ISSN 2234-4438
융합정보논문지 제7권 제2호 pp. 119-124, 2017 DOI : https://doi.org/10.22156/CS4SMB.2017.7.2.119

자원 제약하의 중소기업 정보보안계획 수립방안 연구

권장기[1], 김경일[2*]
[1]한국교통대학교 대학원 경영정보학과, [2]한국교통대학교 경영정보학과

A Study on Establishment of Small and Medium Business Information Security Plan under Resource Restrictions

Jang-Kee Kwon[1], kyung-Ihl Kim[2*]
[1]Dept. of MIS, Korea National University Grauduate School Of Transportation
[2]Dept. of MIS, Korea National University Of Transportation

요 약 정보는 기업의 규모와 무관하게 소중한 자산이며 정보보안은 기업의 생존과 번영을 위해 필수적인 요소이다. 하지만 대기업의 경우 정보보안경영시스템(ISMS)의 신속한 도입을 통해 안전을 확보해 나가지만, 중소기업의 경우는 예산 제약, 보안 지침의 미흡, 보안에 대한 인식 부족 등, 복합적인 요인들로 인해 보안시스템이 구축되지 않거나 구축이 지체되고 있다. 본 논문에서는 중소기업의 정보보안 관리 실태를 설문조사를 통하여 문제점을 분석하고, 중소기업을 위한 무료 또는 저렴한 방법으로 종합적인 보안계획 수립 방안을 제시하고자 한다. 본 논문이 제시하는 방법을 적용해 중소기업들은 최저 비용의 기본적인 정보보안을 구현할 수 있을 것이며, 정보보안 계획을 수립하고자 하는 중소기업들에 도움이 될 것이라고 믿는다.

키워드 : 정보보안, 중소기업, 보안계획수립, IT보안, 위험계획

Abstract Information is a valuable asset regardless of the size of the enterprise and information security is an essential element for the survival and prosperity of the enterprise. However, in the case of large corporations, Security is ensured through rapid introduction of information security management system. but In the case of SMEs, security systems are not built or construction is delayed due to complex factors such as budget constraints, insufficient security guidelines, lack of security awareness. In this paper, we analyze the actual situation of information security management of SMEs through questionnaires, and We would like to suggest a comprehensive security plan for SMEs in free or inexpensive ways. We believe that by applying the method presented in this paper, SMEs will be able to implement the lowest cost basic information security and will benefit SMEs who plan to establish an information security plan.

Key Words : Information Security, Business, Security Planning, IT Security, Risk Planning.

1. 서론

정보는 기업의 규모와 무관하게 소중한 자산이며 정보보안은 기업의 생존과 번영을 위해 필수적인 요소이다. 기업의 정보 보안은 지난 10년간 복잡하게 성장해 왔다[1]. 특히 최근에는 NFC 기반의 모바일 서비스 이용자가 급증하고 있으며, 이러한 이용환경 속에 보안에 대한 관심을 소홀히 한다면 피해가 극심할 것이라는 것은 자명하다[2]. 하지만, 대기업의 경우 정보보안 관리 시스템의 신속한 도입을 통해 안전을 확보해 나가지만, 중소기업의 경우, 예산 제약, 보안 지침의 미흡, 보안에 대한 인식 부족 등, 복합적인 요인들로 인해 정보보안 시스템이 구

Received 2017-03-07 Revised 2017-03-28 Accepted 2017-04-03 Published 2017-04-30
*Corresponding author : Kyung-Ihl Kim (kikim@ut.ac.kr)

축되지 않거나 구축이 지체되고 있다. 이로 인하여 기업 정보화가 기업을 중심으로 정보화 역기능으로 확산되고 있다[3]. 또한 정보화 역기능을 줄이기 위한 연구에서 임직원들의 태도, 규범적 신념, 대처 효능감, 중화, 준수혜택 등의 만족도가 조직원들의 정보화 역기능에 영향을 미친다고 하였다[4]. Power et. al과 Raymond는 기업 정보화에 영향을 미치는 요소로 정보화 도입기, 시스템 개발방식, 시스템 운영종류, 응용업무 등으로 정의하였다[5]. 따라서 본 연구에서는 한정된 자원 하에서 중소기업의 정보보안 계획 수립, 구현 및 이행 하는 적절한 방법을 제시하는 것이며, 중소기업이 누구나 쉽게 따라 할 수 있는 종합적이면서도 아주 간단한 정보보안계획을 고안하는 것이지만, 적절한 실행 계획은 철저한 교육 과정이 수반되어야 한다.

