융합보안 강화를 위한 정보보안 정책 효과성 측정도구 개발

임명성
삼육대학교 경영학과

Development of Measures of Information Security Policy Effectiveness To Maximize the Convergence Security

Myung-Seong Yim
Dept. of Business Administration, Sahmyook University

요 약 정보보안 정책은 산업융합의 흐름에 맞추어 융합보안시대가 가속화되어가고 있는 요즈음 조직의 보안을 실현하고 지속하는데 필요한 가장 중요한 도구 중 하나이다. 하지만, 지금까지도 정보보안 정책의 효과성을 측정하는 연구는 많이 부재한 실정이다. 본 연구의 목적은 정보보안 정책의 효과성을 측정할 수 있는 측정지표를 개발하는 것이다. 이를 위해 데이터 품질, 정보 품질에 관한 문헌을 기반으로 품질의 기반 요인들을 살펴보았다. 문헌 검토 결과 내용 관점에서 정확성, 완전성, 해석의 용이성, 관련성 등을 그리고 형식 관점에서 이해의 용이성, 표현의 간결성, 그리고 적정성 등이 정보보안 정책의 품질을 측정하기 위해 중요한 구성요소라 판단된다.

• Key Words : 정보보안, 보안 정책, 정책 효과성, 융합, 측정

Abstract The information security policy is one of the most important tools for organization to manage the implementation and ensure the organizational security. However, we do not have metrics for measuring its effectiveness. The ultimate purpose of this study is to develop the measures of information security policy effectiveness. To do this, this study review data quality and information quality literatures and investigate appropriate subfactors for information security policy. Rooted in these concepts, we suggest accuracy, completeness, interpretability, and relevance from content aspect and understandability, concise representation, and amount from form aspect as factors for information security policy effectiveness.

• Key Words : Information Security, Security Policy, Policy Effectiveness, Convergence, Measures

1. 서론

2013년 6월 KCB(코리아크레딧뷰로) 신용평가사 직원 한 명이 카드사로 파견을 나가 주요 카드사인 국민, 롯데, 농협카드 사의 고객 개인정보를 USB에 담아 대출공고업자와 대출모집인 대량으로 유출시키는 사고가 있었다. 그러나 카드사는 7개월 동안 이를 인지하지 못하고 2014년 1월에 이르러서야 알게 되었다. 이 사고로 2014년 대한민국 사상 가장 많은 고객 개인정보가 유출되는 사건으로 기록되었으며, 유출된 개인정보만 1억 4000만 건에 달하는 것으로 밝혀졌다. 이와 유사하게 2012년 7월 KT 가입자 870만 명의 개인정보가 해커 2명이 만든 고객정보를 몰래 조회하는 프로그램을 통해 유출되었으나 KT는 5개월간 유출 사실을 파악하지 못했었다.

해외에서도 정보유출 사고는 빈번하게 발생하고 있는데 일례로 최근에 미국 영화사 소니 픽처스 엔터테인먼트의 컴퓨터 해킹 사고로 유출된 개인정보에는 영국 베아트리스 공주의 신상정보도 포함된 것으로 나타났다.

*교신저자 : 임명성(msyim@syu.ac.kr)
접수일 2014년 9월 22일 수정일 2014년 12월 1일 게재 확정일 2014년 12월 14일

유출된 정보는 이름과 거주지, 급료 등을 포함한 직원 신상명세서 내용 등이다. 또한 이번 사고로 유명 배우와 직원 등 4만 7000명의 개인정보가 유출됐다.

주목할 점은 해외의 경우 여러 가지 경제적 거래를 위해 요구하는 정보가 국내에 비해 상대적으로 적다. 하지만 최근에 다양한 예방책이 시행되고 있기는 하나 지금까지 국내의 많은 기업들은 지나치게 많은 개인정보를 요구해왔기 때문에 저장된 정보의 상대적 가치가 매우 낮아 허술하게 관리되어 와서 정보유출 사고는 어느 나라보다도 심각하다.

최근 Trend Micro의 시장 조사 결과에 따르면 2014년 3분기까지 전 세계 데이터유출사고 중 한국에서 가장 많은 정보 유출 사고가 발생한 것으로 나타났다. 국내에서 유출된 개인정보는 2억 2000만 건에 달했다[16].

