한국컴퓨터정보학회 하계학술대회 논문집 제19권 제2호 (2011. 6)

시스템 사고를 이용한 이러닝 서비스의 정보보호관리

이준희°
°충북대학교 경영정보학과
e-mail: luxmea@lycos.co.kr

Information Security Management in e-Learning Service Using System Thinking

Jun-Hee Lee°
°Dept. of Management Information System, Chungbuk National University

● 요 약 ●

본 논문에서는 시스템 사고를 이용한 이러닝 서비스의 정보보호관리를 제안하였다. 이러닝 활용이 증가되면서 이러닝 시스템에 불법적인 접근을 통한 정보의 유출, 변조, 삭제 등 다양한 위협 요인도 병존하고 있기 때문에 정보자산에 대한 위협 및 위험요소에 대한 체계적인 대책과 지속적인 관리의 중요성이 지속적으로 증가하고 있다. 현재 이러닝 운영 기관에서 정보자산을 보호하기 위해 다양한 정보보호 활동과 노력을 하고 있으나, 하루가 다르게 변화하고 있는 IT 환경에서는 조직의 운영 환경과 여건에 맞게 정보자산을 보호하기 위해서 시스템 사고를 활용한 동태적인 관리가 종합적이고 지속적인 정보보호관리체계 수립을 위해서 필요하다.

키워드: 시스템 사고(System Thinking), 정보보호(Information Security), 이러닝(e-Learning)

I. 서론

과거 2009년 해킹사고 피해 기관별 분류 결과를 보면 기타(개인)(76%), 기업(19.7%), 대학(2.8%), 비영리(1.1%)이었다. 또한 2010년 1월부터 3월까지 해킹사고 피해를 기관별 분류한 결과를 보면, 기타(개인)(51.4%), 기업(42.8%), 비영리(3.6%), 대학(2.2%)로 기업의 해킹 사고(비율)이 점차적으로 증가되는 것으로 보고한다[1].

앞의 조사 결과는 기업이나 대학에서 이러닝 서비스 운영 증가로 해킹사고로 인한 정보 자산에 대한 위협 및 위험 요소에 대한 체계적인 대책수립이 필요함을 보여준다.

이러닝에서 위험관리는 그림 1과 같이 조직의 정보시스템을 이루고 있는 각 자산을 식별하고 자산의 가치와 자산을 위협하는 요소 및 취약성을 분석하여 위험도를 산정하는 위험분석 과정과 자산의 위험도를 조직이 감수할 수 있는 수준으로 낮추기 위하여 보안 대응책을 마련하는 과정을 포함한다.

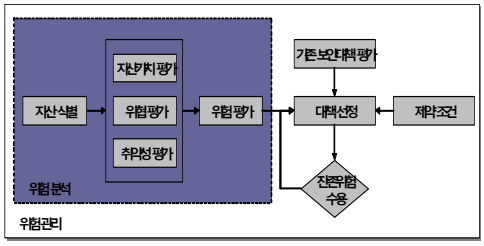

그림 1. 위험관리
Fig. 1. Risk Management

특히 급속한 IT 환경 변화로 정보의 공유와 위험관리를 포함한 정보보호를 동시에 만족할 수 있기 위해서 단편적인 사고에서 벗어나 시스템 사고를 통한 종합적인 정보보호관리가 필요하다.

시스템 사고(system thinking)는 다음과 같은 점을 강조하고 있다. 첫째, 문제요인들의 순환적 인과관계와 피드백구조를 강조하는데 피드백 구조는 변수들간의 인과관계가 상호 연결되어서 하나의 폐쇄회로를 형성하는 것을 의미한다. 둘째, 문제를 유발하는 요인의 상대적 중요성이 고정되어 있는 것이 아니라 시간의 흐름에 따라 변하는 것으로 본다. 셋째, 문제요인을 찾아내고 요인들이 어떻게 문제를 유발하는지도 설명한다. 넷째 분석적 사고와 통합적 사고의 조화를 강조하여 시스템을 구성하는 부분들을 분석하고 차례로 부분들을 연결하여 시스템 전체를 이해한다.

본 논문의 목적은 시스템 사고를 활용하여 이러닝 서비스의 정보보호관리를 체계적으로 관리하는데 있다.

II. 관련 연구

교육 서비스에서의 정보보호에 관한 선행연구와 정보보호관리체계(ISMS)를 살표보면 다음과 같다.

