조직내 정보시스템 보안 전략의 성공적 구현을 위한 정보시스템 보안 전략의 특성

박상서* · 박춘식*

요 약

조직의 정보시스템 보안을 향상시키기 위해서는 전략의 도입이 필수적이다. 그리고, 이들 전략을 조직내에 성공적·효율적으로 구현하기 위해서는 전략의 특성 중 전략의 구현에 영향을 주는 요인들을 고려하여야 한다. 본 논문에서는 전략의 여러 특성들 중 이러한 특성들을 연구하였다.

Features of Information Systems Security Strategies Affecting Their Successful Implementation in Organizations

Sangseo Park* · Choon Sik Park*

ABSTRACT

It is essential for organizations to employ strategies for improving their information systems security. It is also required to consider features of information systems security strategies which affect their successful and efficient implementation in organizations. This paper identifies those features from various information systems security and strategies literatures.

Key words : Information Systems Security, Information Systems Security Strategy, Success Factor

* ETRI 부설연구소

1. 서 론

정보보안 제품이 조직에 속속들이 도입되고 있음에도 불구하고 경제적 손실과 피해는 줄어들지 않고 있다[1]. Anderson[2]과 Caralli[3]에 따르면 실세계의 정보시스템 보안은 기술적 접근만으로는 실패할 수 밖에 없다. 또한, Ein-Dor와 Segev[4]에 따르면 보안제품이나 도구가 설치·운용되는 조직의 영향을 강하게 받는다. 즉, 조직의 보안은 기술과 보안이 균형을 갖출 때에만 비로서 제 역할을 수행한다고 할 수 있다. 조직뿐 아니라 정보시스템 보안 관련 연구도 기술적 측면에 치우쳐 있기는 하지만[5-9], 조직이 기술중심의 사고에서 사회 및 조직의 측면으로 관심을 옮겨가고 예산도 증액하기 시작한 것은 그나마 다행이라 할 수 있다[3, 10, 11].

여러 전문가들과 실무자들은 조직의 정보시스템 보안을 위하여 전략을 도입하여야 한다고 주장하고 있다[12-29]. [28]은 조직의 정보시스템 보안에 적용되어야 할 전략의 개념을 소개하였고, Straub [17]는 보안 전략을 도입함으로써 조직의 보안이 향상된다는 것을 실증적으로 보였고, Park and Ruighaver[29]는 정보시스템 보안 전략을 식별하고 각 전략을 분류하기 위한 프레임워크를 제안하였다. 하지만 전략을 조직내에 구현할 때 전략의 어떠한 측면을 고려하여야 하는지에 관한 연구는 찾아보기 어렵다.

유사한 연구로, 보안을 조직내에 구현할 때 고려하여야 할 요소에 관한 연구를 찾아볼 수 있다. 먼저, Torres et al.[23]은 정보보안 인식, 정보보안 담당자의 경쟁력 등 12개의 요인을 식별하고 76개의 indicator를 개발하였다. Wood[5]는 시스템 보안에 대한 책임감, 정보보안 조직 등 14개의 요인을 식별하였고, Kankanhalli et al.[16]은 기업의 규모, 최고 관리자의 지원 등 7가지의 요인을 식별하였다. 이 중 앞의 두 연구는 관리 측면에서의 점검요인에 초점을 맞추고 있다. 세 번째 연구는 조직내의 보안 구현과는 관련이 있지만 전략의 구현과는 관계가 없다. 즉, 정보시스템 보안의 조직내 구현에 관련된 연구는 관리 및 조직의 측면에서는 연구가 진행되었으나 전략의 적용 측면에서의 고려사항에 관한 연구는 아직까지 찾아보기 어려운 실정이다.

따라서, 본 연구에서는 조직에 정보시스템 보안 전략을 도입할 때 전략의 어떠한 측면들을 고려하여야 하는지에 관하여 수행한 문헌 연구 결과를 기술한다.