일반적으로 조직 내에서 정보의 유출을 위해 사용되는 조치는 기술적 접근법과 관리적 접근법이 사용된다. 기술적 접근법은 접근권한 관리, 비밀번호 관리, 접근통제 시스템 설치 및 운영, 암호화, 접속기록 보관 및 관리 등이 있으며, 관리적 접근법으로는 보안 프로그램 설치 및 운영, 수집/이용 동의 획득, 개인정보처리방침 작성 및 공개, 파기, 프로그램 유지보수 등이 있다.

하지만 이러한 조치에도 불구하고 정보보안의 가장 큰 위협이 되고 있는 것은 내부인에 의한 위협이다[9,15]. 2014년 11월 우체국 직원이 고객의 개인정보를 임의로 제3자에게 유출한 사건이 발생하였다. 비슷한 시기에 경기 지역 일선 파출소에 전화를 걸어 경찰을 사칭하며 주민 개인정보를 빼낸 피의자가 전직 경찰로 드러난 사건도 있었다. 이러한 사건은 국내에만 한정된 것은 아니다.

미국 중앙정보국(CIA)도 내부자의 위협에 노출된 사건이 2013년에 발생했다. 에드워드 스노든은 미 국가안보국(NSA)이 세계를 불법 감청했다고 폭로했다. 그는 NSA와 계약한 컨설팅 회사의 시스템 관리자로 관리자 권한을 이용해 NSA 공유폴더에 있는 수많은 기밀문서에 접근했다. 같은 해 미국의 전직 국세청(IRS) 직원이 백악관에 보수단체 및 관련 인사에 대한 중요한 세무 정보를 유출한 것으로 알려지기도 했다.

따라서 아무리 기술적 요인이 잘 마련되어 있다하더라도 이를 사용하게 되는 내부 구성원들의 정보보안에 대한 의지가 확고하지 못할 경우 조직에서 마련한 대안들이 제대로 효과를 발휘할 수 없기 때문에 인적요인에 대한 고려가 우선시 되어야 한다[2,8].

내부인의 정보보안 사고를 줄이기 위해 필요한 조치는 조직적으로 모든 구성원들이 정보보안 정책을 준수하도록 유도하는 것이다. 대부분의 보안 사고는 조직원들이 조직 내의 정보 보안 정책을 준수하지 않음으로 인해 발생한다[15].

여기서 정보 보안 정책이란 보안을 위한 기대사항들을 명확하고, 구체적이며, 측정 가능한 목표와 준수조항들로 기술해 놓은 문서를 말한다[2].

보안정책은 이를 준수하는 사용자의 관점에서 접근하는 것이 중요하기 때문에 보안정책의 효과성에 대해 이해해야 한다. 왜냐하면 보안정책이 기술적인 전문용어와 장황한 문장으로 작성되어 있는 경우 조직원들은 이를 읽어보려는 시도보다는 부담감과 거부감을 느낄 수 있다[2]. Herath and Rao(2009)도 조직 구성원들이 보안정책을 준수하는데 있어서 불편함이 따르기 때문에 조직 내 정보보안 정책을 제대로 준수하지 않는다고 주장하였다. Chan et al.(2005)은 정보보안 정책의 준수가 업무 생산성과 일부 상충되기 때문에 보안 정책을 준수하도록 유도하는데 어려움이 있다고 주장하였다. 따라서 조직의 정보보안 정책을 이를 준수해야 하는 당사자들인 조직 구성원들의 관점에서 효과적으로 수립해야 한다. 그러나 보안정책이 효과적인가에 대한 의문은 여전히 답을 찾지 못하고 있다[12]. 이로 인해 조직 구성원들에게 정보보안 정책이 비효과적이고, 불필요하고, 준수해야 할 의무도 느끼지 못하게 하며, 업무생산성의 장애요인으로 느껴지기도 한다[4,12]. 따라서 본 연구는 정보보안 정책의 효과성을 평가할 수 있는 지표를 개발하고자 한다. 본 연구에서 제시하고자 하는 지표의 특징은 사용자 관점에서 평가할 수 있는 지표라는 점이다. 기존의 정보보안 정책은 정책 입안자들에 의해 개발되고 유지/보수되어 왔다. 따라서 이를 준수해야 하는 조직 내 전 계층에 적합한 것은 아니라는 비판을 받아왔다. 이를 해결하기 위해서는 준수자들의 평가 과정을 통해 정보보안 정책을 수정 및 개선하는 것이다. 하지만 여전히 관련 연구 및 지표가 명확히 제시되지 못하고 있다는 문제점이 있다.