1. 교육 서비스에서 정보보호

표 1. 선행 연구
Table 1. Preceding Research

출처	연구 내용
최영미(2004)[2]	DRM관련 기술에 대하여 소개하고 이러닝 기술에서 정보보호 기술의 위치를 살펴보고 교육용 디지털콘텐츠의 특성을 분석하여 교육콘텐츠의 DRM을 활용사례 중심으로 기존의 Commerce DRM과 Enterprise DRM과 비교하여 제시
김경희 외 2인 (2008)[3]	효율적인 사이버 교육 운영 및 발전적인 개선을 촉진하기 위하여, 한 대학을 중심으로 개설된 사이버교육에 대한 학습자 만족도를 실시하고 분석하여, 그 결과를 토대로 사이버교육을 효과적으로 운영하기 위한 방안을 제안
한국인터넷진흥원(2010)[4]	대학의 정보보호 관리 수준이 크게 미흡, 전문인력 및 예산 확보 미흡, 정보보호 중요성은 인식하고 있으나 실제 시스템 투자 등에는 소극적으로 파악

2. 정보보호관리체계(ISMS)

정보보호관리체계는 정보보호관리에 대한 표준적 모델 및 기준을 제시하여 기업의 정보보호관리체계 수립·운영을 촉진하고 기업의 정보보호를 위한 일련의 활동 등이 객관적인 인증 심사 기준에 적합한지를 한국 인터넷진흥원이 인증하는 제도로 정의되며 그림 1과 같이 시설, 장비, 조직, 문서, 정책이 통합되어 운영된다[5].

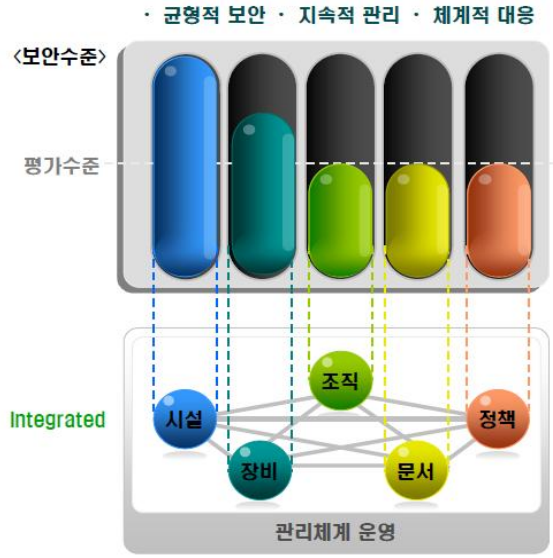

그림 2. 정보보호관리체계 운영
Fig. 2. ISMS Operations

선행연구와 정보보호관리체계를 통한 시사점은 이러닝에서 학습자 만족도 향상과 콘텐츠 보호를 위해서 정보보호관리체계를 도입하고 정보보호 시스템 투자에 대한 효율성을 높이기 위해서 시스템 사고를 통한 동태적인 정보보호관리의 필요성이다.

III. 본 론

본 논문에서 제안한 시스템 사고를 통한 이러닝 서비스에서 정보보호관리를 위한 정보보호관리 영역 구성은 다음과 같다.

1. 이러닝 서비스에서 정보보호관리

1.1 정보보호정책 관리

정보보호정책은 정보보호의 대상, 정보보호의 요구사항, 정보보호 기능 요구사항, 정보보호 조직의 구성, 정보자산의 분류, 정보의 비밀 등급 분류, 인적 보안, 물리적 보안, 운영 보안, 접근 통제, 업무 복구 등의 정책을 관리한다.

1.2 정보보호조직 관리

정보보호 강화를 위해 보안조직을 구성하고 이를 체계적으로 운영 및 관리하기 위해서 정보보호책임자, 보안 감사자, 개인정보보호관리자, 정보통신보안관리자, 정보보호담당자를 두고 역할을 부여한다.

1.3 인적보안 관리

업무 취급인가 및 승인, 정보자산에 대해서 접근권한을 부여하여 해당대상자만 사용하고, 부여된 접근권한 이외의 의도적, 비의도적 접근 수행을 방지한다.

1.4 정보보호교육 관리

보안정책, 관리지침, 규정, 절차 등의 보안관리 기초지식 및 정보시스템의 안전한 운영을 위해 필요한 사항들을 주지시켜 자발적인 보안의식을 고취시키고 부주의나 고의에 의한 보안 사고를 최소화한다.

1.5 사용자 계정 및 비밀번호 관리

정보시스템 접속을 위한 사용자 ID 및 비밀번호의 관리 및 사용에 대한 준수사항을 규정함으로써 정보시스템의 안정적인 운영 및 효율적 관리를 가능하게 한다. 사용자 계정 분류, 사용자 계정 등록 및 관리 절차, 사용자 계정 생성 및 정지, 사용자 계정 폐기, 비밀번호 관리기준 설정, 관리자 계정과 패스워드 관리 등을 수행한다.

