디지털산업정보학회 논문지 제10권 제4호-2014년 12월

인적 및 직무특성과 보안교육 이수율 및 사이버테러 대응과의 연관성 분석*

신 현 조** · 이 경 복*** · 박 태 형***

Association Analysis on The Completion Rate of Security education and Cyber Terror Response According to Personal and Job characteristics

Shin, Hyun Jo · Lee, Kyung Bok · Park, Tae Hyoung

〈Abstract〉

The development of ICT has led positive aspects such as popularization of Internet. It, on the other hand, is causing a negative aspect, Cyber Terror. Although the causes for recent and continuous increase of cyber security incidents are various such as lack of technical and institutional security measure, the main cause which threatens the cyber security is the users' lack of awareness and attitude. The purpose of this study is the positive analysis of how the personal and job characteristics influence the cyber security training participation rate and the response ability to cyber terror response training with a sample case of K-corporation employees. In this paper, the relationship among career, gender, department, whether he/she is a cyber security specialist, whether he/she is a regular employee), "ratio of cyber security training courses during recent three years", "ratio that he/she has opened the malicious email in cyber terror response training during recent three years", "response index of virus active-x installation (higher index means poorer response)" is closely examined. Moreover, based on the examination result, the practical and political implications regarding K-corporation's cyber security courses and cyber terror response training are studied.

Key Words : Personal Characteristics, Job Characteristics, Cyber Security, Security Training, Cyber Terror

Ⅰ. 서론

정보통신기술의 발달은 인터넷의 대중화 등 긍정적 측면이 있는 반면, 사이버테러라는 부정적 측면도 야기하고 있다. 국내 사이버 공간상에서 발생한 범죄는 2011년 기준으로 약 91,496건이 발생하였는데, 2004년 63,384건에 비해 무려 69% 이상 증가한 수치이다[1]. 이러한 사이버보안사고가 지속적으로 늘어나는 이유는 기술적 보안장치의 미흡, 제도적 장치의 미흡 등과 같이 매우 다양할 수 있다. 그러나 사이버

*본 논문은 미래창조과학부 및 정보통신산업진흥원의 '지식정보보안인력양성 최고정보보안전문가과정' 사업의 연구결과로 수행되었음(과제번호: NIPA-H2102-13-1002)

** 한국전력공사
*** 고려대학교 정보보호대학원

공간에서의 보안에 대한 사용자의 인식과 태도가 사이버보안을 위협하는 가장 큰 핵심요인으로 작용할 수 있다고 한다[2]. 이는 사이버보안의 주체는 사람이기 때문이며 사람에 대한 보안교육이 중장기적으로 사이버위협과 사이버테러를 예방하는데 가장 중요한 대책 중에 하나임을 강조한 것이라 할 수 있다. 본 연구는 18, 119명의 K공사 전 직원을 대상으로 인적 및 직무특성, 최근 3년간 사이버보안교육 이수율, 최근 3년간 사이버테러 대응훈련 대응과의 관계를 실증적으로 규명하고자 구체적인 표본, 측정, 모형, 가설 등을 제시하고 통계분석을 시행하였다. 연구시료인 18, 119명의 교육자료와 훈련자료를 SPSS v21.0 통계프로그램과 Excel 2010을 이용하여 양적인 통계자료 처리방법에 의해 분석하였다. 세부 통계분석 방법으로 빈도분석, 다중회귀분석 등을 활용하였다. 이를 통해 다양한 인적 및 직무특성에 따라 교육 이수율에 어떠한 차이를 보이는지, 나아가 사이버테러 대응훈련의 대응행태는 어떻게 달라지는지를 실증적으로 규명함으로써 향후 보안교육의 개선방안을 제시하고자 한다.

Ⅱ. 관련연구

2.1 사이버보안과 보안교육의 개념

2.1.1. 사이버보안

일반적인 보안의 사전적 의미로는 “위험, 손실 및 범죄가 발생하지 않도록 방지하는 상태”를 의미하며, 피해발생의 원인이 ‘인간의 행위’라는 점에서 안전이라는 개념과 구분된다[3].

그러나 시대가 변화함에 따라 보안은 기존의 물리적 보안에서 최근 사이버 보안으로 무게 중심축이 이동하고 있다. 사이버 보안의 대상은 사이버 공간에서의 하드웨어 및 소프트웨어 요소뿐만 아니라 사이버 공간에서 저장된 데이터 요소 및 이를 이용하는 개인의 행태적인 요소 등을 모두 포함한다.

따라서 사이버 보안은“사이버 공간에서의 위협으로부터 정보인프라, 정보사용자 및 컨텐츠를 보호”하는 것으로 정의할 수 있다. 이 개념 속에는 기술적 요소(컴퓨터, 인터넷, 네트워크, 인프라요소), 사람요소(조직내부 및 인터넷이용자), 컨텐츠요소(데이터, 정보 및 언어), 문화요소(온라인 및 오프라인에서의 인터넷 사용에 따른 전반적인 분위기와 인식체계) 및 이들 요소가 통합하여 나타나는 파급효과 요소 등이 포함된다[2].