본 연구는 이러한 문제점을 인식하여, 정보보안 정책의 효과성을 평가할 수 있는 지표를 제안하고자 한다. 이를 위해 데이터 품질 및 정보 품질관련 문헌을 검토하였다. 선행연구에서는 오직 데이터 품질에서 정보보안 정책의 효과성을 측정할 수 있는 지표를 제시하였으나[12], 본 연구에서는 이를 확정하여 정보 품질의 관점도 반영

하였다. 그 이유는 문서화된 정책은 결국 정보로 볼 수 있기에 이러한 관점에서 정보 품질은 정보보안 정책의 효과성을 위한 측정지표 개발에 중요한 기반연구가 될 수 있다[12].

2. 문헌 연구

정보보안 정책은 명확하고(clear), 구체적이고(specific), 측정가능(measurable)해야 한다[1,12]. 본 연구에서는 정보 보안 정책의 품질을 측정하기에 적절한 지표를 개발하기 위해 데이터 품질과 정보 품질 문헌을 살펴보았다.

2.1 데이터 품질

Wang and Strong(1996)은 데이터 품질은 크게 4가지 카테고리로 구분하였다. 그들이 제시한 카테고리는 1) 내재적 품질(intrinsic quality, content quality), 2) 상황적 품질(contextual quality), 3) 표현성(representation), 4) 접근성(accessibility) 등이다[5,11]. 각각의 품질은 세부적 차원을 동반한다. 내재적 품질은 정확성(accuracy), 객관성(objectivity), 신뢰 가능성(believability), 명성(reputation) 등을 포함한다[3]. 상황적 품질은 관련성(relevance), 가치성(value-added), 적시성(timeliness), 완전성(completeness), 적정성(amount of data) 등을 포함한다[3]. 표현성은 해석의 용이성(interpretability), 이해의 용이성(ease of understanding), 표현의 간결성(concise representation), 표현의 일관성(consistency representation) 등을 포함한다[3]. 접근성은 접근의 용이성(accessibility), 접근의 안전성(access security) 등을 포함한다[3].

Wand and Wang(1996)은 다양한 문헌 조사를 통해서 Wang and Strong(1996)이 제시한 방대한 데이터 품질 차원들의 중요성을 인용횟수를 이용하여 분석하였는데, 분석결과 정확성(accuracy, 25회 인용, 참조의 오류)이 가장 중요한 것으로 나타났으며, 다음으로 신뢰성(reliability, 22회 인용, 에러나 실패를 예방할 수 있는 확률과 산출된 정보의 일관성), 적시성(timeliness, 19회 인용, 필요할 때 정보가 제공되는가), 관련성(relevance, 16회 인용, 데이터를 업무의 모든 상황에 적용할 수 있고 도움이 되는가), 완전성(completeness, 15회 인용, 필요한 모든 내용이 포함되어 있는가), 현실성(currency, 9회 인용, 최근에 주어진 내용인가), 일관성(consistency, 9회 인용, 동일한 내용을 산출하는가) 순으로 나타났다(나머지는 5회 이하)[5,19]. Pipino et al.(2002)은 그동안 개발된 데이터 품질 평가 지표가 산발적으로 개발되어 사용된 것이 많다고 지적하면서 보편적 지표로 사용될 수 있는 15개의 데이터 품질 평가 차원을 제시하였다. 15가지 차원은 접근성(accessibility), 적정성(appropriate amount of data), 신뢰성(believability), 완전성(completeness), 간결성(concise representation), 일관성(consistent representation), 조작의 편의성(ease of manipulation), 낮은 오류(free-of-error), 해석의 용이성(interpretability), 객관성(objectivity), 관련성(relevancy), 명성(reputation), 보안(security), 적시성(timeliness), 이해의 용이성(understandability), 가치성(value-added) 등이다. 15가지 차원에 대한 구체적인 평가지표는 Lee et al.(2002)에 의해서 제시되었다.

