 위원 등
〈관심분야〉 사이버 국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등

이 경 호(Kyung-Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사 졸업
2009년 8월: 고려대학교 정보경여대학원 박사 졸업
1994년 2월~현재: 삼성그룹, nhn, 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 위험관리, 정보보호 컨설팅, 정보보호 및 개인정보보호 정책