소규모 IT 서비스 기업 비즈니스 특성을 고려한 보안 관리모델 실증연구

An Empirical Study on Security Management Model for Small IT Service Business

김 양 훈 (Yanghoon Kim) 상명대학교 소프트웨어 & 미디어 연구소
나 영 섭 (Youngsub Na) 상명대학교 경영학부
장 항 배 (Hangbae Chang) 상명대학교 경영학부, 교신저자

요 약

IT 고도화에 따라 정보 유출 및 침해 사고가 날로 증가하고 있다. 이에 따라 대다수의 기업들은 보안 위한 투자를 확대하고 있지만, 여전히 정보 유출의 취약점에 노출되어 있다. 소규모 IT 서비스 기업은 대기업에 비하여 상대적으로 한정된 자원과 인력으로 기업 활동을 수행하고 있으며, 실제 가치를 창출하는 방법에 따라 SI/SM, DB, IR, IP 업종으로 분류되고 있다. 그러나 현재까지 소규모 IT 서비스 기업을 위한 보안관리에 관한 연구는 소규모라는 기업규모와 IT 서비스라는 비즈니스 특성을 고려한 핵심 정보자산식별에 머물러 있는 상황이다.

따라서 본 연구에서는 소규모 IT 서비스 기업의 보안대책 수립을 위한 보안관리 모델을 설계하였다. 그리고 설계된 보안관리 모델에 대해 비즈니스 특성을 고려한 소규모 IT 서비스 기업을 대상으로 실증분석을 수행하고 분석된 결과를 바탕으로 추진전략을 제시하였다.

키워드 : 소규모 IT 서비스, 보안관리 모델, 비즈니스 특성, 보안 추진전략

Ⅰ. 서 론

IT 고도화에 따라 정보 유출 및 침해 사고가 날로 증가하고 있다. 이에 따라 대다수의 기업들은 보안관리를 위한 투자를 확대하고 있지만, 여전히 정보 유출의 취약점에 노출되어 있다(강종구 등, 2011).

소규모 기업은 국내 전체 사업체수의 99%, 총 고용의 86% 이상(2008년 사업체기초 통계조사 결과 300인 미만 사업체수 및 해당 종사자수)을 차지하는 등 국가 경제에 막대한 비중을 차지하고 있으며, 국가경제 발전 및 경쟁력 창출의 원동력 역할을 수행하고 있다. 지난 10년간 소규모 기업은 꾸준한 외형적 성장을 보이고 있으나, 중견기업이나 대기업으로 전환하는 기업의 비율이 극

† 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 연구되었음(NRF-2011-332-1-B00109).
본 논문은 지난 2012년 한국경영정보학회 추계학술대회에서 우수논문상을 수상했으며, Information Systems Review 편집위원회에 의해 12월 23일 게재확정된 논문임을 알려드립니다.

히 낮아 소규모 기업의 실질적인 성장을 뒷받침할 수 있는 국가차원의 정책적 지원이 필요한 시점이다. 특히, 한 기업의 정보화는 기업의 양적 질적 성장에 매우 중요한 필수 요소이므로, 기업의 정보화가 해당 기업의 비즈니스 등 사업 성격에 가장 적합한 방향과 수준으로 향상되는 것은 소규모 기업의 발전을 통한 국내 산업 전체의 성장으로 이어질 수 있는 매우 중요한 요소이다(김지숙 등, 2010).

소규모 IT 서비스 기업은 비즈니스 형태에 따라 SI(System Integration), SM(system Management), DB(Data Processing), IR(IT Rent), IP(Information) 업종으로 분류될 수 있다. 이러한 소규모 IT 서비스 기업은 대기업에 비하여 상대적으로 적은 인력으로 핵심 자산에 대한 보호 활동을 수행하고 있다(강종구 등, 2011). 그러나 소규모 IT 서비스기업들의 정보화 현황과 비즈니스 영속성을 위한 핵심 정보 자산에 대한 분석은 이루어지지 않은 채 모든 정보화 도구와 다양한 핵심 정보 자산을 갖춘 대기업들에 적합한 보안 관리체계를 부분적으로 도입하고 있다. 이러한 적합하지 않은 보안관리 체계 구축 및 투자는 과다한 투자로 인한 비용적 자원 손실과 실제 핵심 자산을 보호하지 못하고 범용적인 보안관리에만 인력을 투입하는 손실을 가지게 되었다.