2.2 정보 품질

정보품질(information quality)이란 정보시스템에 의해 제공되는 결과물(output)의 특성을 말하는 것으로 정확성(accuracy), 적시성(timeliness), 완전성(completeness) 등이 해당된다[13].

Chae et al.(2002)는 Wang and Strong(1996)의 네 가지 데이터 품질 차원을 기반으로 모바일 인터넷의 정보품질을 측정하기 위한 지표를 제안하였는데 이는 접속 품질(connection quality), 내용 품질(content quality), 상호작용 품질(interaction quality), 상황 품질(contextual quality) 등이다. 접속 품질은 모바일 서비스에 어떠한 장애도 없이 안정적으로 접속할 수 있는 정도를 말하다[7]. 내용 품질이란 모바일 서비스를 통해 제공되는 정보의 본질적 가치(inherent value)와 유용성(usefulness)을 의미한다[7]. 상호작용 품질은 모바일 서비스 상에서 쉽고 효율적인 방법으로 상호작용이 이루어지는지를 나타낸다[7]. 상황 품질은 사용자가 존재하는 상황 내에서 모바일 서비스가 제공되고 있는지를 나타내며, 언제 혹은 어디서든 정보에 접근할 수 있는가와 관련된다[7].

3. 정보보안 정책 효과성

정보보안 정책의 효과성은 내용(content)과 형식(form)의 관점에서 평가할 수 있다[12]. 따라서 본 연구에

서도 정보보안 정책의 효과성을 평가하기 위한 지표를 제안함에 있어서 두 가지 관점에서 제시하고자 한다.

3.1 내용(content) 효과성

내용의 효과성은 사용자에게 문서상으로 보이는 정보의 관련성(relevance), 정확성(accuracy), 완전성(completeness) 등으로 평가된다[10]. DeLone and McLean(2003)이 제시한 정보 품질은 전자상거래의 내용적 이슈(content issue)를 반영하고 있다. 이들이 제시한 정보품질의 하위 속성은 개인화(personalization), 완전성(completeness), 이해의 용이성(ease of understanding), 관련성(relevance), 보안(security) 등이다[17]. 이들이 제시한 5개의 하위 차원은 정보시스템의 정보품질을 결정하기 위한 정확성(accuracy), 적시성(timeliness), 완전성(completeness), 관련성(relevance), 일관성(consistency)을 전자상거래 상황에 맞게 수정한 것이다. Gorla et al.(2010)은 정보의 품질을 정보의 내용과 정보의 형식으로 구분하고, 정보의 내용에 정확성, 완전성, 관련성, 일관성을 포함시키고, 적시성은 시스템 품질의 일부라 판단하여 제외하였다. 또한 사용의 편의성과 같은 요소도 시스템 품질을 평가하는 지표라고 주장하고 이를 정보품질 평가요소에서 제외하였다[10].

3.2 형식(form) 효과성

그 동안 정보보안 정책에 관한 연구들은 정책의 내용(content)에 관해 광범위하게 연구를 수행해 왔다[12]. 특히 산업 표준과 가이드라인을 활용한 보안정책의 개발에 많은 연구가 진행되어 왔다[9]. 반면에 보안 정책의 형식에 대한 연구는 거의 부재한 실정이다.

정보보안 정책은 모든 조직구성원들에게 전달되고 읽히고, 이해되어야 한다. 이에 대해 여러 학자들은 정보보안 정책의 형식의 중요성을 강조하였다. Höne and Eloff(2002)는 정책 문서의 작성방법(styling, the manner of writing)의 중요성에 대해 주장하면서, 정책이 조직의 모든 구성원들이 이해할 수 있는 의사소통 스타일로 작성되어야 하며, 사용자 친화적이고, 명확해야 한다고 주장하였다.

