http://dx.doi.org/10.24173/jge.2017.12.6.4 일반논문

인간의 요소에 초점을 맞춘 정보 보안 전략 탐색※

이려화·황인호·허성호*

【목차】

1. 서론

정보 보안이란 불법적인 방식의 접근, 사용, 공개, 파괴, 손실, 수정, 혹은 운영중단으로부터 소중한 데이터를 보호하는 전략을 의미한다. 정보 보안은 흔히 컴퓨터 보안 및 시스템 보안의 개념으로 접근하기도 하고, 근래에는 인간의 요소로 접근하는 경향이 높아지고 있다. 아울러, 이들 용어는 모두 정보의 기밀성, 무결성, 그리고 가용성을 보호한다는 일반적인 목표를 지닌다.[1)]

※ 이 논문은 2017년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-과제번호)(NRF-2017S1A5A8021221)

* 허성호: 교신저자, 중앙대학교 심리학과, powerrcy@hanmail.net

1) S. L. Pfleeger & D. D. Caputo(2012), "Leveraging Behavioral Science to Mitigate Cyber Security Risk", McLean: MITRE, pp. 4~6.

한편, 이제 정보의 대부분은 디지털 컴퓨터의 방식에 의해 수집, 처리 및 저장되고 있고, 네트워크를 통해 다른 사용자들에게로 전송된다. 만약, 이러한 과정에서 기업의 고객이나 재무상태, 그리고 새 제품라인에 관한 기밀 정보가 경쟁사의 손에 들어오게 된다면, 보안 침해의 결과로 예상되는 매출의 급락, 법률소송, 혹은 사업 쇠퇴 결과는 참혹할 수 있다. 따라서 기밀 정보를 보호하는 것은 조직이나 기업에 있어 생사가 걸린 주된 요구사항이 될 수 있으며, 다차원의 법적인 요구사항이기도 하다. 아울러, 개인에게 있어서 정보 보안은 프라이버시에 관한 침해를 비롯해 다양한 보안침해로 접근해 볼 수 있으며, 이는 개인사에 중요한 영향을 미친다. 하지만, 정보보안에 대한 접근은 의례적으로 컴퓨팅 기술에만 지나치게 의존하는 경향이 있다. 이에, 정보보안의 개념적 접근을 검토하고, 적용되는 자세한 실태를 파악하여, 인간의 요소에 해당하는 주요 안들을 제시할 필요성이 대두된다.

2. 정보 보안의 주요 원칙

2.1. 기밀성

기밀성(confidentiality)이란 비밀유지가 반드시 필요한 정보가 합법적으로 접근, 사용, 훼손, 혹은 공개 권한이 있는 자에 의해서만 정보를 접근하도록 제한하는 원칙을 가리킨다.[2] 예를 들면, 기밀정보를 컴퓨터 화면에서 조회하고 있을 때, 접근허용을 허가 받

2) ISACA(2009), “An Introduction to the Business Model for Information Security”, Rolling Meadows, IL: ISACA, pp. 14~5.

지 아니한 누군가가 슬쩍 화면을 들여다본다면 이는 정보 보안 차원에서 기밀성의 침해에 해당한다. 또 우리 조직의 전 직원에 관한 인사관련 정보가 저장되어 있는 휴대용 저장장치나 노트북이 도난당한 경우에도 접근이 허용되지 않은 제3자의 수중에 넘어가 있기 때문에, 기밀성이 침해됐다고 판단할 수 있다.

이러한 관점에서 본다면 우리 생활의 전반에 걸쳐 정보 보안의 개념은 매우 밀접하게 관련되어 있다고 해도 과언이 아니다. 우리가 면허증을 신청하고, 온라인 쇼핑몰에서 회원가입을 하고, 보험상품을 구매하거나 은행대출을 신청할 때, 개인 정보에 해당하는 이름, 성별, 주민등록번호, 주소, 전화번호, 생년월일, 연소득 금액, 직장 정보 등과 같은 다양한 신상 정보를 제공하는 절차를 거치게 된다. 이들 정보는 매우 개인적인 정보이지만, 비즈니스 거래를 성사시키기 위해서는 신뢰성의 차원에서 이러한 정보를 제공이 절대적으로 필요하다. 그리고 이러한 과정에서 우리가 전제하는 조건은 자신의 정보를 제공할 때, 제공한 정보가 불법적인 루트를 거쳐 공개되지 않도록 보호될 것이며 또 그 정보가 사용권한자들에 의해서만 정당한 목표를 위해 이용될 것이라는 사항들이 포함된다.

특히, 기밀성은 앞서 언급한 바와 같이 개인 신상정보가 제공한 개인 각각의 프라이버시를 유지하는데 보안침해를 받지 않는 조건을 충족해야 하는 필수 조건이 된다. 그리고 프라이버시(privacy)란 단순한 전자상거래 관점의 정보를 포함한 제공한 모든 개인정보의 사용을 통제하는 것을 의미하는 용어로서 기밀성보다는 상위 개념으로 볼 수 있다.[3)]

3) PCI(2014), "Information Supplement: Best Practices for Implementing a Security Awareness Program", PCI SSC Standard, pp. 19~25.