따라서 본 연구에서는 소규모 IT 서비스 기업의 보안대책 수립을 위한 보안관리 모델을 설계하고자 한다. 그리고 설계된 보안관리 모델에 대해 비즈니스 특성을 고려한 소규모 IT 서비스 기업을 대상으로 실증분석을 수행하고자 한다.

Ⅱ. 선행연구

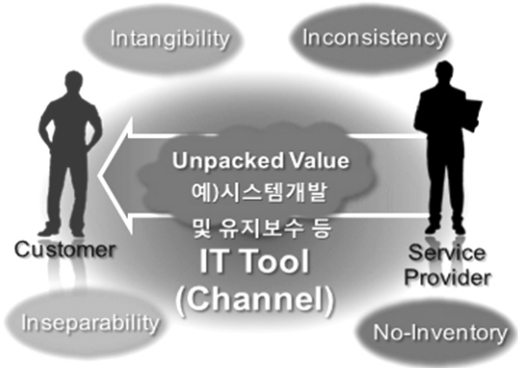
2.1 해외 보안관리 평가 제도

정보보호 관리체계(Information Security Management System, ISMS)는 조직의 자산에 대한 안정성 및 신뢰성을 향상시키기 위한 절차와 과정을 체계적으로 수립하고 문서화하여 지속적으로 관리하고 운영함으로써 앞서 설명한 보안의 3요소를 실현하기 위한 일련의 과정 및 활동을 이야기한다(김지숙 등, 2010). 보안 관리체계는 기업의 민감한 정보를 안전하게 보존하도록 관리할 수 있는 체계적 경영시스템이며 이에는 인적 자원, 프로세스 및 정보시스템 모두를 대상으로 포함한다. 대표적인 보안 관리체계에는 ISO/IEC 27001, IT Baseline Protection Manual 등등이 있다.

2.2 국내 보안관리 평가 제도

국내 보안관리 관련 평가 체계는 정부에서 시행하는 체계 및 지표와 민간에서 시행하는 지표로 나눌 수 있다. 정부에서 운영 중인 정보보호관련 평가 체계 및 지표는 국가정보원, 방송통신위원회, 행정안전부 주관으로 개발되었으며, 민간에 운영 중인 정보보호 관련 평가 지표는 한국정보통신산업협회의 주관으로 시행 중에 있다.

정부에서 주도적으로 시행하는 관리 체계 및 평가 지표로는 국가정보원/방송통신위원회의 국가정보보호지수, 국가정보원의 정보보안 관리수준 평가, 방송통신위원회의 정보보호 안전진단과 K-ISMS(KISA-Information Security Management System)을 시행하고 있으며, 행정안전부의 전자정부서비스 보안수준 실태조사, G-ISMS(Government-Information Security Management System) 그

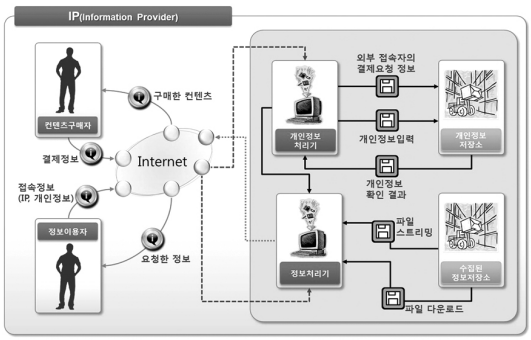


〈그림 1〉 소규모 IT 서비스 기업 정의

리고 공공기관 개인정보보호 수준진단이 있다. 그리고 지식경제부 산하 정보통신산업진흥원에서 eTRUST를 시행하고 있다. 또한 방송통신위원회는 2010년 9월 PIMS(Personal Information Management System)의 도입 방안 마련을 추진 중에 있다.

2.3 소규모 IT 서비스 기업 정의

소규모 IT 서비스를 “기본단위 형태로 구성되어 있지 않은(unpacked value) 무형의 제품(intangible goods)을 IT적 수단(IT tool)을 통하여 고객에게 제공(≒ IT 활용을 서비스 하는 것) 하는 것”으로 정의되었다. 소규모 IT 서비스 기업은 한국 IT 서비스 산업협회에서 분류한 IT 서비스 산업 분류와 한국 제8차 표준산업분류체계 기준, 한국 제9차 표준산업분류체계 기준을 기반으로 하여 분류하였으며(강종구 등, 2011), 대 분류, 즉 비즈니스 종류를 SI(System Integration), SM(system Management), DB(Data Processing), IR(IT Rent), IP(Information)로 분류된다.