Goel and Chengalur-Smith(2010)는 보안 정책의 형식을 평가하기 위한 지표로 3가지를 제시하였는데, 이는 명확성(clarity), 포괄성(breadth), 간결성(brevity) 등이다. 정책의 명확성은 정책의 모호함과 이해하기 쉬운 정도를 나타나고, 포괄성은 정책의 범위(scope, range, coverage)

[Table 1] Measurements for Information Security Policy Effectiveness

Factor	Dimension	Items
Content	Accuracy	The policy is accurate.
		The policy is reliable.
		The policy is correct.
		The policy is incorrect.
	Completeness	The policy protects the organization from the legal consequences of violations.
		The policy specifies the legal ramifications of violations.
		The policy contains all the elements essential to security.
		The policy has sufficient breadth and depth for information security.
	Interpretability	It is easy to interpret what the policy means.
		The policy is difficult to interpret.
		It is difficult to interpret the contents of the policy.
	Relevance	The policy is relevant for decision making.
		The policy is useful in my daily jobs.
		The policy is relevant to my work.
		The policy is appropriate for my work.
		The policy is applicable to my work.
Form	Clarity (Understandability)	The policy is easy to understand.
		The meaning of policy is difficult to understand.
		The policy is easy to comprehend.
		The policy is easy to read.
		The policy represented the information clearly.
		The policy is written using common words and phrases.
		The policy can be understood without reference materials.
	Brevity (Concise representation)	The policy is long.
		The policy is concise.
		The policy represented the information compactly.
		The policy is presented in a compact form.
		The representation of the policy is compact and concise.
		The policy is verbose/wordy.
		The policy is repetitive.
		The policy is comparable to other outputs.
		The policy is good appearance and format.
	Amount	The policy is of sufficient volume for understanding overall organizational security.
		The amount of policy does not match my job requirements.
		The amount of policy is not sufficient for my job requirements.
		The amount of policy is neither too much nor too little.

를 나타내고, 간결성은 정책의 장황함(verbosity)을 나타낸다[12]. 이들은 이러한 3가지 특성이 보안정책의 효과성의 전부가 아니라 필요조건을 제시한 것이라 강조하고 지속적인 개선이 필요함을 주장하였다[12].

Gorla et al.(2010)은 정보의 형식을 정보의 표현 형태(style of presentation)와 정보가 이해하기 쉬운 형식(easy-to-understand format)으로 제공되는지 여부로 평가되어야 한다고 주장하였다.

4. 결론 및 함의

정보보안 정책의 개발은 반복적인 과정(iterative process)이다[12]. 본 과정에서 보안 정책은 조직에 미치는 영향을 측정하고 측정 결과를 반영하여 지속적으로 개선되어야 한다[12]. 이를 위해서는 두 가지 요소가 우선적으로 선행되어야 한다. 첫째는 측정지표이다. 명확한 측정지표가 없을 경우 자사의 정책의 무엇이 잘못되었는지 무엇을 수정해야 하는지 방향성을 잃고 답보상태에 이르게 될 수 있다. 따라서 명확한 평가지표의 개발이 선행되어야 지속적 개선이 가능하다. 둘째는 평가를 기반으로 지속적 개선활동이 수행되어야 한다. 한번 만들어진 정책은 영구적이라 생각할 수 없다. 산업 환경, 기술환경, 정부 정책의 변화, 외부 공격 유형의 변화 등 다양한 요인들에 의해 정보보안 환경은 변화하고 있다. 이를 정책에 반영하지 못할 경우 결국 비효과적이고, 강제성이 없으며, 생산성에 결여되어 불필요한 정책으로 남아있을 가능성이 높다. 따라서 평가와 함께 지속적 개선이 뒤따라야 한다.

본 연구는 이러한 두 가지 조건에서 첫 번째 조건을 지원할 수 있는 정보보안 정책의 평가지표를 개발하는 것을 목표로 연구를 수행하였다. 각각의 지표들은 데이터 품질과 정보품질과 관련된 문헌에서 제시한 측정지표를 중심으로 정보보안 정책의 특성에 맞게 차용하고 수정하였다.

여기서 제시한 지표들의 모든 상황에 적합하다고 평가할 수는 없으나 보안 정책의 효과를 사용자 혹은 준수자 관점에서 평가할 수 있는 포괄적인 지표를 제안하였다는 점에서 의의가 있다고 볼 수 있다. 또한 지속적 정책 개선에 필요한 평가지표로도 사용될 수 있다는 점에서 실무적 의의도 있다고 판단된다. 향후 연구에서는 여기서 제시된 지표들을 실증분석을 통해 그 효과성을 규명하는 연구가 수행되어야 할 것으로 보인다.