2. 정보시스템 보안 전략의 구현을 위해 전략이 갖추어야 할 특성

정보시스템 보안 전략을 조직내에 구현하기 위해서는 다음과 같은 특성들이 고려되어야 한다.

- **Alignment** : 정보시스템 보안 전략은 조직에 완전하게 통합되어야 한다[21, 30]. Goodhue and Straub[31]와 Kankanhalli et al.[16]은 기업의 유형이 정보시스템 보안에 대한 관심, 노력 및 투자와 상관관계가 있음을 발견하였다. 특히 Kankanhalli et al.[16]에 따르면 정보보안에 관한 요구사항, 정보보안의 적용 및 역할은 기업에 따라 다양하며, Kankanhalli et al.[16] 및 Wood[5]는 정보시스템 보안을 조직내에 성공적으로 구현하는데 있어서 핵심적인 요인은 최고 경영자의 지원에 달려있음을 발견하였다. 이는 정보시스템 보안 전략을 조직내에 성공적으로 그리고 효과적으로 구현하기 위해서는 정보시스템 보안 전략이 조직에 밀접하게 연계되어야 할 뿐 아니라 조직의 목적을 달성을 지원하여야 한다. 또한 조직 전략과 정보시스템 전략과도 궤를 같이 하여야 한다.
- **Balance** : 정보시스템 보안 전략은 정보시스템 전반에 걸쳐 적용되어야 한다[32]. 정보시

스템 보안 전략은 특정 측면이나, 위치, 정보 또는 자산에만 초점을 맞추지 말고 전체적으로 골고루 분포되어야 한다. 또한, 여러 유형의 전략들이 각각의 목적에 맞추어 조화를 이루어 적용되어야 한다. 예를 들어, 예방차원의 전략과 대응차원의 전략을 동시에 적용함으로써 단일 전략만을 적용하는 것에 비해 보안을 더욱 향상시킬 수 있다. 이 요건은 다중 전략이 적용되는 경우에 한해 관련이 있다.

- **Effectiveness** : 전략은 위협과 공격에 효과적으로 대응할 수 있어야 한다[19]. 전략을 적용하면 사고의 확산을 방지할 수 있어야 하며 실제·잠재 피해도 최소화할 수 있어야 한다. 또한 과거의 공격과 위협뿐 아니라 미래의 위협과 공격에도 대처가 가능해야 한다.
- **Cost** : 정보시스템의 구축과 마찬가지로[4, 33], 정보시스템 보안을 조직에 구현하는데 가장 큰 장애 요소는 재정이다. Torres et al.[23]은 조직의 예산 규모가 정보시스템 보안의 핵심 요소임을 발견하였다. 즉, 정보시스템 보안 전략을 조직에 적용하기 위해서는 전략을 구현하는데 소요되는 비용이 저렴해야 한다[11, 12, 27]. 특히 최근들어 조직은 정보시스템 보안에 소요되는 비용을 "경비"에서 "투자"로 변경하고 있다[3]. 그럼에도 불구하고 정보시스템 보안 전략의 구현 등에 소요되는 비용은 계속 제한적일 수밖에 없을 것이다. 따라서, 최소한의 비용으로 최고의 보안성을 확보할 수 있어야 한다.
- **Impact on Resources** : 보안 전략을 조직내에 구현하게 되면 영향을 받는 부분이 발생하게 마련이다. 따라서 전략을 구현할 때 조직의 자원, 서비스 등에 최소한의 영향을 주면서도 보안이 향상될 수 있어야 한다[19, 34].
- **Tolerance** : 전략들을 연결하여 아키텍처로 구성하게 되면 위협과 공격을 잘 흡수하고 견뎌낼 수 있도록 구성되어야 한다[35]. 이렇게 함으로써 정보시스템의 생존성(survivability)을 강화시킬 수 있으며 동시에 공격에 대응할 수 있는 시간을 벌 수 있도록 해준다.
- **Multiplicity** : 정보시스템의 보안을 향상시키기 위해서는 하나 이상의 전략을 적용하는 것이 당연하다[5, 11]. 최근과 같이 공격기법과 기술이 비약적으로 발전하는 상황에서는 하나의 전략만으로는 조직의 정보 인프라를 보호할 수 없다. 특히, 생산성 향상을 위하여 정보시스템을 지속적으로 확장 및 도입하여야 할 뿐 아니라 이로 인하여 정보시스템의 복잡성이 계속 증가하는 상황에서는 더욱 그러하다.
- **Combination** : 하나 이상의 전략을 적용할 때에는 각 전략이 서로 결합되어 유기적으로 동작하여야 한다[19, 36, 37]. 특정 전략을 조합하여 사용함으로써 사각지대를 최소화할 수 있으며, 전반적으로 보안성을 획기적으로 향상시킬 수도 있다. 이를 위하여 장기적으로 적용될 수 있는 전략과 단기적 효과를 얻을 수 있는 전략이 함께 사용될 수도 있으며, 영구적 전략과 임시전략, 예방 전략과 대응 전략 등이 함께 조화롭게 사용될 수 있어야 한다.
- **Dynamic Nature and Agility** : 공격과 위협 및 이에 대처하는 상황은 계속적으로 변화하기 마련이다. 따라서, 정보시스템 전략이 갖는 동적 측면을 충분히 고려함으로써 상황과 환경의 변화에 따라 신속히 전환될 수 있어야 한다[15, 38].
- **Ease of Implementation** : 전략을 조직내 및 정보시스템내에 구현하기가 용이하여야 한다[11].
- **Simplicity** : 여러 전략이 혼합되어 사용될 때, 각 전략은 마치 거대한 구조물을 구성하는 하나의 빌딩블럭과 같이 여겨질 수 있다. 그리고 이 때, 각 블록들은 손쉽게 교체 및 대치가 가능하도록 단순하여야 한다. 실제적으로