〈그림 2〉 소규모 IT 서비스 기업 비즈니스 프로세스(IP업 예시)

SI/SM 업종은 IT 기술을 활용한 시스템 자문 및 구축/기 구축된 시스템 운영 및 유지보수를 비즈니스 프로세스로 하고 있다. DB 업종 은 물리적 형태의 자료를 디지털화하는 것을 주 비즈니스 프로세스로 보유하고 있다. 그리고 IR 업종은 보유하고 있는 시스템 및 솔루션(서비스) 등을 임대하는 사업을 비즈니스 프로세스로 하고 있다. 마지막으로, IP업은 IT 기술을 통하여 생성된(가공된) 서비스 및 정보를 제공하는 사업을 주 비즈니스 프로세스로 운용하고 있다.

2.4 소규모 IT 서비스 기업 보안관리 요구사항 도출

소규모 IT 서비스 기업의 내부 자산관리 관점에서 단계별로 식별된 핵심 자산을 토대로 정보보호 요구사항을 도출하였고, 각 기업 유형의 비즈니스 서비스 관점의 IT 자산 별 보안관리 요구사항을 도출하였다.

2.4.1 내부 자산관리 관점의 보안관리 요구사항

IT 활용 성숙도 1단계의 보안관리 요구사항을 살펴보면, 1단계에서 식별된 핵심 정보자산은 개별 PC와 수집 데이터이며, 식별된 핵심 정보자산에 대한 보안관리 요구 사항은 개별 PC 별로 관리하고 있는 데이터 및 사용자 데이터에 대한 접근권한 관리, PC 별로 침입한 웜・바이러스, 스팸 등 제거 및 차단, 외부로부터 물리적으로 내부 PC 은닉으로 도출되었다. IT 활용 성숙도 2단계의 보안관리 요구사항을 살펴보면, 2단계에서 식별된 핵심 정보자산은 업무지원 서버, 통합 데이터베이스, 기업 내 네트워크 환경이며, 식별된 핵심 정보자산에 대한 보안관리 요구 사항은 동일한 보안관리 수준 유지를 위한 전사적인 사내 PC 관리, 서버의 사용자 별 이용 통제 및 기업 내에서 사용하는 응용 프로그램 접근통제, 외부로부터의 해킹, 바이러스 공격에 대한 감시 및 대응, 서버와 연결된 통합 데이터베이스에 대한 접근권한 관리 및 모니터링으로 도출되었다. IT 활용 성숙도 3단계의 보안관리 요구사항을 살펴보면, 3단계에서 식별된 핵심 정보자산은 기업 간

협업 정보(자원/재고정보, 수요예측/판매정보, 신상품 개발정보 등) 및 기업 간 협업시스템 및 응용프로그램(CRM, SCM 등)이며, 식별된 핵심 정보자산에 대한 보안관리 요구 사항은 협업 시 공유되는 정보 등에 대한 암/복 호화, 기업 간 협업시스템과 관련된 기업 내·외부 네트워크 접근통제, 서버에 탑재된 응용 프로그램 별로 사용자 접근권한 통제로 도출되었다.

2.4.2 비즈니스 서비스 관점의 보안관리 요구사항

각 기업 유형의 비즈니스 서비스 관점의 IT 자산 별 보안관리 요구사항은 다음과 같이 조사 정리하였다.

- SI/SM 서비스 관점의 IT 자산별 보안관리 요구사항
  - 디렉토리 자산: 기업 내 공유 디렉토리를 식별되지 않은 사용자의 사용 탐지 및 방어, 기업 내 영업 비밀이 공유되어있는 특정 공유 디렉토리에 대한 강한 보안성 유지, 기업 내 공유 디렉토리의 계정 관리, 공유 디렉토리 사용자/사용자 그룹에 대한 인증 지원 솔루션
  - 파일서버 자산: 기업의 파일서버에 개방되어 있는 port를 통한 외부공격 및 비정상적 접근 방어, 파일서버 사용자 인증 솔루션, 파일서버 사용자 권한 관리 솔루션, 열람한 파일/작업시간/작업내용/접속주소별 기록·관리 기능
  - 응용 프로그램 자산: 각 응용프로그램의 잠재적 보안 취약점 방어 및 형상관리