2. 정보보안 실행현황 조사 및 분석

본 연구를 위한 설문조사는 2015년~ 2016년 2년 동안 종업원 200명 이하의 영남권 소재 제조업 25개사를 대상으로 방문 조사하였고, 조사 대상은 정보보호 책임자 및 전산 관리자, 사무직원 등 90명을 대상으로 면담 조사하였고, 설문내용은 정책관리, 취급관리, 인적관리, 물리적 관리, 기술적 관리로 구성하였다.

설문조사 결과 전체적인 보안 등급은 Fig. 1에서와 같이 인적관리 부문을 제외한 전 분야에서 관리 수준이 미흡한 것으로 분석되었으며, 주요 원인으로 관리인력 부족, 정보보호시스템 도입 예산부족, 지식 및 정보 부족이 주요 원인으로 제시되었다.

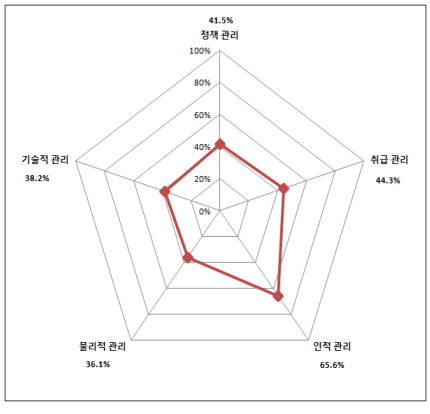

Fig. 1. Security rating by management category

각 분야별 문제점을 분석 한 결과는 Table 1과 같다.

Table 1. Status of Management Problems

	Problem
Policy Management	- Inadequate policies, guidelines and procedures - Insufficient security training and administrative protection measures
Handling Management	- Confidentiality creation, storage, and revocation procedures not yet established - Secret copying, lack of external export control level
Human resource Management	- Lack of security commitment in employment and retirement - Lack of awareness of employees' confidentiality obligations
Physical Management	- Insufficient access control zone designation and control procedures - Inadequate control of portable storage media
Technical Management	- Inadequate introduction of information protection solution - Network, storage media, email control insufficient
Security incident response	- Inadequate measures to deal with spill accidents - Insufficient recognition of legal protection requirements and remedies

3. 자원 제약하의 적용 가능한 보안 대책

3.1 당장 적용 가능한 보안 대책 수립

많은 기업들은 누구든지 "보안" 이라는 단어를 언급하면 많은 돈이 든다고 생각한다. 만일 기업들이 보안에 대하여 지식이 없어도 외부 전문가의 자문을 통하여 중소기업의 보안을 확보할 수 있도록 정부 각 부처에서 지원하는 제도를 이용한다면 용이하게 보안 대책을 수립 할 수 있을 것이다.

1) 보안 정책 및 절차를 수립한다.

중소기업에 적합한 정보보호 정책 및 지침, 절차를 작성하기는 쉽지 않다. 기업의 업종, 규모, 보호대상 정보의 종류, 각종 인프라 현황에 따라 다양한 형태의 정책 및 절차를 작성하게 된다. 보안계획을 수립하는데 가장 어려운 점은 우리가 상상할 수 있는 모든 상황을 해결할 수 있는 모든 종합적인 보안 정책과 절차를 만드는 것이다. 마이크로소프트와 CIA는 모두 각 기업에 맞게 적용하고 수정할 수 있는 정책수립 템플릿을 제공하고 있다[6]. 보안 정책은 회사의 내규에 명확하게 규정하며, ISO 품질

프로그램과 같은 검토 프로그램에 의해 검토되고 승인한다. 기술보호울타리(www.ultari.go.kr)에서는 중소기업에 적합한 표준화된 정책, 지침, 절차서를 제공하고 있으며, 기업의 필요 시 전문가의 자문을 제공하고 있다[7].

2) 비밀분류 및 취급 절차를 작성한다.

기업이 보호해야할 비밀이 무엇인지 분석하는 것이 정보보호의 우선순위이다. 내가 무엇을 보호해야 하는지 모르면서 정보보호를 한다는 것은 하지 않겠다는 것과 같은 의미이다. 비밀 분류 대상으로는 출력문서, 전자문서, 네트워크, 보안시스템, 소프트웨어, pc에 대하여 조사한 뒤 중요 자산에 대하여 비밀 등급을 부여하여 관리하여야 한다.