2.1.2. 사이버 위협

시만텍은 ‘2010년 기업 보안현황 보고서’에서 2009년 1년간 75%의 기업이 사이버 공격을 받았으며 이에 따른 손실 규모가 연평균 2백만 달러를 기록하는 등 기업을 포함한 모든 기관을 대상으로 사이버 공격 위협이 심화되고 있다고 발표하였다[4].

요즘은 기업뿐만 아니라 개인들도 일상의 많은 부분을 컴퓨터와 인터넷에 의존하고 있기 때문에 사이버 공격 위협에 노출되어 있다.

<표 1>은 컴퓨터 사용과 관련된 사이버 위협의 종류를 제시한 것이다. 여러 학자들은 특정 사이버 위협이 개인 또는 기업의 자산에 얼마나 발생확률이 높

<표 1> 사이버 위협의 종류

학자	사이버 위협
B. Howard et al(2001)	해킹, 바이러스·웜, 서비스거부공격, 도청, 능동공격, 스푸핑, 이플라이공격, 패킷공격, 사회공학
SANS Institute(2007)	바이러스, 웜, 트로이목마, 스파이웨어, 애드웨어
Sophos(2008)	멀웨어, 스팸, 악성메일, 웹침투
Lee & Chiang(2010)	Botnet

은가, 그리고 위협이 실제 발생하였을 경우 얼마나 큰 피해를 유발시킬 것인가를 파악하여 적정한 보호 조치를 취하는 것이 중요하다고 강조하고 있다.

2.1.3. 보안교육

보안교육은 기본적으로 정보보호에서 추구하는 3가지 개념인 기밀성, 무결성, 가용성 등의 개념을 바탕으로 해서 발생 가능한 위험을 사전에 방지하는 것을 목적으로 한다. 일반적으로 정보보호의 위험요인은 기밀성이 침해되는 정보의 비인가 공개, 무결성이 침해되는 정보의 불법적인 변조 및 파괴, 가용성이 침해되는 정보서비스 이용불가 등이 대표적이다. 이러한 위험 요인들을 교육을 통해 예방하는 것이 보안교육의 최종 목표하고 정의할 수 있다[17-19].

보안교육의 중요성은 여러 선행연구에서 찾아볼 수 있는데, 보안에 대한 인식의 향상이 보안행동에 영향을 주게 되며 직원의 행동수준이 높아지면 그에 따라 정보보안 성과가 향상된다는 것이다[5].

그래서 많은 기업들이 기업의 정보자원을 보호하기 위해 정보보호 기술에 투자를 진행하고 있는 만큼 조직 구성원이 정보보호의 개념에 대해 인지하도록 하는 것도 중요하다. 즉 정보보호가 효과적으로 이루어지기 위해서는 기업내의 구성원들이 정보보호 중요성에 대한 인식을 함과 동시에 기업의 특성에 적합한 보안교육 및 훈련이 뒷받침되어야 한다.

2.2 보안교육의 원인과 결과(효과)

2.2.1. 보안교육의 다양한 원인

보안교육 프로그램이 유효하기 위해서는 영향을 미치는 여러 요인들을 고려해야 한다. 초기 연구에는 교육프로그램의 설계, 개발 및 운영에 주로 초점을 맞추었다면 1980년 후반부터 교육훈련 프로그램 특성 외에 교육참가자의 태도, 가치, 기대 등과 같은 개인적 특성과 그 참가자가 속해 있는 작업환경 등 상황적 특성이 교육 유효성에 미치는 영향 등을 파악하기 위해 많은 연구들이 꾸준히 이루어져 왔다[6-7].

본 연구에서도 교육 프로그램 효과에 영향을 미치는 여러 요인 가운데, 보안 교육을 받은 직원들이 보안교육에서 학습한 지식, 기술 등을 자신의 업무에 적용하고 활용하는 과정에 영향을 미치는 교육 참여자 개인의 인적 및 직무특성에 보다 주목하고자 한다.

2.2.2. 보안교육 효과

교육의 효과는 궁극적으로 교육이 성과에 기여하였는가와 관련된 개념으로서 프로그램이 잘 수행되었는가를 살펴보는 것뿐만 아니라 실제적인 직원들의 능력 향상을 가져옴으로써 조직이 지원할 만한 가치가 있는가와 같은 근본적 문제를 다루는 것이다[8, 17-19].

그러므로 조직에서 이루어지는 훈련이나 교육이 직원들에게 기대되는 직무수행과 직접적인 관련이 있다는 것을 확인해야 하며 그러한 직무수행이 조직의 경영목표를 달성하는데 기여한다는 점을 증명해야만 한다[9, 17-19].

앞에서 언급했던 보안교육을 통해 기대하는 것은 결국 정보보안 측면에서 성과를 거두는 것이라고 할 수 있다.

2.3 선행연구와의 차별성

앞서 논의한 보안교육의 원인과 결과(효과)에 보다 직접적으로 관련된 선행연구는 <표 2>와 같이 분석대상과 표본, 연구주제, 연구 주요내용 등의 측면으로 요약할 수 있다.