- DB 서비스 관점의 IT 자산별 보안관리 요구사항
  - 입력처리장치 자산: 비 인가자의 입력처리장치 사용 방지 및 보안성 유지, 입력처리장치 오·남용 방지, 입력처리장치에 대한 외부의 악의적 접근 방어
  - 데이터베이스 접점(entrypoint) 자산: 비인가자의 데이터베이스 사용 방지 및 보안성 유지, 데이터베이스 오·남용 방지, 데이터베이스에 대한 외부의 악의적 접근 방어, 불법/악의적 데이터 질의(data query)통제 및 검사결과 데이터 마스킹(data masking)에 대한 보안기능
  - 데이터베이스 콘텐츠(data field) 자산: 비인가자의 데이터베이스 사용 방지 및 보안성 유지, 데이터베이스 오·남용 방지, 데이터베이스에 대한 외부의 악의적 접근 방어, 사용자/관리자 질의 로그기록/분석 및 (데이터베이스 內에)데이터 암/복호화에 대한 보안기능

- IR 서비스 관점의 IT 자산별 보안관리 요구사항
  - 공용자원(저장 공간, 메모리 등) 자산: 암호화된 정보에 대해 검색가능 지원 및 정보소유자의 권한을 침해하지 않으면서 유용한 정보를 추출하는 것에 대한 보안기능
  - 공급되는 IT 응용 서비스(기존, 신규) 자산: 사용자 컴퓨터와 좀비(zombie) 컴퓨터를 분별하는 것에 대한 보안기능, 정밀한 트래픽 감지 및 다양한 외부공격 유형에 대응하는 것에 대한 보안기능

- IP 서비스 관점의 IT 자산별 보안관리 요구사항
  - 사용자 자산: 암/복호화 과정을 통한 전자서명, 접속 시 마다 자동으로 새 비밀번호 생성, Identity Access Management에 대한 보안기능, 키보드 입력정보 암/복호화에 대한 보안기능,
  - 웹 콘텐츠 자산: 웹 정보 불법 도용행위(capture) 차단에 대한 보안기능
  - 이미지/동영상 콘텐츠 자산: 저작권이 있는 콘텐츠의 구매자 확인 및 사용 인가 솔루션, 콘텐츠 유통 및 사용에 대한 보안기능,

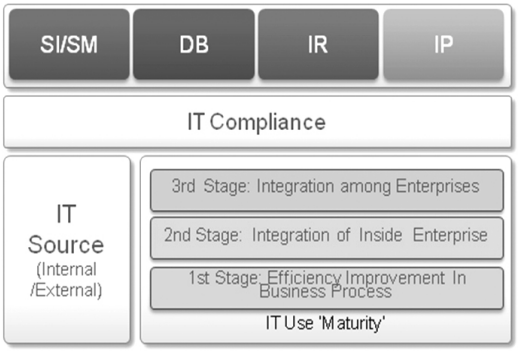
콘텐츠 저작권자 고유마크(fingerprint)를 삽입에 대한 보안기능

◦ (개인정보)데이터베이스 자산: 개인정보 노출(웹, 디렉토리, 파일 등)취약점 점검에 대한 보안기능

Ⅲ. 소규모 IT 서비스 기업 보안관리 모델

3.1 소규모 IT 서비스 기업 보안관리 모델 개념적 설계

소규모 IT 서비스 기업의 보안관리 개념적 체계를 바탕으로 소규모 IT 서비스 기업의 보안관리 모델을 설계하기 위하여 다음과 같은 세 가지 특성을 고려하였다. 첫째, 소규모 IT 서비스 기업은 IT 인프라와 IT 활용 정도를 기반사항으로 고려한다. 둘째, 소규모 IT 서비스 기업 비즈니스 별 자산을 보호한다. 마지막으로 IT 인프라 및 IT 활용도와 비즈니스 자산은 IT 서비스 컴플라이언스(Compliance)로 연결된다.