3) 보안서약서를 주기적으로 징구 한다.

대다수의 중소기업은 보안서약서를 입사 시 근로계약서의 일부 조항으로 삽입하여 징구하고 있다. 그러나 보안사고 발생 시 이러한 형태의 보안서약서 징구는 법의 보호를 받지 못하고 있다. 입사 시 징구한 보안서약서는 고용자의 우월적 지위에서 서약을 받았기 때문이다. 그래서 입・퇴사 및 재직중에 주기적으로 보안서약을 받도록 권고하고 있다. 표준 보안서약서 양식은 기술보호울타리 및 영업비밀보호센터(www.tradesecret.or.kr)에서 제공하고 있다[8].

4) 보호구역 지정 및 휴대용 저장매체 통제 방안을 수립 한다.

기술력이 우수한 중소기업도 기술 및 정보 유출을 방지하기 위하여 정보보호 솔루션 도입 등 많은 노력을 기울이고 있으나, 생산 현장에 대한 외부인의 불법적인 접근에 대한 통제가 상대적으로 미흡한 것으로 나타났다. 보호구역에 대한 상시 출입문 잠금 장치를 설치하고, 보호구역 안내판을 게시하여야 한다. 또한 외부인이 보호구역 방문 시에는 휴대용 저장매체를 사용할 수 없도록 봉인하는 조치가 필요하다.

5) 정부지원제도를 활용한 정보보호 솔루션 도입.

중소기업청에서는 기술력은 있으나 자금여력이 부족한 중소기업을 위하여 정보보호 솔루션 도입을 위한 지원 사업을 하고 있다. DRM, DLP, Firewall, 문서중앙화 솔루션 등 다양한 종류의 정보보호 솔루션을 지원하고 있다[9].

6) 방화벽을 확인한다.

침입에 대한 방화벽을 테스트할 수 있는 소프트웨어 공급 업체들이 훌륭한 무료프로그램들을 제공하고 있다. 몇몇 프로그램들은 단순히 침입을 기록하는 반면 고급 프로그램들은 위협에 기반 하여 반응을 한다. 공급 업체들을 검색하여 프로그램을 찾아서 사용한다.

7) 폴더는 필요한 접근 권한만 부여한다.

폴더에 대한 접근이 직원별 기준으로 하기위해서 NTFS[(New Technology File System)는 윈도우 NT 계열 운영체제의 파일 시스템]를 사용한다. 관리자의 콘텐츠만을 위해 전체 드라이브를 지정할 수 있다. 여기에서 주의할 것은 관리자가 자신의 책상을 이석할 때에는 화면을 잠그는 좋은 습관을 갖는 것이다.

8) 백업을 한다.

백업은 보안 목적 달성을 위해 매우 중요하다. 백업은 데이터와 그 데이터를 사용하는 응용프로그램 및 DBMS를 같이 백업한다(호환성을 위해서).

9) 모든 전자 메일은 악이다.

의심스러운 모든 것에 대해 사용자들을 교육한다. 매일 55,000,000,000건의 스팸 이메일이 사이버 세계(itsecurity.com)에 떠도는 것으로 추정되고 있다. 최근 많은 피해를 초래하고 있는 랜섬웨어 바이러스 등 악성메일 차단을 위하여 인지되지 않은 메일에 대한 무분별한 클릭 습관을 없애도록 직원들을 교육한다.

10) 이동용 컴퓨터와 저장 매체의 관리

이동용 컴퓨터 사용은 정보보안의 큰 위협이 된다. 모든 휴대용 장치에는 암호를 걸어 사용하도록 한다. 외부로부터 내부 네트워크로 반입되는 장비들에 대해서는 방역체계를 이용한 검사와 보안 절차를 준수한다.

3.2 물리적 보안 대책 및 이론적 설명

데이터의 도난은 전자적 수단에 의해 발생할 수 있다. 그러나 정보에 대한 물리적 위협은 기업 내에서 발생할 수 있다. 조직의 물리적 위협은 다음과 같이 정의할 수 있다.

1) 자연 재해

만일 건물이 홍수로 인해 물에 잠겨 어떤 일이 발생한

다면 경영층은 즉각적으로 알릴 수 있는 자동 경보 시스템을 갖추어야 한다. 또한, 위기관리절차(재해복구 및 비즈니스연속성 계획)를 준비하고 훈련하며 긴급 시 대처하도록 해야 할 것이다.