2.2. 무결성

무결성(integrity)이란 데이터가 타당한 승인 없이 조작되거나 개조 혹은 삭제되어서는 안 된다는 원칙을 의미한다. 또한 데이터베이스 체계의 한 영역에 저장된 자료가 동일 데이터베이스 체계의 다른 영역과 혹은 다른 데이터베이스 체계에 저장된 다른 여러 가지 관련자료들과 일치해야만 함을 의미한다.[4] 예를 들어, 데이터베이스 체계에서 유지보수 절차 수행이 적절한 시스템종료 과정을 거치지 않았거나 갑자기 전원공급이 중단될 경우에는 무결성 침해가 발생할 수 있다. 또는 컴퓨터 바이러스가 컴퓨터에 감염되거나, 혹은 온라인 구매자의 관련 정보나 제품의 가격을 임의로 변경하는 경우에도 무결성 침해가 발생한다. 그리고 직원이 실수로 혹은 악의적인 의도로 인해 중요한 데이터 파일들을 삭제하는 경우에도 무결성이 적용 된다. 이 관점은 비교적 최근에 발생하는 보안 침해의 많은 부분으로 기록되고 있으며, 컴퓨팅 기술의 한계라기보다 사람의 정보 보안 의식 결함으로 나타난다고 할 수 있다.

2.3. 가용성

가용성(availability)의 개념은 의도한 바대로 지속적으로 정보를 기반으로 하는 기능이 잘 수행되는 정도를 나타낸다. 즉, 정보가 필요할 때나 그 정보를 처리하기 위해 사용되는 인터페이스 자원이 모두 안정적으로 준비되어 있고 정확히 기능하고 있음을 의미한다. 정보시스템이 정상적으로 가동되기 위해서는 응용프로그

4) ISACA(2009: 15~6).

램, 데이터베이스, 네트워크 등의 제반 구성요소가 정상 동작 상태를 유지하고 있어야 한다.[5] 즉, 이러한 상황이 정지된다면 가용성이 침해된 경우라고 할 수 있다. 예를 들어, 의도적인 디도스 공격이나 트로이목마와 같은 바이러스의 영향으로 사용 자체가 거부당하는 경우라고 할 수 있다. 가용성을 확보하기 위해서는 접근 통제, 데이터 백업, 장비의 이중 보안 등의 방법이 있다. 아울러, 사람의 활동으로 발생하는 경우는 보안 절차를 준수하도록 하는 정보 보안 의식을 높이는 교육이 대표적인 방법이라고 할 수 있다.

2.4. 사후 인증

사후 인증(post-authentication)은 거래 완료 후 고객이 e-메일을 이용해 제품 주문이 완료되었다고 하더라도, 이후에 제품 주문을 한 적이 없음을 알리고 거래사실을 부인하는 경우라고 할 수 있다. 만일 고객으로 하여금 공식적으로 인준된 디지털 서명을 부착해 거래내용을 전송토록 한다면, 미필적 유형의 사후 부인을 봉쇄할 수도 있다. 하지만, 근본적인 목적은 정보 보안의 침해로부터 보호하기 위한 전략의 경우에 주안점을 두어야 하며, 전자상거래에서 불순한 범죄의 피해로부터 보호하기 위한 방책으로 보아야 할 것이다. 즉, 당사자가 인증하는 과정을 이중으로 보안하고자 하는 절차로 구조화하였다고 볼 수 있다. 따라서 고객이 실제로 본인이 주장했던 사실이라는 측면을 확인하는 방법도 사후인증의 또 다른 방식이라고 할 수 있다.

5) ISACA(2009: 15~7).

3. 정보 보안의 실태

전 세계적으로 웹 기반의 기술 및 서비스의 발전은 상당한 속도로 진행되고 있다. 그러나 정보 보안의 문제는 여전히 전문가뿐만 아니라 사용자들 사이에서도 다양한 양상으로 언급되고 있다. 특히 기업과 기업 내 사용자는 사이버 공격에 우려하고 있으며 결과적으로 정보 보안 위험을 최소화하고자 다양한 전략에 초점을 맞추어 정보 보안 유지를 위해 노력한다.[6)]

하지만 인터넷은 방대한 네트워크여서 위협에 대한 잠재력이 크기 때문에, 온라인상의 공격자들은 보안 침해 행동의 다양한 기술을 활용하여 늘 예상치 못하는 방법을 사용하여 치명적인 위협을 가하고 있다. 실제로 최근 해커들은 가짜 웹 사이트를 개발하여 사용자에게 웹 사이트에서 무료 바이러스 백신 소프트웨어를 다운로드하도록 요청하는 경우도 나타나고 있다. 많은 사용자가 위조 된 웹 사이트에서 바이러스 백신 소프트웨어를 다운로드하고 개인 정보를 잃어 버렸으며, 개인정보와 자신이 보유한 타인의 정보까지 누출되는 사건이 되었다.