〈그림 3〉 소규모 IT 서비스 기업 보안관리 모델

3.2 소규모 IT 서비스 기업 보안관리 모델 세부적 설계

기존 소규모 IT 서비스 기업 보안관리 진단 도구 문제점 크게 세 가지의 문제점을 보유하고 있다. 첫째, 체계화된 선행연구 이론에 근거를 두지 않고 있기 때문에 진단결과에 대한 해석이 어렵다. 둘째, 설문영역 및 설문항목에 대한 구성(흐름)이 체계화되어 있지 않으며, 실증연구가 수행되지 않았기 때문에 통계적 신뢰성 분석을 통한 지속적인 개선작업이 필요하다. 셋째, 설문 문항별 응답 예시들 사이에 일관화 된 성숙도(성숙도 결정요인에 따른 분류가 맞지 않음)가 유지되고 있지 않다. 이러한 문제점들을 고려하여 <표 2>와 같은 소규모 IT 서비스 기업 보안관리 모델 실증분석을 위한 진단 모형을 설계하였다.

〈표 2〉 소규모 IT 서비스 기업 보안관리 진단 모형

진단 영역		진단 항목	
기업 일반현황		일반 개요/업종 정보/재무 정보	
정보화 현황		공통 정보자산	
		업종 정보자산	
보안관리 진단 수준	보안관리 지원 환경	보안관리 정책	
		보안관리 조직	
		보안관리 지원운영	자산관리
			인적보안
	보안관리 기반 구조	물리적 보안	
		기술적 보안	공통 정보자산 보안
			업종 정보자산 보안
	보안관리 운영관리	유지보수	
		사고대응	

3.3 소규모 IT 서비스 기업 보안관리 모델 적용 타당성 분석

3.3.1 소규모 IT 서비스 기업 보안관리 모델 적용 결과

실증분석을 수행을 위하여 단일 업종을 수행

하는 소규모 IT 서비스 기업의 정보화 현황 및 보안관리 현황을 진단하였다. 그리고 소규모 IT 서비스 기업 보안관리 진단 모형에 따라 각 기업별 정보화 현황 점수 및 보안관리 현황 점수를 도출하였다. 설문에 참여한 2개 기업의 평균 정보화 현황점수는 100점 기준 21.5점으로 진단되었으며, 평균 보안관리 현황점수는 19.35점으로 나타났다.

〈표 3〉 소규모 IT 서비스 기업 정보화 및 보안관리 현황 진단 결과

진단영역	진단항목	진단결과	
		A 기업	B 기업
정보화 현황	공통 정보자산	6.7	2.0
	업종 정보자산	20.0	14.3
정보화 현황 진단결과		26.7	16.3
보안관리 현황	보안관리 지원 환경	11.7	5.8
	보안관리 기반 구조	6.1	6.3
	보안관리 운영관리	4.4	4.4
보안관리 현황 진단결과		22.2	16.5

3.3.2 소규모 IT 서비스 기업 보안관리 모델 적용 사례

A기업은 SI/SM 업을 주로 수행하는 기업으로써, 정보화 및 보안관리 현황 점수에 따른 민감도와 대응책을 살펴보면 다음과 같다. 민감도는 기업 내 보유 정보시스템과 핵심 정보자산에 따라서 보유하고 있는 양적인 정도에 따라 분석하였다.

내부 자산관리 관점과 비즈니스 서비스 관점 자산 민감도는 최대 25의 값이 도출되었다. 민감도 점수에 따라 우선적으로 보안 대응책을 마련해야 하는 자산은 '재무관리시스템, 공유 디렉토리, 파일 서버, 프로젝트 관리 프로그램'으로 식별되었다.

이와 같은 우선순위와 민감도를 가진 A기업의 보안관리를 위한 추진 전략을 다음과 같이 구성할 수 있다. 디렉토리 자산의 사용자인증 및 사용자 권한관리 요소 보안 대응을 위해 Active Directory를 운용할 수 있다. 그리고 파일서버 자산의 사용자인증 및 사용자 권한관리, 운영관리/사고대응 요소 보안을 위해 보안 파일 서버(File Server Security)를 활용해야 한다. 마지막으로, 응용 프로그램 자산의 프로그램 지원 요소 보안을 위해 응용 프로그램(지원) 보안을 수행해야 한다.

〈표 4〉 소규모 IT 서비스 기업(A) 보안관리 모델 적용사례

자산		민감도	우선순위
기능적 시스템	재무회계시스템	25	1
	인사관리시스템	-	-
공동 작업공간	공유 디렉토리	25	1
	파일 서버	25	1
	프로젝트 관리 프로그램	25	1

B기업은 IP 업을 주로 수행하는 기업으로써, 정보화 및 보안관리 현황 점수에 따른 민감도와 대응책을 살펴보면 다음과 같다.