1.6 서버 보안 관리

내/외부인의 불법적이고 비 인가된 위협으로부터 데이터 및 시스템 자체의 기밀성, 무결성 및 가용성을 확보한다. 서버 시스템의 관리에 관련된 제반 사항을 포함하며, 하드웨어와 소프트웨어 설치와 변경, 서버의 변경, 서버의 운영, 서버의 매각과 폐기 등을 포함한다.

1.7 네트워크 보안 관리

네트워크를 통해 실수나 고의로 정보를 누출, 변조, 파괴하려는 일련의 행위를 탐지하고, 차단하여 정보시스템 및 데이터의 보안성을 확보하기 위해서 네트워크 구성 및 장비운영상의 보안을 제공한다. 네트워크 구성 변경 절차, 외부 접속 절차를 포함한다.

1.8 보안 시스템 보안 관리

효과적인 보안시스템 운영을 통해 실수나 고의로 외부 네트워크로부터 내부 시스템 및 데이터 등의 자원에 접근하여 이의 누출, 손상, 파괴 등 일련의 불법적 행위를 차단하고 감시한다.

1.9 웹서버 및 홈페이지 보안 관리

인터넷 웹 서비스 시스템의 안전한 운영에 관하여 필요한 절차를 제시하는 것을 그 목적으로 하며 웹 서비스 관리 절차, 웹서버 관리 절차를 포함한다.

1.10 데이터베이스 보안 관리

내부인과 외부인의 불법적이고 비인가된 위협으로부터 데이터의 기밀성, 무결성 및 가용성을 확보하는 것을 그 목적으로 하며 데이터베이스 관리에 관련된 제반 사항을 포함하며, 인증, 접근제어 및 로그/감사 등을 포함한다.

1.11 보안사고 대응 관리

내부 혹은 외부로부터의 불법적이고 비인가된 보안 침해 시도에 대해 효과적으로 예방, 대응 및 사후관리 함으로써 업무에 끼치는 위험을 최소화한다. 정보자산 및 이를 사용하고 있는 교직원 및 협력사원, 임시직원, 아웃소싱 직원 등 상근 내/외부 인력을 대상으로 하며 침해사고대응 절차를 포함한다.

1.12 문서 및 운용자료 보안 관리

문서 및 운용자료로 존재하는 내부, 외부 자료를 관리하고 처리하는 원칙을 제공한다. 문서 및 운용자료 보안 적용 범위는 인쇄물 및 정보저장매체(백업매체, 테이프, CD와 같은 매체) 등에 기록된 문서와 운용자료를 포함한다.

1.13 PC 보안 관리

PC에 대한 보안을 유지하게 함으로써 원활한 업무 수행이 지원될 수 있도록 한다. 주요 PC 목록 및 대책, 출입관리 기록부, PC 보안 점검표를 포함한다.

1.14 E-mail 보안 관리

E-mail의 안전한 운영을 통해 내부 자원의 보안성을 확보하는 것에 그 목적이 있다. E-mail 사용의 안전성을 확보하기 위한 제반 사항에 적용되며, E-Mail 사용자 계정의 등록/삭제 및 암호화, E-mail 첨부파일의 보안 등을 포함한다.

1.15 위험 관리

주요 정보자산에 대한 위험분석을 통해 자산의 위험을 감소하기위한 대책을 수립하고 체계적인 정보보호 계획을 수립하는 위험분석의 기준을 제시하는 것을 목적으로 하며 위험분석 절차를 포함한다. 정보시스템에 관련된 투자가 대형화되고 관련된 자산의 특성 및 취약성, 각종 위협의 형태와 대책들이 지속적으로 변화하고 있기 때문에 정보보호계획 수립에 반드시 필요하다[6].

1.16 보안 감사 관리

보안관리가 제대로 유지되는지 확인할 목적으로 보안감사활동을 수행함에 있어서 기본적인 원칙을 정의한다. 직접적으로는 내부에서 보안감사를 실시하는 보안감사팀 및 그 구성원에게 적용되며 간접적으로는 보안감사 대상이 되는 교직원 및 정보자산에 적용되는 것으로 한다. 보안 감사 결과 및 사후 조치 보고서를 산출물로 한다.