이러한 현상은 기술 및 위협적 환경이 자주 변경되면서 치러지는 동적 마찰을 줄이기 위해 만든 소프트웨어의 침투 사례로 이어지기도 한다. 예를 들어, 사물인터넷(Internet of Things; IoT)은 장치, 시스템, 서비스 및 심지어 스마트 개체를 연결하고 다양한 프로토콜, 도메인 및 응용 프로그램을 다루는 수많은 새로운 응용 프로그램을 인터넷에 표시한다. 이러한 동적 연동체제의 변화 과정에서 발생하는 정보 보안 침해의 사건들은 정보 보안 위험을

6) N. S. Safa, & M. A. Ismail(2013), "A customer loyalty formation model in electronic commerce", *Econ Model*, 35, pp. 561~62.

예측하고 계량하기가 더욱 어려워 졌다는 것이 사실이다.[7] 그리고 이 과정에서 가장 큰 공통적인 특징은 관리자나 사용자 등의 사람 요소가 크게 주목받고 있다는 점이다. 왜냐하면 지금까지 매우 절대적으로 사람의 요소가 아닌 기계적 하드웨어나 소프트웨어적인 측면에서 정보 보안의 방어구축이 핵심전략으로 두각을 보이고 있었기 때문이다.

그렇다면 사람의 요소라고 하는 것은 어떤 의미를 내포하고 있는가? 가장 대표적인 것은 담당자가 정보 보안에 적합한 의식적 행동을 얼마나 준수하는가의 문제가 여기에 해당한다. 예를 들어, 의식적인 주의 행동은 이 같이 특이한 공격을 막는 효과적인 방법이 될 수 있다.[8] 의식적인 행동이란 사용자가 시스템에서 작업할 때 정보 보안 측면에서 자신이 취한 조치의 결과에 대해 생각한다는 의미다. 정보 보안 인식, 지식 및 경험은 의식적인 행동에 큰 영향을 주며 이를 괘념행동이라고 한다. 이에 정보 보안 관리에 있어서 의식적이지 않은 행동을 하게 되면 다음과 부정적인 결과를 초래할 수 있다.[9] 먼저, 팝업 차단 기능, 안티 스파이웨어 및 안티 바이러스 소프트웨어와 같은 보안 소프트웨어 및 기능에서 이러한 맹점이 발생할 가능성이 높다. 둘째, 컴퓨터 및 인터넷 사용과 관련된 보안 의식이 있는 행동의 중요성을 간과할 수 있다.

결과적으로, 전문가들은 정보 보안의 기술 측면만으로 안전한 환경을 보장 할 수 없으며 인간의 요소에 주목하고 있으며, 이러

7) S. L. Pfleeger, & D. D. Caputo(2012: 6~7).

8) 허성호·이려화(2017), 『교양인을 위한 심리학 연구』, 솔과학, 44~5쪽.

9) H. Rhee, C. Kim, & Ryu, Y. U.(2009), "Self-efficacy in information security: Its influence on end users' information security practice behavior", *Computer Security*, 28(8), pp. 818~9.

한 관점은 정보 보안의 의식적인 행동에 주목하고 이를 보안행동으로 적극 고려해야 한다고 주장한다.[10]

4. 정보 보안의 인적 요소 모델

정보 보안 영역에서 인적 요소의 중요성은 아무리 강조해도 모자라는 상황이다. 정보 보안 관리는 사용자와 사용자의 인식을 통해 안전한 환경을 유지하는 중요한 요소라는 점에서 충분히 고려되어야 한다. 즉, 사용자는 보안 개념의 가장 핵심이 된다. 인간의 행동에 주목하여 사이버 보안 위험을 완화하고 방지하는 것은 여러 단계로 구현되어야 하며 행동 과학에서는 웹 시스템의 설계, 개발 및 유지 관리 단계에서 중요한 시사점을 안고 있다.[11] 사용자는 사이버 사건에 대한 적절한 대응이 없을 때 보안의 장애 요소로 간주한다. 보안 구현에 어려움을 겪고 보안을 잘못 해석하거나 불신하거나 무시할 수 있다는 의미이다.[12] 즉, 사용자의 태도와 저항 행동은 필수 암호 변경에 직면 했을 때 유동적인 특성을 지닌다. 연구자들은 그러한 유동적 태도가 의도적으로 지연되고 불필요한 침해로 이어진다는 것을 지적하고 있다. 암호에 대한 보안의식이 약화되면 심각한 결과를 초래할 수 있지만 사용자의 보안 정책 구현에 대한 태도는 쉽게 바뀌지 않는 경향이 있다.[13] 의도적으로 혹은 부주의로 사용자는 정보 보안 행동을

10) S. Furnell, & N. Clarke(2012), "Power to the people? The evolving recognition of human aspects of security", *Computer Security*, 31(8), pp. 985~6.