〈표 5〉 소규모 IT 서비스 기업(B) 보안관리 모델 적용사례

자산		민감도	우선순위
기능적 시스템	재무회계시스템	3	2
	인사관리시스템	3	2
디지털 콘텐츠	웹 콘텐츠	20	1
	이미지/동영상 콘텐츠	-	-

내부 자산관리 관점과 비즈니스 서비스 관점 자산 민감도는 최대 20, 최소 3의 값이 도출되었다. 민감도 점수에 따라 우선적으로 보안 대응책을 마련해야 하는 자산은 '웹 콘텐츠'로 식별되었다. 이와 같이 분석된 결과에 따라 B기업의 보

안관리를 위한 추진 전략을 다음과 같이 구성할 수 있다. 웹 콘텐츠 자산의 유출방지를 위하여 웹 콘텐츠 보안(Web Contents Security) 솔루션을 운용할 수 있다. 더불어, 콘텐츠 자산의 사용자인증 및 사용자 권한관리, 사고대응 요소 보안을 위하여 저작물 보안(Contents Digital Right Management), 디지털 워터마킹(Digital Watermarking)을 운용할 수 있다.

Ⅳ. 소규모 IT 서비스 기업 보안관리 추진전략

4.1 소규모 IT 서비스 기업 보안관리 지원체계 구축

소규모 IT 서비스기업 보안관리 지원체계 구성을 위하여 <표 6>과 같이 보안관리 정책, 인적보안, 관리적 보안, 물리/기술적 보안의 4개 대항목으로 구성한다. 세부적으로 보안관리 법 제도, 보안관리 정책, 보안관리 홍보, 보안관리 전문교육, 보안관리 담당조직, 인력변동 관리, 인력변동 체계, 보안관리 업무처리 절차, 보안관리 활동 보안감사, 보안관리 사고처리 절차, 보안관리 현황 관리, 자산분류 및 등급화, 접근통제/책임추적의 13개 세부 항목으로 구성한다.

〈표 6〉 소규모 IT 서비스 기업 보안관리 지원체계

지원체계 항목	지원체계 세부항목	지원체계 영역
보안관리 정책	보안관리 법 제도	보안관리 지원환경
	보안관리 정책	
인적보안	보안관리 홍보	보안관리 지원역량
	보안관리 전문교육	
	보안관리 담당조직	
	인력변동관리	
	인력보상체계	
	보안관리 업무처리 절차	
	보안관리 활동 보안감사	보안관리 운영관리
	보안관리 사고처리 절차	
관리적 보안	보안관리 현황관리	보안관리 기반구조
	자산분류 및 등급화	
물리적/ 기술적 보안	접근통제/ 책임추적	

4.2 소규모 IT 서비스 기업 보안관리 세부 추진과제

보안관리 지원환경 부분에서는 네 가지 핵심적인 추진전략을 제안하고자 한다.

첫째, 소규모 IT 서비스 컴플라이언스(Service Compliance) 체계화 및 실천방법을 보급해야 한다. 지속가능한 IT 서비스 제공을 위하여 세부 업종마다 기본적으로 요구되는 서비스 컴플라이언스 항목을 선정하고 이를 실천하기 위한 최소한의 방법을 제시해야 한다.

- SOX (J-SOX, K-SOX) : Protect Financial Information
- PCI : Protect Card Data
- HIPPA : Protect Patient Information
- GLBA : Protect Private Financial Information
- Basel II : Protect financial Data
- EU Directive : Protect Individual (Personal) Information
- PIPEDA (Canada) : Protect Personal Information
- CA1386 : Protect Personal Information
- FDA Title 21 CFR Part 11 : Protect Clinical trial Data
- Law 8204 : Protect Financial Information

〈그림 4〉 소규모 IT 서비스 기업을 위한 컴플라이언스 항목 예시

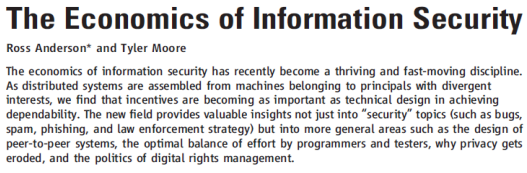
둘째, 소규모 IT 서비스 기업 보안관리 현황 자가 진단 및 쿠폰 제 컨설팅 서비스를 시행해야한다. 소규모 IT 서비스 기업이 보안관리 현황을 용이하게 진단하고 개선방향이 도출되면 그간의 보안관리 활동 참여 실적(교육, 홍보 캠페인 참여, 보호나라를 통한 패치다운로드 등)을 마일리지로 축적하여 간략 수준의 보안관리 컨설팅을 제공해야 한다.