2) 건물 침입

외부자의 출입이 거의 없는 곳에 회사는 CCTV 또는 건물에 들어가기 위한 키 카드 액세스 같은 것에 투자할 이유가 없다. 또한 불특정 다수의 인원이 빈번히 출입하는 곳에 위치한 사무실의 출입 통제에 대해 모든 방문자가 쉽게 인지할 수 있도록 출입문에 "방문 사절"이나 "출입 시 안내 데스크 이용" 등의 안내 문구를 통하여 출입 통제를 실시하도록 한다.

3) 컴퓨터 침입

이러한 유형은 도난의 형태로 발생할 수 있으며, 확실하게 도난을 방지할 수 없다. 강력한 암호를 설정하고, 안전한 노트북 이동 케이스를 제공하고 직원들이 항상 적절한 여행용 가방에 자신들의 노트북을 가지고 다니도록 독려한다.

4) 정전

우리는 중요한 시스템들(즉, 서버, 방화벽, 전화 시스템, 네트워크 장치, 포장 기계 등)은 UPS에 연결해야 한다. UPS는 장기 정전의 상황에서 필요한 준비를 수행할 수 있는 충분한 시간을 계산하여(예, 2시간 동안 백업) 전원을 유지해야 한다[10].

3.3 인증(AUTHENTICATION)

사용자 인증은 사용자 액세스뿐만 아니라, 장치 또는 프로세스 인증의 두 가지 접근 유형을 정의하는데 사용된다[11]. 인증을 위한 암호 방법은 키 로깅, 피싱, 강탈, 우발적 또는 의도적인 발견을 통한 데이터 절도, 심지어는 사회 공학을 포함하는 다수의 기술에 의해 발견될 수 있다. 이러한 위험들은 최근 2단계 인증(two factor authentication)의 전개를 이끌었다.

3.4 권한부여

사용자 인증은 시스템에 접근하기 전에 발생하고, 권한부여는 접근한 후에 발생하는 것이 다르다. 권한부여 시 마이크로소프트와 대부분의 보안 전문가는 최소 권한의 원칙을 사용할 것을 권고한다. 미 국방성의 "신뢰 컴퓨터 시스템 평가 기준(Trusted Computer System Evaluation Criteria)"에서 최소 권한의 원칙이란, 시스템의 각 주체가 승인된 작업의 수행에 필요한 권한의 가장 제한적인 집합을 부여할 것을 요구하는 원칙으로 정의하고 있다. 이 원칙의 적용은 사고, 오류 또는 무단 사용으로 인해 발생할 수 있는 피해를 제한한다[12].

권한 부여 및 권한 계정에 대한 브리티시 컬럼비아 대학에서 실시한 연구는 연구에서 모든 사용자가 최소 권한의 원칙을 실천하지 않았다는 것을 발견하고 모든 노트북에 관리 권한을 부여했다[13]. 그들의 연구 결과에 따르면 높은 권한을 갖는 계정을 사용할 때의 이점에 대한 전문 교육의 부족이 원인인 것으로 발견되었다.

3.5 감사(AUDITING)

컴퓨터 네트워크상의 정보와 장치를 감사하는데 사용할 수 있는 몇 개의 도구가 있다. 현장검사를 수행하기 위해, "WinDirStat"이라는 이름의 유틸리티를 사용할 수 있다. 이 유틸리티는 색상 코드 파일 형식으로 드라이브의 시각적 묘사를 제공한다. 다음으로 "경험"이라는 도구로서 비록 대부분의 영역이 자동화될지라도 인간이 검사할 필요성은 여전히 존재한다.

하드웨어에 관해서, 감사 및 재고관리 도구뿐만 아니라 사용자가 인트라넷 포털과 통합된 IT 요청의 추적을 입력하고 유지하도록 하는 IT 티켓 로그 관리를 위해 "Spiceworks"를 사용할 수 있다.

3.6 방화벽 구축

방화벽은 네트워크 보안의 가장 중요한 요소이고, 인터넷을 통해 전 세계에 노출되는 모든 비즈니스는 강력한 방화벽 솔루션에 투자해야 한다. FireEye(2013)에 의한 연구에서 최근 사이버 공간이 중국에 의해서 미국의 특정산업으로 SNS등 다양한 수단으로 공격한다고 보고했다[14]. 방어 수단으로 원격 액세스, 서비스 거부 공격, 봇넷, 워 드라이빙(war driving), 모바일 감염 등과 같은 다른 중요한 진화하는 기술들을 목록에 추가할 필요가 있다. 또한 행동과 패턴을 "학습하고" 적응할 수 있는 방화벽을 설치하는 것이다.