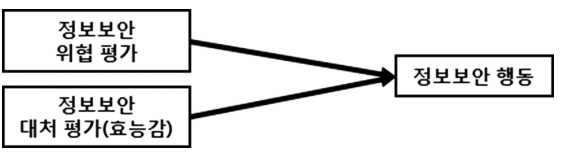
11) K. Padayachee(2012), "Taxonomy of compliant information security behavior", *Computer Security*, 31(5), pp. 676~8.

12) J. Cox James(2012), "Information systems user security: a structured model of the knowingedoing gap", *Computer and Human Behaviour*, 28(5), pp. 1850~2.

게을리하게 되고, 이것은 심각한 주요 문제인 조직의 정보 보안을 위협하는 결과를 초래할 수도 있다. 따라서 본 연구는 사용자의 행동을 정보 보안 영역의 의식 행동으로 강화하는 전략 구상을 목표로 하고, 이에 적합한 세 가지 유형의 모형을 소개하고자 한다.

4.1. 개인의 정보 보안 전략

보호 동기 이론(Protection Motivation Theory, PMT)은 보호 행동에 참여하려는 사용자의 의도를 예측하는 가장 강력한 설명 이론 중 하나이다.[14] 이 이론은 위협적 메시지는 위협에 대한 평가(threat appraisal)와 대처에 대한 평가(coping appraisal)라는 두 가지 인지적 과정을 통해 태도 변용의 효과를 유발한다고 설명하였다.[15] 즉, 위협적 메시지의 영향을 인지적으로 평가하는 정도를 개념화하는 부분과, 그 상황에 대한 적응 혹은 극복을 위한 대처에 관련된 인지적 평가로 구분하여 설명할 수 있다(그림 1 참조).



〈그림 1〉 정보보안에 적용되는 보호 동기 이론

13) J. M. Stanton, K. R. Stam, P. Mastrangelo, & J. Jolton(2005), "Analysis of end user security behaviors", *Computer Security*, 24(2), pp. 125~7.

14) C. L. Anderson, & R. Agarwal(2010), "Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions", *MIS Q*, 34(3), pp. 613~43.

15) C. Roser, & M. Thompson(1995), "Fear appeals and the formation of active publics", *Journal of Communication*, 45(1), pp. 103~22.

위협에 대한 정보는 위험인지에 주안점을 두어 위협적인 자극에 대한 보호 동기의 유발 관점에서 여러 연구에 적용되었다. 공포에 대한 호소력과 개인이 어떻게 대처할 수 있는지 이해하기 위해 이 이론을 적용할 수도 있다. 인지적 처리와 기대 가치 이론은 이 이론의 기본적인 접근을 같이하는 대표적인 이론들이다.[16]

위협 감정과 대처 감정은 이 이론의 두 가지 주요 개념이다. 먼저, 위협 평가는 사용자의 정보 보안 측면에서 부주의한 태도로 인한 위험 수준 평가와 관련이 있고, 이 위험은 정보의 가용성, 무결성 및 기밀성을 위협 할 수 있다. 또한, 위험의 감지된 취약성과 심각성은 위협 평가의 두 가지 중요한 부분이 된다. 둘째, 대처 감정은 위험이나 위협에 대처할 수 있는 사용자의 능력을 나타내는데 자기효능감의 개념이 적용된다.[17] 자기효능감이란 권장 행동에 대처하거나 수행 할 수 있는 능력을 의미하는데, 일부 연구들의 맥락에서 정보 보안 위반의 위험이 최소화되는 방식으로 사용자의 자기효능감이 보안 행동을 긍정적으로 수용하는 것으로 나타났다.[18]

한 연구에서는 정보 보안 조직 정책의 준수행동이 사용자의 행동 위험을 감소시키는 방법을 보여주기 위해 PMT를 적용했다.[19] 즉, 이 이론은 사용자가 조치를 취하기 전에 정보 보안 측

16) R. W. Rogers(1983), "Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation", New York: Guilford Press, pp. 142~8.

17) M. I. Woon, A. Kankanhalli(2007), "Investigation of IS professionals' intention to practise secure development of applications", *Int J Hum Comp Stud*, 65(1), pp. 32~4.

18) P. Ifinedo(2014), "Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition", *Inf Manag*, 51(1), pp. 71~3.

19) M. I. Woon, A. Kankanhalli(2007: 35~6).

면에서 그들의 방식의 결과에 대해 생각하고 발생할 수 있는 손상 및 비용 수준을 고려하면 신중하게 행동한다는 것을 보여주었다. 따라서 보호 동기 이론에 기반한 개인의 행동은 정보 보안 위협 평가하는데 중요한 영향을 미치고, 이는 정보 보안 행동으로 이어진다는 것을 나타낸다. 이 과정에서 실제로 컴퓨터 능력이 반영되는 자기효능감의 영향력도 상당한 것으로 나타났다.