<표 2> 주요 선행연구 검토결과([10~16])

저자 (연도)	분석대상과 표본	주제	주요 연구결과
백민정 · 손승희 (2011)	1000명이하 중소규모 기업 설문 152부	중소규모 조직구성원의 정보보안 인식과 행동이 정보보안성과에 미치는 영향에 관한 연구	조직구성원의 정보보안인식이 정보보안행동과 조직의 정보보안사고 빈도감소 및 사고손실 감소에 영향을 미침
홍기향 (2003)	국내 300여 기업 80부	정보보호 통제와 활동이 정보보호 성과에 미치는 영향에 관한 연구	정보보호 통제와 활동은 정보보호 성과에 영향을 미치나 활동이 통제보다는 직접적인 영향을 미침
김종기 · 강다연 (2008)	경영대학원생 168부	보안정책, 보안의식, 개인적 특성이 패스워드 보안효과에 미치는 영향	정보시스템 사용자의 패스워드 사용이 보안효과에 영향을 미치는 요인으로 보안정책, 보안의식, 개인적 특성이 모두 통계적으로 유의한 영향을 미치는 것으로 나타남
김경규 · 신호경 (2009)	매출액 기준 100대 기업 및 기관 중 50여개 기업 및 기관 31부	정보자산보호 성과가 조직성과에 미치는 영향에 관한 연구	정보자산보호 성과를 위해서는 강제적이고 단편적인 통제 중심의 활동보다는 체계적인 관리적, 정책적 활동과 이에 따른 조직구성, 구성원의 정보보호에 대한 인식변화가 긍정적인 영향을 미침
정구헌 (2010)	정부, 공공기관, 민간기업 종사자 210부	정보보호 아키텍처 구성과 보안활동이 정보자산보호 및 조직성과에 미치는 영향	분류식별과 위험분석 관리요인이 내부정보 유출 방지를 위한 정보보호 통제활동에 유용성을 가짐
백민정 · 손승희 (2010)	공기업, 사기업 설문 280부	조직의 정보윤리실천이 구성원의 정보보안 인식과 행동에 미치는 영향에 관한 연구	정보윤리정책, CEO의 정보윤리실천의지, 동료의 정보보안행동이 정보보안인식에 영향을 미치며, 정보처리관련자와 비관련자 사이의 행동에 차이가 있어, 정보보안관련 지식의 차이에 따른 차별화된 교육이 필요
김영곤 (2010),	정보보안시스템을 판매, 설치한 기관 설문 375부	정보보안 거버넌스의 구성요소가 종업원의 보안의식과 행위에 미치는 영향에 관한 연구	구성원의 보안의식과 행위는 경영진의 리더십과 IT거버넌스의 적용에 강한 영향을 받으며, 사용자의 보안관리를 위해 구체적인 실행계획(교육, 훈련, 홍보 등)이 필요.
최응렬 · 이영일 · 송봉규 (2011)	국가핵심기술대상기관 50개	국가핵심기술 보호수준과 보안요인과의 관계연구	성과금 지급 등의 성과관리는 국가핵심기술 보호수준에 무의미한 영향을 미침

<표 2>와 같이 많은 연구에서 보안인식이나 교육이 개인의 수준에 따라 차이가 있을 수 있으며 이러한 차이에 따라 효과에도 차이가 있을 수 있음을 강조하고 있다는 점은 본 연구와 유사한 경향을 보인다. 그러나, 분석표본이 일반기업 대상으로 극히 일부 직원에 의한 주관적인 설문조사에 한정되어 있다는 점에서 극명한 차이를 보인다.

따라서 본 연구는 다음과 같은 차별성을 가진다.

첫째, 사이버 보안이 민간부분과 정부부문에 관심을 두고 다양한 조직과 개인을 대상으로 연구를 진행해 왔으나 본 연구와 같이 공공기관 중 공기업을 대상으로 한 연구는 드물다는 점에서 의의를 가진다.

둘째, 본 연구는 K공사 전 직원을 모집단으로 거의 전수조사에 가까운 18, 119명을 대상으로 한다는 점에서 기존 연구의 제약된 일부 표본의 한계를 최소화하고 빅데이터에 의한 연구결과를 제공한다는 점에 의의가 있다.

Ⅲ. 분석 방법론

3.1 연구설계

3.1.1. 측정 및 조작화

연구설계에 있어서 측정은 중요하며 측정이 올바르지 못할 경우 연구결과의 타당성에 문제가 발생할 수 있음을 강조하고 있다. 이에 본 연구에서는 이론적 논의 및 선행연구 검토를 바탕으로, K공사 내부직원을 대상으로 다음과 같이 독립변수, 매개변수, 종속변수를 설정하고 이를 측정을 하였다. 구체적인 사항은 <표 3>과 같이 요약된다.