여러 경우에 있어서 단순한 전략만으로도 복잡하고 강력한 공격에 대처할 수 있기도 하다[35]. 따라서 각각의 단위가 되는 전략들은 단순하여야 한다. 하지만 각 전략들이 조화를 이룰 때 더 큰 대응력을 가지게 된다.

- **Continuity** : 전략의 적용으로 인한 시스템적 혼선이나 사용자의 혼란을 최소화할 수 있도록 전략을 너무 자주 변경하지는 말아야 한다[19, 38]. 대신 긴급상황 등을 제외하고는 전략을 일정기간 이상 지속적으로 적용하여야 효과를 발휘하는 경우가 많다.

3. 결 론

우리는 완벽한 보안보다는 적절한 보안을 지향하여야 하며. 보안은 완성이라기 보다는 중간과정임을 잊지 않아야 한다[11]. 특히, 인력, 예산, 기술 등과 같은 보안을 위한 자원은 항상 부족한 상황이므로 전략을 적용하여 최소한의 노력으로 최대한의 효과를 발휘하기 위한 지혜를 결집시켜야 한다.

이를 위해서는 정보시스템 보안 전략을 조직내에 실현할 때 여러 사항들을 종합적으로 고려하여 적용하여야 한다. 본 논문에서는 이와 같은 상황에서 전략의 적용시 검토하여야 할 전략의 특성들을 문헌연구하였으며, 12가지 특성들을 제시하였다.

정보시스템 보안을 위한 전략의 도입이 필요하다는 주장은 제기되고 있으나, 각 전략이 어떠한 특성을 가져야 하는지에 대한 연구는 아직까지 시도되지 않았다. 따라서 학술적으로 볼 때 본 논문은 정보시스템 보안을 위한 전략을 조직내에 구현할 때 각 전력들이 갖추어야 할 요건들을 정리하였다는 데 의의가 있다.