4.2. 조직의 정보 보안 전략

대부분의 조직 기능은 정보 보안 시스템(ISS, Information Security System)에 크게 의존한다. 그리고 보안 위협과 관련된 위험 관리는 정보 보안 위반이 기업 및 고객에게 심각한 재정적 및 명성을 가져올 수 있으므로 점점 더 중요해지고 있다.[20] 이에, 정보 보안을 보장하는 것이 조직의 우선순위이며 중요한 과제 중 하나가되었다.

학계와 기업은 정보 보안 시스템(ISS) 위협을 효과적으로 줄일 수 있는 방법에 관심을 가지고 있다.[21] 조직이 정보 보안을 위해 기술 솔루션을 계속 사용하고 있지만 일화적이고 경험적인 증거는 사건의 수와 심각도가 인간 요소에 기인되는 사례가 점점 증가하고 있음을 나타내고 있다. 조직의 기존 정보 보안 추세와 마찬가지로 ISS에 대한 이전 연구는 주로 암호화 기술, 스파이웨어 및 바이러스 탐지 또는 방화벽과 같은 기술적 문제에 집중되었던

20) H. Cavusoglu, B. Mishra, & S. Raghunathan(2004), "A Model for Evaluating IT Security Investments", *Communications of the ACM*, 47(7), p. 88.

21) J. D'Arcy, A. Hovav, & D. Galletta(2009), "User awareness of security countermeasures and its impacton information systems misuse: A deterrence approach", *Information Systems Research*, 20(1), pp. 81~4.

것이 사실이다.[22]

실제로 조직에서는 전체 ISS 사건의 50~70%가 순진한 실수에서부터 고의적인 해악에 이르기까지 직간접 적으로 발생한다고 전제하고 있는 실정이다.[23] 그러므로 정보 보안을 향상시키기 위해서는 기술 및 사회 및 조직 자원에 대한 인성적 차원의 정보 보안 전략에 대한 투자가 필요하다.[24] 이러한 배경에서 최근의 연구들은 정보 보안에서 가장 약한 링크로 간주되는 정보 사용자의 행동에 영향을 미치는 조직적, 환경적, 개별적인 요인에 초점을 옮기는 분위기다.[25] 선행 연구에 따르면 증가하는 직원의 정보 보안 의식(Information Security Awareness, ISA)은 정보 보안 정책(Information Security Policy, ISP)의 준수 행동에 매우 긍정적 인 영향을 미치는 것으로 나타났다.[26] 또한 관리자는 충분한 수준의 ISA를 설정하는 것이 보안 관리의 우선순위 중 하나라고 주장하였다. 이와 관련하여 보안 관리는 직원이 행동의 정보 보안에 대한 잠재적 파급 효과를 인식하고 조직 IS 리소스를 책임 있게 사용할 수 있는 자격을 부여하는 것을 말한다(NIST, 2003).[27]

ISA의 중요한 역할이 널리 인식되고 있지만 ISA에 영향을 미치는 요소에 대한 이해는 거의 없다. 이에, 정보 보안 인식으로 이어

---

22) J. L. Spears, & H. Barki(2010), "User participation in information systems security risk management", *MIS Quarterly*, 34(3), pp. 510~2.

23) M. Siponen(2000), "A conceptual foundation for organizational information security awareness", *Information Management and Computer Security*, 8(1), pp. 32~5.

24) B. Bulgurcu, H. Cavusoglu, & I. Benbasat(2010), "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, 34(3), pp. 524~6.

25) B. Bulgurcu, H. Cavusoglu, & I. Benbasat(2010: 525~7).

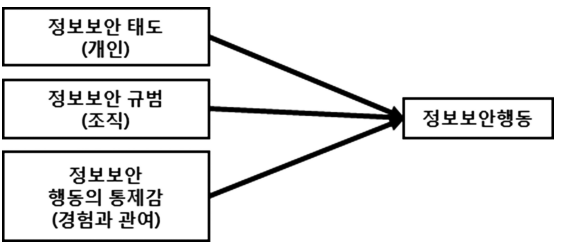
26) J. D'Arcy, A. Hovav, & D. Galletta(2009: 85~6).

27) NIST(2003), "Building an information technology security awareness and training program", M. Wilson(eds.), *Gaithersburg: National Institute of Standards and Technology*, NIST Special Publication, pp. 822~30.

지는 요인을 파악하는 것이 학계에 중요한 공헌이 될 것이라고 주장이 나타났다.[28] 왜냐하면 이 요소를 사용하여 실무자뿐만 아니라 이 방향의 맥락에 차이가 있는 다양한 정보 보안 인식 프로그램에 중요한 기반을 마련하는 근거를 제공하기 때문이다.