3.1.2. 분석모형과 가설

본 연구에서는 다양한 인적 및 직무특성이 사이버 보안교육 이수율을 비롯하여, 사이버테러훈련 대응에

<표 3> 측정도구

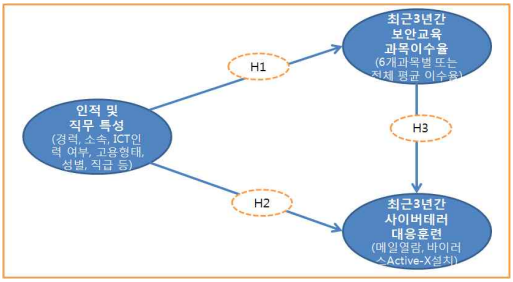
구분	변수명	구분
독립변수 : 인적 및 직무특성	경력	사번으로 경력 산출
	소속	본사, 운영사업소, 건설사업소
	성별	남자, 여자
	ICT인력(정보보호전담) 여부	정보보호 전담 직무 여부
	채용구분	정규직, 비정규직
	직급	간부급(1-3급), 직원급(4급 이상)
매개변수 : 최근3년간 보안교육 이수율	과목1(패스워드 보안)	6과목 평균한 경우와 6개 과목별로 나누어 분석(0-100)
	과목2(DDoS와 좀비PC)	
	과목3(스마트폰 보안위협)	
	과목4(안전한 이메일 사용법)	
	과목5(악성코드 종류 및 감염경로)	
	과목6(안전한 스마트폰 사용)	
	6개 과목 평균이수율	
종속변수 : 최근 3년간 사이버테러 대응훈련 대응	메일열람	2012년부터-2014년 상반기 및 하반기의 정보를 최근 3년간으로 종합 수치로 변환(0-5) (해당 수치가 높을수록 사이버 테러대응훈련 정도가 낮음을 의미하는 역척도)
	바이러스Active-x 설치	

미치는 효과를 검증하는데 초점을 둔다. 즉, <그림 1>과 같이 분석모형을 도식화하였다.

<그림 1>을 토대로 다음과 같이 3가지의 연구가설을 설정한다.

(H1) 다양한 인적 및 직무특성에 따라서 최근 3년간 사이버 보안교육 이수율에 차이가 있을 것이다.

(H2) 다양한 인적 및 직무특성에 따라서 최근 3년간 사이버 테러 대응훈련의 대응정도(메일열람, 바이러스 Active-x설치)에 차이가 있을 것이다.



<그림 1> 분석모형

(H3) 최근 3년간 사이버 보안교육 이수율에 따라서 최근 3년간 사이버 테러 대응훈련의 대응정도(메일열람, 바이러스 Active-x설치)에 차이가 있을 것이다.

3.2 분석방법

본 연구의 연구모형을 바탕으로 가설을 실증적으로 규명하기 위해서 분석자료에 대한 데이터 마이닝을 거친 후, SPSS(Statistical Packages for Social System) 21.0 통계 패키지와 엑셀(Excel) 2010을 이용하여 분석하였다. 그리고, 인적 및 직무특성 변수에 대한 현황을 빈도분석(Frequency Analysis), 기술통계(Descriptive Stat-istics)를 통해 파악하였다. 더불어, 인과관계(causal relationship)를 규명하기 위해 다중회귀분석(multiple regression analysis)을 다양하게 실시하여 주요 가설을 검증하고 주요 분석결과를 해석하고자 한다.

Ⅳ. 분석결과

4.1 표본현황

K공사 내부직원 가운데 최근 3년 이상 보안교육을

이수하고 최근 3년 이상 사이버테러 대응훈련을 받은 직원을 선별하고 최종적으로 분석에 활용된 표본은 18, 119명으로 분석대상의 주요현황을 살펴보면 다음의 <표 4> 와 같이 요약할 수 있다

<표 4> 표본 현황

구분		빈도(명)	비율(%)
경력 수준	10년 미만	2,237	12.35
	10년이상-20년미만	5,395	29.78
	20년이상-30년미만	5,805	32.04
	30년이상	4,682	25.84
소속	본사	2,742	15.13
	운영사업소	14,551	80.31
	건설사업소	826	4.56
성별	여자	2,879	15.89
	남자	15,240	84.11
ICT 인력 여부	그외	17,501	96.59
	ICT인력(정보보호 전담)	618	3.41
채용형태	비정규직	38	0.21
	정규직	18,081	99.79
직급	직원급(4급이상)	13,022	71.87
	간부급(1-3급)	5,097	28.13
합계		18,119	100.00

4.2 다중회귀분석 결과

각 변수간의 인과관계를 규명하기 위해서 다중회귀분석을 실시하였으며, 이를 통해서 변수간의 구체적인 관계를 보다 엄격한 조건에서 파악할 수 있다.

4.2.1 인적 및 직무특성에 따른 최근 3년간 보안교육 이수율에 대한 다중회귀분석결과

<표 5>의 분석결과에서 R제곱(설명력 또는 결정계수)은 0.35로 분석에 포함된 인적 및 직무특성과 관련된 독립변수에 의해서 종속변수가 설명되어지는 정도가 약 35% 정도로 임을 의미한다. 또한 모든 변수들이 ***p<0.01, **p<0.05, *p<0.1에서 통계적으로 유의미한 것으로 나타났으며, 경력이 높을수록, 본사가 아닌 사업소에 해당될수록, 여자보다 남자일수록, ICT인력에 해당될수록, 정규직에 해당될수록, 간부급보다는 직원급에 해당될 수록 사이버 보안교육의 최근 3년간 평균 이수율이 높아지는 것으로 나타났다.