셋째, 경량 형/맞춤 형 소규모 IT 서비스 정보보호 관리 매뉴얼을 개발 및 보급해야 한다. 가치 창출방법이 업종마다 상이하고 경영자원이

부족한 소규모 IT 서비스 기업에게 적합한 실천적 수준의 보안관리 매뉴얼을 개발하여 보급할 필요가 있다.

〈그림 5〉 소규모 IT 서비스 기업을 위한 보안관리 매뉴얼 예시

넷째, 소규모 IT 서비스 기업 보안관리 경제성 분석모형을 연구해야 한다. 의사결정이 집중화되어 있는 소규모 IT 서비스 기업 임원진들에게 보안관리 투자를 효과적으로 이끌어 낼 수 있도록 지원하기 위하여 간략하게 피해규모 예측(negative view) 및 보안투자를 통한 효과성/생산성(positive view) 규모를 설계할 수 있는 방법을 개발해야 한다.



The Economics of Information Security

Ross Anderson* and Tyler Moore

The economics of information security has recently become a thriving and fast-moving discipline. As distributed systems are assembled from machines belonging to principals with divergent interests, we find that incentives are becoming as important as technical design in achieving dependability. The new field provides valuable insights not just into "security" topics (such as bugs, spam, phishing, and law enforcement strategy) but into more general areas such as the design of peer-to-peer systems, the optimal balance of effort by programmers and testers, why privacy gets eroded, and the politics of digital rights management.

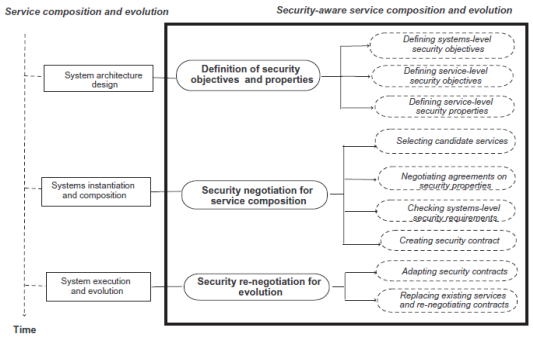
〈그림 6〉 보안관리 경제성 분석 문헌 예시

보안관리 지원역량 부분에서는 다음과 같이 핵심적인 추진전략을 제안하고자 한다.

소규모 IT 서비스 기업을 위한 보안관리 교육을 체계화해야 한다. 기존 이론 중심의 보안관리 교육을 조직의 보안관리 인식제고, 업종별 차별화된 보안관리 스킬(skill) 향상, 보안관리 개발자보다는 보안 관리자 양성을 위한 보안관리 교육 프로그램을 재구성할 필요가 있다.

보안관리 기반구조 및 운영관리 부분에서는 두 가지 핵심적인 추진전략을 제안하고자 한다.

첫째, 경량 형 보안관리 시스템을 구축 및 운영지원해야 한다. 대기업에 비하여 상대적으로 작은 규모의 소규모 IT 서비스기업 시스템 구성 현황(architecture)을 고려한 시스템 개발과 구축을 지원하며, 궁극적으로 서비스 형태로 보안수준을 유지할 수 있는 지원체계(Security Oriented Service)를 구성



〈그림 7〉 서비스 지향형 보안 서비스 구성 예시

둘째, 소규모 IT 서비스 보안사고 상시 지원체계를 운영해야 한다. 온라인 형태로 가치를 전달하고 있는 소규모 IT 서비스 기업의 특성을 고려하여, 실시간 원격으로 소규모 IT 서비스 자체에 대한 보안침해 상황을 점검하고 대응방법(ontology 기반의 pattern형 침해대응 방법 제공)을 제공할 수 있는 상시 지원체계를 운영할 필요가 있다.

Ⅴ. 결 론

정보통신의 발달에 따라 역기능으로 대두되는 정보유출 등의 취약점을 해결하기 위해 많은 기업들이 보안관리 체계를 구축하고 있다. 그러나 대기업과 상이한 특성을 지닌 소규모 IT 서비스 기업은 대기업들과 동일한 분석 및 대응책을 세우기가 어려운 실정이다.