4.3. 조직과 개인의 상호작용 전략

아첸(Ajzen)은 개인적 태도, 사회적 규범, 그리고 행동 통제가 개인의 행동에 미치는 영향을 설명하기 위해 계획된 행동 이론(Theory of Planed Behaviour, TPB)을 제안했다.[29]



〈그림 2〉 정보보안에 적용되는 계획된 행동 이론

TPB는 개인의 행동을 예측하기 위해 다양한 연구에 널리 적용되고 있으며, 정보보안에도 적용이 가능한 이론이다. 특히, 개인의 동기에 해당하는 태도와 사회조직적 맥락에 해당하는 주관적 규범은 이성적 행동 모형으로 설명이 되며, 여기에 경험과 관여도를 반영한 지각된 행동 통제 요소를 추가한 모형을 정보 보안에 대입하여 계획된 행동모형으로 설명하였을 때, 다음과 같은

28) B. Bulgurcu, H. Cavusoglu, & I. Benbasat(2010: 524~5).

29) I. Ajzen(1991), "The Theory of Planned Behavior", *Organizational Behavior and Human Decision Processes*, 50(2), 179~211.

의미로 해석될 수 있다(그림 2 참조).

첫째, 그 구성 요소들 중에 태도는 특정 행동에 대한 사용자의 긍정적이거나 부정적인 느낌을 말하며 특정 방식으로 사물을 평가하는 학습 된 경향으로 정의된다. 평가는 사물, 이슈, 사람 또는 사건에 대해 긍정적이거나 부정적 일 수 있다. 평가가 바뀌면 태도와 연관되며 결과적으로 행동이 바뀐다. 태도는 또한 암묵적이거나 현시적일 수도 있다. 현시적인 태도에서 우리는 사회적 신념과 행동에 영향을 미치는 의식적으로 인식하고 있다. 대조적으로 암묵적 태도는 우리의 행동과 신념에 무의식적으로 영향을 미친다. 즉, 인간의 지식은 자신의 태도에 직접적인 영향을 미친다. 이 효과는 직접적인 개인적인 경험이나 관찰 결과에 기인하며, 다양한 훈련 방법은 특정 문제에 대한 우리의 태도를 변화시킨다.[30] 이에, 위험에 대한 정보 보안 인식은 사용자의 행동 태도에 영향을 미친다.

둘째, 이 연구에서 제시된 모델은 주관적인 정보 보안 의식이 정보 보안 행동 측면에서 주의 깊은 태도에 영향을 미치는 것을 보여주고 있다. 여기서 주관적인 규범은 개인에게 있어서 행동을 수행하거나 수행하지 않겠다는 사회적 압박으로 이어지고, 사람들이 생각할 때 그들이 중요하다고 생각하는 것에 대한 당사자 관점의 인식을 의미하는 것이다. 즉, 개인적인 측면에서의 상사, 부서장, 관리자는 조직에 정보 자산의 중요성 때문에 정보 보안 정책이 중요한 인물이 될 수 있고, 이는 조직적 요소로 작용하는 것이다.

셋째, 정보 보안 조직 정책이 주관적인 규범에 의식적인 행동

30) J. Abawajy(2014), "User preference of cyber security awareness delivery methods", *Behav Inf Technol*, 33(3), pp. 237~9.

방식의 영향을 받는다고 예측할 수 있다. 이는 지각된 행동통제의 영향력으로 정보 보안 행동이 작용할 수 있다는 점을 시사한다. 지각된 행동통제란 개인이 인식하는 특정 행동의 용이함 또는 어려움을 의미한다. 사용자의 경험과 참여 정도는 신중한 태도를 거쳐 정보 보안 영역에서 어려운 작업이 아니라는 사용자의 인식에 영향을 주게 된다. 따라서 정보 보안은 이 세 가지 요인들로 구성된 계획된 행동 이론에 기초한 개인의 행동에 미치는 영향을 보여줄 수 있다.

따라서 이러한 관점에서 태도, 주관적 규범 및 행동 통제가 정보 보안 조직 정책을 준수하겠다는 사용자의 의도에 영향을 미친다는 사실을 알 수 있다.[31]

5. 결론

현재, 사회 및 경제 생활에서 IT 기술의 급속한 발전과 폭 넓은 적용은 사람들이 네트워크 정보 시스템에 대한 의존성을 더욱 강력하게 만들고 네트워크 정보 보안 기술의 요구가 점점 더 강력 해지고 있다. 이에, 정보 보안의 성공여부는 사회적 기술 시스템의 일종인 정보 보안 기술 시스템이 성공을 거둘 수 있을지 여부는 발전과 전문성에 따라 결정될 뿐만 아니라 사용자의 인식과 수용 태도에 달려있다는 점을 인식해야 한다. 이에 본 연구는 사용자의 행동 관점에서 정보 보안 기술의 적용 요소를 세 가지 관점에서 조직적 요소와 사용자 행동 간의 관계를 파악하며 정보 보안 기술의 설계 및 실제 사용에 매우 중요하다는 점을 제시하

31) P. Ifinedo(2014: 75~6).