<표 5> 인적 및 직무특성에 따른 최근 3년간 보안교육 이수율(6개 과목 평균)에 대한 다중회귀분석결과

구분	종속변수: 최근 3년간 보안교육 이수율_평균이수율		
	비표준 계수	표준 계수	유의 확률
	B	베타	
(상수)	61.98		0.00
경력년수	0.03	0.02	0.02
소속더미1(본사=1,그외=0)	-24.67	-0.44	0.00
소속더미2(운영사업소=1, 그외=0)	3.55	0.07	0.00
성별(남자=1, 여자=0)	5.33	0.10	0.00
ICT인력(정보보호전담)=1, 그외=0	1.21	0.01	0.07
채용구분(정규직=1, 비정규직=0)	26.76	0.06	0.00
1=간부급(1-3급), 0=직원급(4급이상)	-6.58	-0.15	0.00
R제곱	0.35		
수정된 R제곱	0.35		
F값	1373.41		
표본수	18,119		

주) ***p<0.01, **p<0.05, *p<0.1에서 통계적으로 유의미한 것으로 나타남

4.2.2 인적 및 직무특성과 최근 3년간 보안교육 이수율에 따른 사이버테러 대응훈련에 대한 다중회귀분석결과

<표 6>은 인적 및 직무특성을 고려한 상태에서 최근 3년간 보안교육 이수율(%)이 사이버테러 대응훈

<표 6> 인적 및 직무특성과 최근 3년간 보안교육 이수율(6개 과목 평균)에 따른 사이버테러 대응훈련에 대한 다중회귀분석결과

구분	종속변수: 사이버테러 대응훈련_메일열람_합계			종속변수: 사이버테러 대응훈련_바이러스Active-x설치_합계		
	비표준계수	표준계수	유의확률	비표준계수	표준계수	유의확률
	B	베타		B	베타	
(상수)	0.77		0.00	0.30		0.00
경력년수	0.01	0.09	0.00	0.01	0.14	0.00
소속더미1(본사=1, 그외=0)	0.69	0.27	0.00	0.16	0.12	0.00
소속더미2(운영사업소=1, 그외=0)	0.09	0.04	0.00	0.05	0.04	0.00
성별(남자=1,여자=0)	0.32	0.13	0.00	0.11	0.08	0.00
ICT인력(정보보호전담)=1, 그외=0	-0.27	-0.05	0.00	-0.09	-0.03	0.00
채용구분(정규직=1, 비정규직=0)	0.01	0.00	0.96	-0.04	0.00	0.62
1=간부급(1-3급), 0=직원급(4급이상)	0.05	0.03	0.00	0.03	0.03	0.00
최근 3년간 보안교육 이수율_6개과목 평균	-0.01	-0.18	0.00	0.00	-0.17	0.00
R제곱	0.15			0.07		
수정된 R제곱	0.15			0.07		
F값	395.39			170.79		
표본수	18,119			18,119		

주) ***p<0.01, **p<0.05, *p<0.1에서 통계적으로 유의미한 것으로 나타남

련 대응에 미치는 효과를 보여주며, 종속변수가 메일열람인가 바이러스Active-x 설치인가에 따라서 모형1과 모형2로 나누어 분석한 것이다.

모형1과 모형2에서 핵심이 되는 최근 3년간 보안교육 이수율(6개 과목 평균)은 사이버테러대응훈련을 대리하는 메일열람(-0.01), 바이러스Active-x 설치(-0.17)에 (-)의 영향을 미치고 있으며, 이는 ***p<0.01, **p<0.05, *p<0.1에서 통계적으로 유의미한 것으로 나타났다.

종속변수인 사이버테러 대응훈련이 해당 수치가 높을수록 대응 정도가 낮음을 의미하는 역척도임을 고려할 때, 이러한 결과가 의미하는 것은 보안교육 이수율이 높을수록 대체로 사이버테러대응훈련에 효과가 있음을 나타나는 것으로 해석할 수 있다.

그 외에 인적 및 직무특성에 해당되는 변수 중에서 채용구분을 제외한 나머지 변수들은 ***p<0.01, **p<0.05, *p<0.1에서 통계적으로 유의미한 것으로 나타났다. 즉, 경력년수가 높을수록, 본사에 해당될수록, 남자일수록, ICT인력에 해당되지 않을수록, 간부급에 해당될수록 종속변수인 메일열람과 바이러스Active-x 설치는 높아지는 것으로 나타나, 대체로 사이버테러 대응훈련 정도가 떨어지는 것으로 해석할 수 있다.

Ⅴ. 결론 및 논의

5.1 분석결과 종합

최근 사이버 보안사고가 지속적으로 늘어나고 있으며, 관련된 연구가 지속적으로 증가하는 추세이나 본 연구와 같이 공기업의 빅데이터(Big Data)를 중심으로 다양한 개인수준의 특성과 보안교육 이수율, 사이버테러 대응훈련 등의 관계를 심층적으로 분석한 연구는 거의 없었다.