References

[1] B. Stvilia, L. Gasser, M. B. Twidale and L. C. Smith, "A Framework for Information Quality Assessment", Journal of the American Society for Information Science and Technology, Vol. 58, No. 12, pp. 1720-1733, 2007.

[2] C. J. Park and M. S. Yim, "An Understanding of Impact of Security Countermeasures on Persistent Policy Compliance", Journal of Digital Convergence, Vol. 10, No. 4, pp. 23-35, 2012.

[3] D. M. Strong, Y. W. Lee and R. Y. Wang, "Data Quality in Context", Communications of the ACM, Vol. 40, No. 5, pp. 103-110, 1997.

[4] K. Höne and J. H. P. Eloff, "What Makes an Effective Information Security Policy?", Network Security, Issue 6, No. 1, pp. 14-16, 2002.

[5] L. L. Pipino, Y. W. Lee and R. Y. Wang, "Data Quality Assessment", Communications of the ACM, Vol. 45, No. 4ve, pp. 211-218, 2002.

[6] M. Chan, I. Woon and A. Kankanhalli, "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior", Journal of Information privacy & Security, Vol. 1, No. 3, pp. 18-41, 2005.

[7] M. Chae, J. Kim, H. Kim and H. Ryu, "Information Quality for Mobile Internet Services: A Theoretical Model with Empirical Validation", Electronic Markets, Vol. 12, No. 1, pp. 38046, 2002.

[8] M. S. Yim, "A Path Way to Increase the Intention to Comply with Information Security Policy of Employees", Journal of Digital Convergence, Vol. 10, No. 10, pp. 119-128, 2012.

[9] M. Theoharidou, S. Kokolakis, M. Karyda and E. Kiountouzis, "The Insider Threat to Information Systems and the Effectiveness of ISO17799", Computers & Security, Vol. 24, pp. 472-484, 2005.

[10] N. Gorla, T. M. Somers and B. Wong,

"Organizational Impact of System Quality, Information Quality, and Service Quality", Journal of Strategic Information Systems, Vol. 19, pp. 207-228, 2010.

[11] R. Y. Wang and D. M. Strong, "Beyond Accuracy: What Data Quality Means to Data Consumers", Journal of Management Information Systems, Vol. 12, No. 4, pp. 5-34, 1996.

[12] S. Goel and I. N. Chengalur-Smith, "Metrics for Characterizing the Form of Security Policies", Journal of Strategic Information Systems, Vol. 19, pp. 281-295, 2010.

[13] S. Petter and E. R. McLean, "A Meta-Analytic Assessment of the DeLone and McLean IS Success Model: An Examination of IS Success at the Individual Level", Information & Security, Vol. 46, pp. 159-166, 2009.

[14] T. Herath and H. R. Rao, "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations", European Journal of Information Systems, Vol. 18, pp. 106-125, 2009.

[15] T. S. Jeong, M. S. Yim and J. B. Lee, "A Development of Comprehensive Framework for Continuous Information Security", Journal of Digital Convergence, Vol. 10, No. 2, pp. 1-10, 2012.

[16] Trend Micro, "Vulnerabilities under Attack: Shedding Light on the Growing Attack Surface", TrendLabs^{SM} 3Q 2014 Security Roundup, 2014.

[17] W. H. DeLone and E. R. McLean, "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update", Journal of Management Information Systems, Vol. 19, No. 4, pp. 9-30, 2003.

[18] Y. W. Lee, D. M. Strong, B. K. Kahn and R. Y. Wang, "AIMQ: A Methodology for Information Quality Assessment", Information & Security, Vol. 40, pp. 133-146, 2002.

[19] Y. Wand R. Y. Wang, "Anchoring Data Quality Dimensions in Ontological Foundations", Communications of the ACM, Vol. 39, No. 11, pp. 86-95, 1996.

저자소개

임 명 성(Myung-Seong Yim) **[정회원]**

- 2002년 2월 : 삼육대학교 경영정보학과 (경영학사)
- 2004년 2월 : 한국외국어대학교 경영정보대학원 (경영학 석사)
- 2011년 8월 : 서강대학교 경영전문대학원 (경영학 박사)
- 2012년 3월 ~ 현재 : 삼육대학교 경영학과 조교수

<관심분야> : 정보보안, 정보심리학, 서비스 시스템, IT의 부작용