였다.

이에 본 연구에서는 정보 보안을 위해 인성적 요소에 주목해야 한다는 점을 알 수 있다. 이에 앞으로 정보 보안 기술 연구 측면에서 볼 때, 정보 보안 기술의 인간 요소의 영향력 요인에 주목해야 하며 다음의 몇 가지 논의점을 제시한다.

첫째, 지각된 정보 보안의 유용성을 제고해야 한다. 지각된 유용성은 사용자에게 유용하고 경제적인 한 가지 기술을 사용하여 의도를 가져 오는 것을 주관적으로 평가한 결과이다.[32] 이는 주관적인 판단에 의해 결정되는 부분이기 때문에 인식된 정보 보안의 유용성 수준이 높을수록 사용자의 정보 보안 행동은 증가할 것으로 예측할 수 있다.

둘째, 인식된 정보 보안 행동 사용 편의성을 고려해야 한다. 실제 사용자가 사용하기 쉽다는 것이 인식되면 기술이 개별 사용자에게 긍정적인 행동전략 양식을 수용되고 이는 결과적으로 정보 보안 기술을 선택할 가능성을 높일 것이다.

셋째, 사회적 영향력이 있다는 점을 간과해서는 안 된다. 사용자의 가족, 친구, 동료, 네트워크 포럼 및 네트워크 사회와 같은 주변 그룹 및 환경이 개인의 정보 보안 행동에 영향을 미칠 수 있다. 즉, 친밀한 대상 누군가에 의해 보안 위반 행동이 유도 될 수도 있는 것이다. 따라서 정보 보안 행동은 개인의 조건부 의식화 전략이 놓치는 부분을 고려할 때, 사회적 영향력의 요인에 주목할 필요가 있는 것이다.

넷째, 조직이 제공하는 정보 보안 기술을 신뢰하는 태도를 형성하는데 관심을 가져야 한다. 정보 보안의 기술적 효과는 사용

32) G. Furong(2010), "The New Evolution of Research Information Technology Acceptance Models", *Journal of Information*, 29(6), pp. 94~5.

자가 느끼는 특정 기술의 실행과 그 효율성을 의미한다. 정보 보안 기술의 뚜렷하고 효과적인 기능을 제공하는 정보 보안 기술을 선택할 때 기술 효과가 포함되며 사용자는 조직적 지원에 대한 적극 수용의지가 필요한 것이다.[33] 따라서 인지적 필요성의 증가로 사람들은 기술에 대해 요구도가 높아지고, 실제 제공되는 기술의 유용성의 인식이 긍정적일수록 사용자의 정보 보안 행동 의도는 증가하게 될 것이다.

다섯째, 컴퓨터를 사용할 때 적용되는 컴퓨터 자기효능감의 정도를 고려해야 한다. 컴퓨터 자기효능감이란 컴퓨터를 사용하여 목표를 달성하는 능력에 대한 자기 인식을 의미한다. 즉, 정보 보안은 대부분 컴퓨터를 활용하는 상황이 많다. 이에, 컴퓨터 자기효능감이 보안 기능을 광범위한 작업 분야에 사용할 수 있는지 여부에 대한 긍정적인 판단과 관련이 있다.

여섯째, 인지적으로 추산된 물적 심적 비용을 낮추어야 한다. 경제 및 비용 의도는 항상 정보 기술 채택 연구의 중심이며 비용은 대개 채택 행동의 주요 영향 요인 중 하나이다. 사용자는 정보 보안 기술 서비스 공급 업체가 제시 한 심리적 비용에 대해 서로 다른 태도를 취하고 있는지를 파악하고, 이를 해소하는 전략을 구사해야 한다.

마지막으로 개인 혁신적 태도를 함양하도록 독려한다. 개인 혁신은 새로운 생각을 받아들이고 혁신의 결정을 내리는 개인 사용자의 수준이며, 사회 시스템에서 다른 사람들보다 먼저 채택되는 개인 혁신 능력을 의미한다.[34] 따라서 개인의 혁신은 개인에게

33) A. Venkatesh, M. G. Morris, & G. B. Davis(2003), "User acceptance of information technology: Toward a unified view", *MIS Quarterly*, 27(3), pp. 455~60.

34) Z. Honghong, G. Dongling and X. Jili(2010), "An Empirical Study of Adoption-willingness of Innovative Technology Product Based on TAM Model", *Science &*

새로운 기술 수단을 배우고, 이 기술을 사용하여 더 많은 기술적인 기능을 찾고, 습관을 이용하여 개발하는 데 유익하며, 개인 혁신이 높을수록 대중적인 정보 보안 기술의 적용이 용이하게 될 것이다.

Technology Progress and Policy, 27(18), p. 3.

참고문헌

허성호·이려화(2017), 『교양인을 위한 심리학 연구』, 솔과학.