이에 본 연구에서는 인적 및 직무특성이 사이버 보안교육 이수율 및 사이버 테러 대응훈련 대응에 미치는 영향력을 K공사 직원을 중심으로 실증적으로 분석하고, 이를 통해 다음과 같은 주요 연구결과를 도출하였다.

첫째, 경력, 소속, 성별, ICT전문인력여부, 정규직여부, 직급 등의 인적 및 직무특성에 따라서 "최근 3년간 보안교육 과목 이수율(%)"에 차이가 존재하는 것으로 분석되었다. 특히, 표본들의 경력이 높을수록,

본사보다 사업소에 해당될수록, 여자보다 남자일수록, ICT전문인력에 해당될수록, 정규직에 해당될수록, 직급이 낮을수록 “최근 3년간 보안교육 과목 이수율(%)”이 상대적으로 높은 것으로 분석되었다. 이에 따라서 본 연구에서 설정한 가설1은 대체로 채택 가능한 것으로 판단된다.

H1) 다양한 인적 및 직무특성에 따라서 최근 3년간 사이버 보안교육 이수율에 차이가 있을 것이다.
⇒ 채택

둘째, 경력, 소속, 성별, ICT전문인력여부, 정규직여부, 직급 등의 인적 및 직무특성에 띠라서 “최근 3년간 사이버테러 대응훈련 대응지수(메일열람, 바이러스Active-x설치)”가 달라지는 것으로 분석되었으며, 대체로 경력이 낮을수록, 본사보다 사업소에 해당될수록, 남자보다 여자일수록, ICT전문인력에 해당될수록, 정규직에 해당될수록, 직급이 낮을수록 “최근 3년간 사이버테러 대응훈련”에 잘 대응하는 것으로 분석되었다. 이에 따라서 본 연구에서 설정한 가설2는 대체로 채택 가능한 것으로 판단된다.

H2) 다양한 인적 및 직무특성에 따라서 최근 3년간 사이버 테러 대응훈련의 대응정도(메일열람, 바이러스Active-x 설치)에 차이가 있을 것이다.
⇒ 채택

셋째, “최근 3년간 사이버 보안교육 과목 이수율(%)”이 높을수록 “최근 3년간 사이버테러 대응훈련 대응(메일열람, 바이러스Active-x설치)”에 긍정적인 영향을 미치는 것으로 분석되었다. 즉, 보안교육 과목 이수율이 높을수록 메일열람, 바이러스Active-x설치에 대한 대응이 낮아져 긍정적인 효과를 유발하는 것으로 분석되었다. 이에 따라서 본 연구에서 설정한 가설3은 채택 가능한 것으로 판단된다.

H3) 최근 3년간 사이버 보안교육 이수율에 따라서 최근 3년간 사이버 테러 대응훈련의 대응정도(메일열람, 바이러스Active-x 설치)에 차이가 있을 것이다.
⇒ 채택

이상의 3가지 가설을 독립변수(인적특성 및 직무특성), 매개변수(보안교육 이수율), 종속변수(사이버테러 대응훈련대응)의 세부 변수별로 나누어 분석결과를 종합한 결과는 <표 7>과 같이 구체화할 수 있다.

<표 7> 분석결과 종합

가설	독립변수 (인적특성 및 직무특성)	매개변수 (보안교육이수율)	종속변수 (사이버테러 대응훈련대응)
H1 및 H2	경력수준이 높을수록	이수율은 높으나	대응정도는 낮다
	본사가 사업소에 비해서	이수율도 낮고	대응정도도 낮다
	남자가 여자에 비해서	이수율은 높으나	대응정도는 낮다
	ICT정보보호인력이 그외 직무에 비해서	이수율도 높고	대응정도도 높다
	정규직이 비정규직에 비해서	이수율도 높고	대응정도도 높다
	간부급이 직원급에 비해서	이수율도 낮고	대응정도도 낮다
H3		이수율이 높으면	대응정도가 높다

5.2 정책적 제언

5.2.1 정보보호 지식을 갖춘 일반직 직원의 채용프로그램 도입

연구결과에 따르면 정보보호업무를 수행하는 ICT 전문인력이 보안교육 이수율도 높고 사이버테러 대

응력도 우수한 것으로 나타났다. 그러나, 해당 인력이 전체 정원에서 차지하는 비율은 3% 정도에 불과하며, 이는 K-공사에만 국한된 것이 아니라 대부분의 공공기관에도 적용이 가능하다. 많은 공공기관 및 민간기업에서 정보보호 전문인력에 대한 중요성을 알지만 경영여건상 전문인력 확충에 어려움을 겪고 있는 것이 사실이다.

이를 극복하기 위해 다른 직무(사무, 기술 등)의 신입사원이나 경력사원 채용에도 정보보호 관련 과목을 이수하거나 자격증을 취득한 지원자에게 가산점을 부여하는 방안 등이 필요할 것으로 판단된다. 비록 ICT 전문인력은 아니지만 맡은 직무를 수행하면서 정보보호 취약점을 발굴하고 정보보호 부서와 합동으로 대처할 수 있는 기본역량을 보유하는 것이 필요하기 때문이다.