1.17 개발 보안 관리

응용프로그램의 개발시 검토되어야 할 정보보안 통제를 소프트웨어 수명 주기별로 작성하여 응용프로그램의 보안성, 안전성, 신뢰성을 확보한다. 기획 및 분석 단계 보안, 설계 및 개발 단계 보안, 테스트 및 운영 이관 단계 보안, 외주 개발시의 보안을 포함하고 요구사항 타당성 검토 보고서, 보안성 검증 결과 보고서, 외주 개발업체 평가표, 시스템 변경 영향분석 검토 보고서 등을 산출물로 한다.

1.18 개인정보보호 관리

개인정보를 처리하는 정보시스템을 운영함에 있어 개인정보를 체계적으로 관리하고, 허가 받지 않은 공개, 변조 및 파괴 등으로부터 보호한다. 교육목적을 위하여 정보통신망 또는 정보통신망 이외의 수단을 통하여 수집, 저장, 사용, 전송 및 폐기되는 개인정보에 대해서 적용되며, 이러한 개인정보를 취급하는 교직원 및 협력업체 직원에 대해서 적용한다. 개인 정보 취급 및 관리, 물리적 보안, 침해 대응 및 복구, CCTV 관리를 포함한다.

1.19 업무연속성 관리

장애, 침해사고 및 재해 발생시 정보시스템의 서비스 연속성을 확보를 목적으로 한다. 조직의 구성, 업무영향 분석, 업무연속성계획 수립, 업무의 중요도 등급 분류, 비상연락망 구축, 장애 및 사고대응, 사후 관리 등을 포함한다.

1.20 암호 관리

중요 정보를 보호하기 위한 암호화 방안을 제시하는데 목적이 있다. 비밀성이 요구되는 중요 정보를 대상으로 하며, 해당 정보를 처리 및 저장, 전송하는 정보시스템을 대상으로 한다. 암호 키 신청 대장(생성, 분배, 복구, 폐기)과 암호 키 관리대장을 포함한다.

2. 이러닝 서비스의 정보보호관리 인과지도

이러닝 서비스에서 정보보호관리를 위한 20개의 관리영역을 중심으로 인과지도를 사용한 정보보호관리 모델링은 그림 3과 같다. 체계적인 정보보호관리는 사용자 만족과 이러닝 성과로 이어진다.

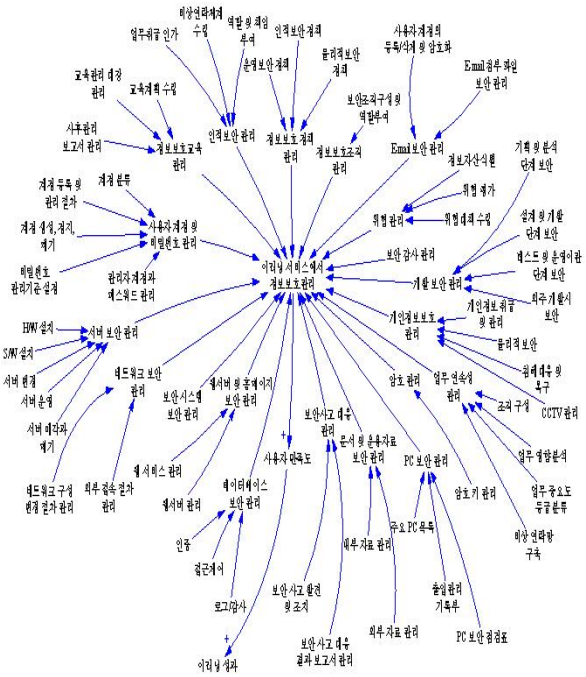

그림 3. 이러닝 서비스에서 정보보호관리를 위한 인과지도
Fig. 3. Causal Loop Diagram for Information Security Management in e-Learning Service

Ⅳ. 결론

본 논문에서는 시스템 사고를 활용한 이러닝 서비스의 정보보호관리를 제안하였다. IT 환경의 급속한 변화로 통합적이고 동태적인 정보보호관리체계는 정보의 기밀성, 무결성, 가용성을 실현하는 동시에 사용자 만족과 이러닝의 성과로 이어지기 때문에 이에 대한 지속적인 개선과 보완이 이루어져야 할 것이다.

참고문헌

[1] KISA, “Information Security Management System(ISMS) to build and operate educational practitioners course,” 2010.

[2] ymchoi, “Digital Rights Management of Education Contents,” Digital Contents, Vol. 5, No.3, pp.192-198, 2004.

[3] khkim, kskim, yksong, “A Study on the Analysis of Participants’ Satisfaction Ratings for the Promoting Cyber Education,” Informaton · Security, Vol. 8, No. 4, 2008.

[4] KISA, “ISMS Certified auditor training materials,” 2010.

[5] KISA, “ISMS Management Process,” 2009.

[6] KISA, “Information Security Management System Risk Management Gide,” 2005.