A. Venkatesh, M. G. Morris, & G. B. Davis(2003), "User acceptance of information technology: Toward a unified view", *MIS Quarterly*, 27(3), pp. 425~78.

B. Bulgurcu, H. Cavusoglu, & I. Benbasat(2010), "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, 34(3), pp. 523~48.

C. L. Anderson, & R. Agarwal(2010), "Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions", *MIS Quarterly*, 34(3), pp. 613~43.

C. Roser, & M. Thompson(1995), "Fear appeals and the formation of active publics", *Journal of Communication*, 45(1), pp. 103~22.

G. Furong(2010), "The New Evolution of Research Information Technology Acceptance Models", *Journal of Information*, 29(6), pp. 93~99.

H. Cavusoglu, B. Mishra, & S. Raghunathan(2004), "A Model for Evaluating IT Security Investments", *Communications of the ACM*, 47(7), pp. 87~92.

H. Rhee, C. Kim, & Ryu, Y. U.(2009), "Self-efficacy in information security: Its influence on end users' information security practice behavior", *Computer Security*, 28(8), pp. 816~26.

I. Ajzen(1991), "The Theory of Planned Behavior", *Organizational*

Behavior and Human Decision Processes, 50(2), pp. 179~211.

ISACA(2009), "An Introduction to the Business Model for Information Security", *Rolling Meadows*, IL: ISACA.

J. Abawajy(2014), "User preference of cyber security awareness delivery methods", *Behav Inf Technol*, 33(3), pp. 236~47.

J. Cox James(2012), "Information systems user security: a structured model of the knowingedoing gap", *Computer and Human Behaviour*, 28(5), pp. 1849~58.

J. D'Arcy, A. Hovav, & D. Galletta(2009). "User awareness of security countermeasures and its impacton information systems misuse: A deterrence approach", *Information Systems Research*, 20(1), pp. 79~98.

J. L. Spears, & H. Barki(2010), "User participation in information systems security risk management", *MIS Quarterly*, 34(3), pp. 503~22.

J. M. Stanton, K. R. Stam, P. Mastrangelo, & J. Jolton(2005), "Analysis of end user security behaviors", *Computer Security*, 24(2), pp. 124~33.

K. Padayachee(2012), "Taxonomy of compliant information security behavior", *Computer Security*, 31(5), pp. 673~80.

M. I. Woon, A. Kankanhalli(2007). "Investigation of IS professionals' intention to practise secure development of applications", *Int J Hum Comp Stud*, 65(1), pp. 29~41.

M. Siponen(2000), "A conceptual foundation for organizational information security awareness", *Information Management and Computer Security*, 8(1), pp. 31~41.

N. S. Safa, & M. A. Ismail(2013). "A customer loyalty formation model in electronic commerce", *Econ Model*, 35, pp. 559~64.

NIST(2003), "Building an information technology security awareness and training program," M. Wilson(eds.), *Gaithersburg: National Institute of Standards and Technology*, NIST Special Publication, pp. 800~50.

P. Ifinedo(2014), "Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition", *Inf Manag*, 51(1), 69~79.

PCI(2014), "Information Supplement: Best Practices for Implementing a Security Awareness Program", PCI SSC Standard, pp. 19~25.

R. W. Rogers(1983), "Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation." New York: Guilford Press, pp. 142~68.

S. Furnell, & N. Clarke(2012), "Power to the people? The evolving recognition of human aspects of security", *Computer Security*, 31(8), pp. 983~8.

S. L. Pfleeger, & D. D. Caputo(2012), "Leveraging Behavioral Science to Mitigate Cyber Security Risk", *Computers & security*, 31(4), pp. 597~611.

Z. Honghong, G. Dongling and X. Jili(2010), "An Empirical Study of Adoption-willingness of Innovative Technology Product Based on TAM Model", *Science & Technology Progress and Policy*, 27(18), pp. 203~10.

Abstract

Exploratory research of information security strategy focused on human factors

Lee Ryowhoa & Hwang Inho & Hu Sungho

Keywords: information security, protection motivation theory, information security system, theory of planned Behaviour, information security awareness

This study focused on human behavior of threatening information security. Until now, it has been overly focused on technical factors. And many studies support the fact that information security awareness which is human element that cause information security problems are increasing. Three research models focusing on human behavior (individual perspective, organization perspective, personal/organizational interaction perspective) were proposed. First, information security in the individual perspective is explained by the protection motivation theory. Second, information security in the organizational perspective is explained by the information security system theory. And the perspective of individual / organization interaction is explained by theory of planned Behaviour. And some suggestions are about human behavior control. The factors of behavior control include the importance of security, usability, social influence, information security technology trust, computer self - efficacy, cognitive cost, and individual innovation.

이 논문은 2017년 11월 10일에 투고 완료되어 2017년 12월 7일부터 12월 17일까지 심사위원이 심사하고 2017년 12월 27일에 심사위원 및 편집위원 회의에서 게재 결정된 논문임.