3.7 침입 탐지 및 예방 모니터링

때때로 네트워크를 떠나거나 네트워크 내에서 거래되

는 정보는 인터넷으로부터 도착하는 정보보다 훨씬 더 악성이다. 산발적으로 발생할 수 있는 물리적인 탐지가 존재한다. 오펜하이머는 자동화된 모니터링이 생성하는 거짓 경보 중 일부는 도움보다 더 성가시다고 주장한다[15]. 종합적인 예방 계획은 다음의 탐지 및 방지 기술의 네 가지 주요 영역을 고려해야 한다[16].

1) 네트워크 기반

이는 네트워크를 통해 이동하는 데이터의 모든 비트를 추적하는 WiresharkTM와 같은 내부 네트워크 트래픽을 분석할 수 있는 도구를 사용할 수 있다.

2) 무선네트워크

보안 정책이 기업의 네트워크에 무선 연결을 허용하지 않도록 결정할 경우, 우리는 위에서 언급 한 바와 같이 문제 발생을 관리한다.

3) 네트워크 행동 분석

이것은 정책 위반, 서비스 거부 공격, 악성 코드, war driving 등과 같은 문제들이 방화벽에 도착한 트래픽의 분석을 통해 수행된다.

4) 호스트 기반

이것은 지정된 호스트 또는 문제를 일으키는 호스트의 서비스의 모니터링을 통해 수행한다.

3.8 훈련

직원들이 정보 보안의 가장 높은 위협으로 계속됨에 따라, 조직원들의 보안 목표 달성을 위한 교육 과정 운영이 필요하다. 정보기술 부서는 사업 연도의 많은 시간을 보안 교육 및 훈련을 하며, 내외부적으로 전문 인력 양성을 하고 온-오프라인의 교육과정에 참여시키고 있다. 또한 새로운 보안 위협에 대한 대처 능력이 향상된다. 따라서 보안 교육, 훈련 계획 수립 및 시행을 통한 위협 대처 능력을 향상시키고 조직의 안정성을 확보하는 것이 중요하다.

3.9 예방

정보기술 전문가들은 미래의 새로운 위협에 대처하기 위해 인터넷을 연구 도구로 사용할 필요가 있을 뿐만 아니라 네트워크를 모니터링하고 새로운 위협을 자세히 살피는 방법에 대해 교육을 받아야 한다. 그렇게 하는 방법은 다음과 같은 여러 가지가 있다.

1) 연구 온라인

새로 출현하는 위협을 모니터링하고 공표하는 웹사이트에 가입한다. (예 : http://www.capella.edu/blogs/iascommunity/). 이 사이트는 새로운 연구를 위한 좋은 사이트임.

2) 동향 분석 자료

사이버 위협에 관한 예측 자료를 많이 읽는다. (예 : "2014년 가장 큰 3가지 사이버 위협"[17])

3) 컴퓨터 보안 전문가 협회 웹 사이트

SANS 연구소.

4) 실시간 위험 모니터링 서비스

새로 발견되는 위협을 지속적으로 모니터링하고 보고하는 전용 웹 사이트(예 : Internet Storm Center).

4. 결론

본 연구에서는 예산 제약 및 보안 지침이 부족한 상황의 중소기업을 위한, 최단 시간, 최저 비용으로 보안 위협에 대처할 수 있도록 종합적인 보안 계획 수립 방안을 제시하였다. 제안 모델은 설문조사를 통하여 제시된 관리적, 물리적, 기술적 문제점에 대하여 중소기업에서 추가적인 예산 투자 없이 보안 위협에서 살아 남기위한 대응 방안을 제시하였다. 다만 본연구의 한계점은 조사 대상 기업이 200명 이하의 중·소규모 기업만을 대상으로 조사된 자료인 관계로 200명 이상 및 중견기업 등에 적용하기에는 결과가 상이할 수 있다고 판단되며, 또한 제시한 수립 방안을 실행하기 위한 정보보호 전문 인력 보유에 대한 조사가 미흡하여, 제시된 대안의 실행에 영향을 미칠 것으로 보인다. 향후 연구결과의 일반화 및 실효성 검증을 위하여 설문 대상 확대 및 정보보호 전문 인력이 실행에 영향을 미치는지에 대한 연구도 필요할 것으로 보인다.