5.2.2 인적 및 직무특성에 차별화된 보안교육 도입

획일적인 보안교육의 실시보다는 다양한 인적 및 직무특성의 차이를 고려하여 보안교육의 난이도, 질적 수준, 과목의 차별성 등을 반영한 교육체계 마련이 필요하다. 특히 기술변화가 급변하는 현재 시점에서 연령대 등의 세대 차이는 정보보호 또는 정보보안 분야의 핵심적인 고려요인일 수밖에 없다.

본 연구결과에서 보듯이 경력이 높은 직원이 사이버 보안교육 이수율은 높지만 사이버테러 대응훈련에서는 대응정도가 낮아 바이러스에 감염될 확률이 높게 나타났다. 즉 교육내용에 대한 이해 없이 단순히 듣기만 했다고 볼 수 있는 것이다.

이를 극복하기 위해 교육원에 정보보호 관련 집합교육과정을 개설하여 고참직원들이 기초부터 교육받을 수 있는 환경여건을 조성하고 사업소 현장에서는 “정보보호 멘토링 제도”를 도입해 IT에 익숙한 젊은 직원들이 고참직원들의 후견인이 되어 정보보호 교육을 돕는 프로그램을 마련할 필요가 있을 것이다. 이는 보안교육이 향상될수록 사이버테러 대응훈련의 대응력도 상승한다는 것을 분석결과(H3)에서 확인되며, 특히 다양한 개인특성의 차이의 고려가 필요하기 때문이다.

5.2.3 상하구별 없는 제재규정 강화

연구결과에서 본사 및 간부의 보안교육 이수율과 사이버테러 대응훈련의 대응정도가 사업소 및 직원의 보안교육 이수율과 사이버테러 대응훈련의 대응정도보다 현적이 낮게 나타났다. 특이한 점은 본사에 소속되면서 경력이 높고 남성인 간부급 직원이 보안교육 이수율은 높지만 상대적으로 사이버테러 대응훈련의 대응정도는 낮다는 점이다.

사업소의 경우 지속적으로 사업소 경영평가에 반영하여 본사의 평가를 받기에 높은 실적을 유지할 수 있는 반면, 본사는 경영평가에서 제외됨에 따라 본사 직원들의 관심이 저조할 수밖에 없고 그 결과 교육이수나 사이버테러 대응 등에 소홀할 수 밖에 없었다. 특히 간부직원의 경우, 정보보호 업무가 회사의 주력업무가 아닌 부수적인 업무로 인식하는 경향이 많아서, 일반직원에 비해 소극적이고 관심이 적을 수밖에 없다.

이를 극복하기 위해 본사 처실에도 정보보호 이행평가제도를 도입하여 보안교육 이수와 사이버 테러 대응의 동기를 부여하고 간부직원의 인사평가에 반영함으로써 보안강화를 의무화 할 필요가 있는 것으로 판단된다.

5.2.4 비정규직의 정보보호 역량강화

정규직의 경우 비정규직에 비해서 상대적으로 보안교육 이수율과 테러훈련 대응 정도가 높은 것으로

분석되었다. 이는 정규직이 비정규직에 비해서 상대적으로 조직에 대한 몰입도가 높고 책임의식이 높을 수 있다는 점에서 기인한 결과로 판단된다. 따라서 기존의 비정규직의 인력을 정규직으로 확대 전환하거나, 비정규직인력도 정규직인력과 동일하게 다양하고 차별화된 보안교육의 기회를 부여함으로써, 상대적인 역량제고를 꾀할 필요가 있을 것으로 판단된다.

5.3 연구의 한계와 후속연구 필요

본 연구에서는 주로 개인적인 수준에서 인적 및 직무특성에 초점을 두고 보안교육 이수율과 사이버테러 대응훈련간의 관계를 규명하였다. 따라서, 이들 관계를 실증적으로 정립하여 K-공사를 중심으로 향후 관련된 분야에 대한 시사점을 제공하고 있다는 점에서 의미를 가진다.

그러나 본 연구는 다음과 같은 한계를 가질 수 있으며, 향후 추가적인 보완 연구 등이 이루어져야 한다.

본 연구는 양적인 방법론을 활용한 연구결과이며, 그 가운데서도 주로 개인수준의 다양한 변인을 고려하여 분석한 결과이다. 따라서 교육효과의 다양한 수준의 요인, 즉, 교육자의 자질, 프로그램의 질, 조직분위기 등의 추가적인 변인에 대한 고려가 부족하다는 한계를 가지며, 이에 대한 고민이 후속적인 연구로 이어질 필요가 있다.

더불어, 본 연구결과는 K-공사 내부직원들의 일반적인 경향을 파악하는데 용이하나 각 표본들 간의 특수하고 개별적인 특성을 파악하는 데는 용이하지 못하다. 즉 이상의 양적인 방법이 가지는 기본적인 한계를 보완하기 위해서 각각의 주요 특성별로 세분화하여 분석하거나, 추가적으로 심층면담, 인터뷰, 면접조사 등의 보완적인 질적 방법론을 활용한 연구가 이루어질 필요가 있다.

참고문헌

[1] 경찰청, “사이버범죄 유형별 현황,” 2012, pp. 1-2.