본 연구의 결과를 발전시키기 위해서는 이 특성들외에도 전략이 가져야 할 여러 특성들을 추가로 발굴하여야 할 것이며, 이들을 종합적으로 표현할 수 있는 프레임워크를 구성하여야 할 예정이다. 그 후, 각 특성의 중요도와 조직의 특성 등에 따라 우선순위화 또는 가중치 부여의 방법을 통해 조직에 따라 맞춤형 전략을 구현할 수 있는 방안을 모색할 예정이다.

참 고 문 헌

[1] R. Richardson, CSI Survey 2007 : The 12th Annual Computer Crime and Security Survey, Computer Security Institute, 2007.

[2] R. Anderson, “Why Information Security is Hard-An Economic Perspective”, 17th Annual Computer Security Applications Conference(ACSAC) 2001, pp. 358-365, 2001.

[3] R. A. Caralli, Managing for Enterprise Security, CMU/SEI-2004-TN-04, Carnegie-Mellon University, 2004.

[4] P. Ein-Dor and E. Segev, Organizational Context and the Success of Management Information Systems, Management Science, Vol. 24, No. 10, pp. 1064-1077, 1978.

[5] C. C. Wood, Information Systems Security : Management Success Factors, Computers and Security, Vol. 6, pp. 314-320, 1987.

[6] R. A. Botha and T. G. Gaadingwe, Reflecting on 20 SEC Conferences, Computers and Security, Vol. 25, No. 6, pp. 247-256, 2006.

[7] S. Landau and M. R. Stytz, Overview of Cyber Security : A Crisis of Prioritization, IEEE Security and Privacy, Vol. 3, No. 3, pp. 9-11, 2005.

[8] M. R. Benioff, E. D. Lazowska, and R. Bajcsy et al., Report to the President, Cyber Security : A Crisis of Prioritization, President's Information Technology Advisory Committee(PITAC), 2005.

[9] R. Bajcsy, T. Benzel, and M. Bishop et al., Cyber Defense Technology : Networking and Evaluation, Communications of the ACM, Vol. 47, No. 3, pp. 58-61, 2004.

[10] G. Dhillon, and J. Backhouse, Current Directions in IS Security Research : Towards Socio-Organizational Perspectives, Information Systems Journal, Vol. 11, pp. 127-153, 2001.

[11] S. Liu, J. Sullivan, and J. Ormaner, A Practical Approach to Enterprise IT Security, IEEE IT Professional, Vol. 3, No. 5, pp. 35-42, 2001.

[12] J. Sherwood, SALSA : A Method for Developing the Enterprise Security Architecture and Strategy, Computers and Security, Vol. 15, pp. 501-506, 1996.

[13] O. S. Saydjari, Cyber Defense : Art to Science, Communications of the ACM, Vol. 47, No. 3, pp. 53-57, 2004.

[14] R. K. Betts, Is Strategy an Illusion?, International Security, Vol. 25, No. 2, pp. 5-50, 2000.

[15] W. Tirenin, "A Concept for Strategic Cyber Defense", MILCOM '99, pp. 458-463, 1999.

[16] A. Kankanhalli, H.-H. Teo and B. C. Y. Tan et al., An Integrated Study of Information Systems Security Effectiveness, International Journal of Information Management, Vol. 23, pp. 139-154, 2003.

[17] D. W. Straub, Effective IS Security : An Empirical Study, Information Systems Research, Vol. 1, No. 3, pp. 255-276, 1990.

[18] D. W. Straub and R. J. Welke, Coping with Systems Risk : Security Planning Models for Management Decision Making, MIS Quarterly, Vol. 22, No. 4, pp. 441-469, 1998.

[19] T. Grance, K. Kent, and B. Kim, Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology, NIST Special Publication(SP), 800-61, National Institute of Standards and Technology, 2004.

[20] P. Mel, K. Kent, and J. Nusbaum, Guide to Malware Incident Prevention and Handling, Recommendations of the National Institute of Standards and Technology, NIST Draft Special Publication(SP), 800-83, National Institute of Standards and Technology, 2005.

[21] P. Bowen, J. Hash, and M. Wilson et al., Information Security Handbook A Guide for Managers(Draft), Recommendations of the National Institute of Standards and Technology, NIST Draft Special Publication(SP), 800-100, National Institute of Standards and Technology, 2006.