REFERENCES

[1] M. S. Todd1 and S. M. Rahman, "Complete Network Security Protection For SME'S Within Limited Resources," *International Journal of Network Security & Its Applications (IJNSA)*, Vol. 5, No. 6, pp. 1-13, Nov. 2013. DOI: 10.5121/ijnsa.2013.5601

[2] K. I. Kim, G. S. Jeon and G. S. Chae, "NFC Payment System for Security Privacy and Location Information of User," *Journal of Convergence Society for SMB*, Vol. 6, No. 2, pp. 21-26, June. 2015. DOI: 10.22156/CS4SMB.2015.6.2.021

[3] Y. S. Jeong, "Design of Prevention Model according to a Dysfunctional of Corporate Information," *Journal of Convergence Society for SMB*, Vol. 4, No. 3, pp. 7-13, June. 2016. DOI: 10.22156/CS4SMB.2016.4.3.007

[4] J. K. Kwon and J. T. Lee, "An Empirical Study on the factors Information Protection Policy of Employee's Compliance Intention," *Journal of Convergence Society for SMB*, Vol. 4, No. 3, pp. 7-13, Aug. 2014. DOI: 10.22156/CS4SMB.2014.4.3.007

[5] Y. S. Jeong, "Design of Security Model for Service of Company Information," *Journal of Convergence Society for SMB*, Vol. 2, No.2, pp. 43-49, Nov. 2012. DOI: 10.22156/CS4SMB.2012.2.2.043

[6] M. S. MCS, "Business continuity planning: best practices for your organization," Retrieved from http://www.mcsmanagement.com/WhitepapersUpload, 2007.

[7] https://www.ultari.go.kr/portal/psi/techPrtcManual.do

[8] https://www.tradesecret.or.kr/bbs/standard.do

[9] https://it.smplatform.go.kr/prSysCnstc/intrcnView?bsns-ClCodeSe=0000002G

[10] K. Ojdana, and A. Watmore, "Getting physical with network security," Retrieved from http://www.molexpn.com/Media/docs/Getting-Physical-with-Network-Security-cb5ed721-977d-4f7d-a4c5-995b6524d3aa.pdf, 2010. 10.

[11] P. Oppenheimer, "Developing network security strategies," Retrieved from http://www.ciscopress.com/articles/article.asp?p=1626588&seqNum=2. 2010. 10.

[12] Microsoft. "Applying the principle of least privilege to user accounts on windows xp," Retrieved from http://technet.microsoft.com/en-us/library/bb456992.aspx, 2006. 01.

[13] S. Motiee, K. Hawkey and K. Beznosov, "Do windows users follow the principle of least privilege? investigating user account control practices. Symposium on Usable Privacy and Security (SOUPS)," Retrieved from http://cups.cs.cmu.edu/soups/2010/proceedings/a1_motiee.pdf, 2010.

[14] FireEye, "The advanced cyber attack landscape," Retrieved from http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-cyber-attack-landscapereport.pdf?mkt_tok=3RkMMJWWfF9wsRogs63NZKXonjHpfsX57O4kXqO%2BlMI%2F0ER3fOvrPUfGjI4ETcFlI%2FqLAzICFpZo2FFeE%2FKQZYU%3D. 2013.

[15] P. Oppenheimer, "Developing network security strategies," Retrieved from http://www.ciscopress.com/articles/article.asp?p=1626588&seqNum=2, 2010.

[16] K. Scarfone and P. M. Mell, *Guide to intrusion detection and prevention systems*, NIST SP, No. 800-94, 2007.

[17] J. Lazauskas, "the-3-biggest-cybersecurity-threats-of-2014-and-how-the-federal-government-plans-stop-them," http://www.forbes.com/sites/centurylink/, 2014. 10.

저 자 소 개

권 장 기(Jang-Kee Kwon) [정회원]

- 1988년 3월 : 공군사관학교 산업공학과 (학사)
- 2010년 8월: 경북대학교 경영정보학과(경영학 석사)
- 2015년 2월 ~ 현재 : 한국교통대학교 경영정보학과(박사과정 수료)

<관심분야> : ISMS, IMS, BCM

김 경 일(kyung-Ihl Kim) [종신회원]

- 1983년 2월 : 명지대학교 경영학과(학사)
- 1994년 2월 : 명지대학교 경영학과 (경영학 박사)
- 1993년 4월 ~ 현재 : 한국교통대학교 경영정보학과 교수

<관심분야> : IMS, Design of AIS