[2] 이기식, “인터넷시대 사이버보안의 인식양태 및 정책 대안,” 한국공공관리학보, 제22권, 제5호, 2008. pp. 99-127.

[3] 이신권, “공공기관 IT보안업무 종사자의 직무스트레스 결정요인에 대한 실증연구,” 고려대학교 정보보호대학원 석사학위논문, 2012.

[4] 시만텍, “기업 보안현황 보고서(Symantec 2010 State of Enterprise Security Study),” 2010.

[5] 백민정 외, “조직의 정보윤리실천이 구성원의 정보보안 인식과 행동에 미치는 영향에 관한 연구,” 경상논총, 제28권, 제4호, 2010. pp119-145.

[6] Al-ammer, S. A. “The Influence of Individual and Organizational Characteristics on Training Motivation and Effectiveness. Unpublished Dissertation,” The Stat University of New York at Albany, 1994.

[7] Tannenbaum, S. and Yukl, G., “Training and Development in Work Organizations,” Annual Review of Psychology, Vol.43, 1992. p399~441

[8] Bramley. P, “Evaluating Training Effectiveness-translating Theory into Practice,” McGraw-Hill Book Company, 1991.

[9] Dubois, D., “Competency based performance improvement: A Strategy for Organizational Change,” Amherst, MA: HRD Press., 1993.

[10] 백민정 외, “중소규모 조직구성원의 정보보안인식과 행동이 정보보안성과에 미치는 영향에 관한 연구,” 중소기업연구, 제133권, 제2호, 2011. pp. 113-132.

[11] 홍기향, “정보보호 통제와 활동이 정보보호 성과에 미치는 영향에 관한 연구,” 국민대학교 대학원

박사학위논문, 2003.

[12] 김종기 외, “패스워드의 정보시스템 보안효과에 영향을 미치는 요인에 관한 연구,” 경영정보학연구, 제18권, 제4호, 2008, pp. 1-26.

[13] 김경규 외, “정보자산보호 성과가 조직성과에 미치는 영향에 관한 연구 : 관리활동과 통제활동을 중심으로,” 정보관리연구, 제40권, 제3호, 2009, pp. 61-77.

[14] 정구헌 외, “정보보호 아키텍처 구성과 보안활동이 정보자산보호 및 조직성과에 미치는 영향,” 정보처리학회논문지, 제17권, 제3호, 2010, pp. 223-232.

[15] 김영곤, “정보보안 거버넌스의 구성요소가 종업원의 보안 인식과 행위에 미치는 영향에 관한 연구,” 한국항행학회논문지, 제14권, 제6호, 2010, pp. 935-950.

[16] 최응렬 외, “국가핵심기술 보호수준과 보안요인과의 관계연구,” 한국공안행정학회보, 제44권, 2011. pp. 365-413.

[17] 오문석 외, “디지털 컨버전스 환경에서 교육용 콘텐츠 활용방안에 관한 고찰,” 디지털산업정보학회 논문지, 제7권, 제4호, 2011, pp. 101-110.

[18] 이종락, “수요자 중심의 정보보호 전문 인력 양성을 위한 교육과정 설계,” 디지털산업정보학회 논문지, 제9권, 제3호, 2013, pp. 99-106.

[19] 최재영, “수요자 중심의 e-비즈니스 교육과정 개발에 관한 연구,” 디지털산업정보학회 논문지, 제7권, 제4호, 2011, pp. 141-152.

■ 저자소개 ■

신 현 조
Shin, Hyun Jo

1998년 1월~현재
한국전력공사 근무
1998년 2월 아주대학교 전기전자공학과(학사)
2014년 12월 고려대학교 정보보호대학원
(석사졸업예정)

관심분야 : 정보보호정책, 사이버보안, SCADA, 스마트그리드
E-mail : shj3@korea.ac.kr

이 경 복
Lee, Kyung Bok

2008년 2월 고려대학교 공과대학
산업시스템정보공학과 학사 졸업
2009년 3월~2010년 2월
고려대학교 정보경영공학
전문대학원 정보경영공학과
(정보보호전공) 석사 졸업
2010년 3월~현재
고려대학교 정보보호대학원
정보보호학과 박사 수료

관심분야 : 정보보호정책, 개인정보보호, 융합보안, 소셜네트워크분석
E-mail : isnare@korea.ac.kr

박 태 형
Park, Tae Hyoung

2002년 2월 고려대학교 서양사학과 학사 졸업
2004년 2월 고려대학교 일반대학원 행정학과
석사 졸업
2004년 4월~2008년 4월
한국행정연구원 연구원
2011년 2월 고려대학교 정보보호대학원 박사
졸업
2011년 3월~2014년 11월
고려대학교 정보보호연구원
연구교수
~ 현재 소프트웨어정책연구소 선임연구원
2002년 2월 고려대학교 서양사학과(학사)

관심분야 : 정보보호정책, 사이버국방, 방위사업
E-mail : mosto2004@korea.ac.kr

논문접수일: 2014년 10월 29일
수 정 일: 2014년 11월 16일
게재확정일: 2014년 11월 19일