[22] S. Edwards and M. C. Willimas, "The Need for In-Depth Cyber Defence Programs in Business Information Warfare Environments", 2nd Australian Information Warfare and Security Conf. 2001, pp. 56-63, 2001.

[23] J. M. Torres, J. M. Sarriegi, and J. Santos et al., Managing Information Systems Security : Critical Success Factors and Indicators to Measure Effectiveness, ISC 2006, pp. 530-545, 2006.

[24] H. Yang, H. Luo, and F. Ye et al., Security in Mobile Ad Hoc Networks : Challenges and Solutions, IEEE Wireless Communications, Vol. 11, No. 1, pp. 38-47, 2004.

[25] D. Armstrong, S. Carter, and G. Frazieret al., Autonomic Defense : Thwarting Automated Attacks via Real-Time Feedback Control, Complexity, Vol. 9, No. 2, pp. 41-48,

2004.

[26] J. Mirkovic, and P. Reiher, A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, ACM SIGCOMM Computer Communication Review, Vol. 34, No. 2, pp. 39-53, 2004.

[27] B. W. Lampson, Computer Security in the Real World, Computer, Vol. 37, No. 6, pp. 37-46, 2004.

[28] 박상서, "조직차원의 정보보안 전략의 개념", 정보·보안 논문지, 제7권, 제3호, pp. 15-24, 2007.

[29] S. Park and T. Ruighaver, "Strategic Approach to Information Security in Organizations", 2008 International Conference on Information Science and Security(ICISS 2008), pp. 26-31, IEEE, Seoul, Korea, 2008.

[30] D. Birchall, J.-N. Ezingeard, and E. McFadzean et al., Information Assurance : Strategic Alignment and Competitive Advantage, Grist Ltd., 2004.

[31] D. L. Goodhue and D. W. Straub, Security Concerns of System Users : A Study of Perceptions of the Adequacy of Security, Information and Management, Vol. 20, No. 1, pp. 13-27, 1991.

[32] J. Ölnes, Development of Security Policies, Computers and Security, Vol. 13, No. 8, pp. 628-636, 1994.

[33] L. Raymond, Organizational Context and Information Systems Success : A Contingency Approach, Journal of Management Information Systems, Vol. 6, No. 4, pp. 5-20, 1990.

[34] M. M. Williamson, Resilient Infrastructure for Network Security, Complexity, Vol. 9, No. 2, pp. 34-40, 2004.

[35] B. Martin, Social Defense Strategy : The Role of Technology, Journal of Peace Research, Vol. 36, No. 5, pp. 535-552, 1999.

[36] D. Reiter, Military Strategy and the Outbreak of International Conflict : Quantitative Empirical Tests, 1903-1992, The Journal of Conflict Resolution, Vol. 43, No. 3, pp. 366-387, 1999.

[37] D. Reiter and C. Meek, Determinants of Military Strategy, 1903~1994 : A Quantitative Empirical Test, International Studies Quarterly, Vol. 43, No. 2, pp. 363-387, 1999.

[38] J. S. Nye-Jr., Soft Power. Foreign Policy, No. 80, Twentieth Anniversary, pp. 153-171, 1990.

박 상 서

1991년 중앙대학교 전자계산학과(공학사)
1993년 중앙대학교대학원 전자계산학과(공학석사)
1996년 중앙대학교대학원 컴퓨터공학과(공학박사)
1996년~1998년 국방정보체계연구소 선임연구원
1998년~1999년 국방과학연구소 선임연구원
2000년~현재 ETRI 부설연구소 책임연구원

박 춘 식

1981년 광운대학교 졸업(공학사)
1983년 한양대학교 전자통신전공(공학석사)
1995년 일본동경공업대학교 정보보호전공(공학박사)
1982년~1999년 한국전자통신연구원 부장
2000년~현재 ETRI 부설연구소 책임연구원