이에 따라서, 본 연구에서는 조직, 비즈니스, 정보화 수준 등에 대한 특성을 고려한 보안관리 모델을 설계하고, 소규모 IT 서비스 기업을 대상으로 실증분석을 수행하였다.

이는 소규모 IT 서비스 기업의 특성을 파악하여 기존의 단발성 보안관리 시스템의 단점을 보완할 수 있으며, 기업에 대한 조직, 비즈니스, 정보화 수준 등에 관한 특성을 도출하고 이를 유형화함으로써 간략화 된 목표성 있는 보안관리 투자의 기반을 제공할 수 있다.

향후 연구로는 소규모 IT 서비스 기업의 각 업종을 대상으로 보안관리 모델을 적용시켜 객관타당성을 확보하고자 한다. 그리고 소규모 IT 서비스 기업에서 핵심적인 자원인 조직원들을 대상으로 보안 의식 및 인식 모델에 대하여 연구할 예정이다.

참 고 문 헌

강종구, 임재환, 이홍주, 장항배, “소규모 IT 서비스 기업 비즈니스 특성을 고려한 정보자산 유형분류 설계연구”, 한국전자거래학회, 제16권, 제4호, 2011, pp. 97-108.

김지숙, 이수현, 임종인, “민간기업과 공공기관의 정보보호 관리체계 차이 비교”, 정보보학회지, 제20권, 제2호, 2010, pp. 117-129.

임동희, 여돈구, 염흥열, “국내외 정보보호 수준 평가 체계 및 지표 동향”, 정보보호학회지, 제20권, 제5호, 2010, pp. 74-85.

전성희, 나영섭, 김양훈, 장항배, “비즈니스별 RFID 시스템 도입사례 성과분석 연구”, Information Systems Review, 제13권, 제3호, 2011, pp. 15-26.

Chang, H., J. Kim, and S. Lim, “Information Security Management System for SMB in Ubiquitous Computing, Computational Science and Its Applications”, *ICCSA*, Vol.3983, 2006, pp. 707-715.

ISO/IEC, “ISO/IEC 27001: 2005 Information security management systems-Requirements”, 2005.

Information Systems Review
Volume 14 Number 3
December 2012

An Empirical Study on Security Management Model for Small IT Service Business

Yanghoon Kim* · Youngsub Na** · Hangbae Chang**

Abstract

Depending on the sophistication of IT, it is increasing more and more information leaks and breaches. Accordingly the majority of companies have expand investment protection for the information. However, companies still have been exposed the vulnerability of information leakage. Especially, small IT service businesses than large corporations relatively have some limitations in the points of resources and manpower business activities. For studies on information security for small IT service companies so far, however, there have been insufficient studies considering small business scales and business characteristics of IT services. In this study, we made to design an information security management model for establishing security measures of small IT service companies which are classified SI/SM, DB, IR and IP industry that depending on how the value creation of the business. In detail, we performed an empirical analysis for small IT service business to consider business characteristics and we proposed security implementation strategies based on the analysis results.

Keywords: Small IT services, Security Management Models, Business Characteristics, Security Implementation Strategy

* The Institute of Computer Software & Media Technology, Sangmyung University
** Division of Business Administration, College of Business, Sangmyung University

◐ 저 자 소 개 ◑

김 양 훈 (kimyh7902@smu.ac.kr)

현재 상명대학교 소프트웨어 & 미디어 연구소에서 박사 후 연구원으로 재직 중이며, 대진대학교 컴퓨터공학과에서 소프트웨어공학 박사학위를 취득하였다. 주요 관심분야는 산업보안, 시스템 개발 프레임 워크 및 평가 등이다.

나 영 섭 (ysna@smu.ac.kr)

현재 상명대학교 일반대학원 경영학과 석사과정 중이며, 대진대학교 경영학과에서 학사학위를 취득하였다. 주요 관심분야는 산업 보안, 경영정보 시스템 활용 및 평가 등이다.

장 항 배 (hbchang@smu.ac.kr)

연세대학교에서 정보시스템 전공으로 박사를 취득하고, 현재 상명대학교 경영학부 조교수로 재직 중이다. 주요 관심분야는 기술경영 및 보호(의식, 문화, 관리체계 등), 경제적 성과 분석 등이다.

논문접수일 : 2012년 11월 23일 **게재확정일 : 2012년 12월 23일**