Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.4, Aug. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.4.873

금융 산업에서 발생하는 랜섬웨어 공격에 대한 FAIR 기반의 손실 측정 모델 분석

윤 현 식,† 송 경 환, 이 경 호‡
고려대학교

FAIR-Based BIA for Ransomware Attacks in Financial Industry

Hyun-sik Yoon,† Kyung-hwan Song, Kyung-Ho Lee‡
Korea University

요 약

랜섬웨어가 확산됨에 따라 공격 대상이 개인에서 단체로 변하게 되었고 더 지능적이고 조직적으로 변하게 되었다. 이에 금융 산업을 포함한 국내의 기반시설들은 랜섬웨어의 위협에 대해 더 이상 무시 할 수 없는 단계로 접어들 고 있다. 이러한 보안이슈에 대응하기 위해 기관들은 정보보호 관리체계인 ISMS를 사용하고 있지만 피해가 발생 했을 시 발생하는 피해규모를 산정 할 수 없어 경영진이 피해 현황에 대한 의사결정을 하는 것에 어려움이 있다. 본 논문에서는 ISMS의 문제로 여기어 지는 리스크에 대한 피해규모의 파악 및 합리적인 피해규모 산정을 시나리오를 기반으로 진행되는 FAIR 기반의 손실 측정모델을 통해 금융 산업에 랜섬웨어 공격이 미칠 수 있는 손실 및 위험을 확인하며 ISMS를 수정하는 것이 아닌 현재 적용되어 있는 ISMS 및 ISO 27001의 통제항목을 적용하여 손해금액을 낮출 수 있는 방안을 제시한다.

ABSTRACT

As Ransomware spreads, the target of the attack shifted from a single personal to organizations which lead attackers to be more intelligent and systematic. Thus, Ransomware's threats to domestic infrastructure, including the financial industry, have grown to a level that cannot be ignored. As a measure against these security issues, organizations use ISMS, which is an information protection management system. However, it is difficult for management to make decisions on the loss done by the security issues since amount of the damage done can not be calculated with just ISMS. In this paper, through FAIR-based loss measurement model based on scenario's to identify the extent of damage and calculate the reasonable damages which has been considered to be the problem of the ISMS, we identified losses and risks of Ransomeware on the financial industry and method to reduce the loss by applying the current ISMS and ISO 27001 control items rather than modifying the ISMS.

Keyword: Ransomware, ISMS, FAIR, Financial industry, Risk management

I. 서 론

1.1 연구목적

인터넷의 보급률이 증가함에 따라 SNS나 E-Mail 등 소통하는 기술이 발달 하게 되었고 인터넷을 사용하는 대부분의 사용자들이 SNS 및 E-mail을 사용하게 되었다.

인터넷의 보급이 증가함에 따라 관련 악성코드의 활동 또한 활발해지게 되었고 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 만든 뒤, 이를 인

Received(05. 25. 2017), Modified(1st: 06. 08. 2017, 2nd: 08. 01. 2017), Accepted(08. 02. 2017)

† 주저자, hsyoon900827@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

질로 금전을 요구하는 악성 프로그램을 인 랜섬웨어의 활동이 활발해 졌다. 이스트소프트가 발표한 '2016년 랜섬웨어 동향 결산'에 따르면, 지난 2016년 1월부터 12월까지 '알약'을 통해 사전 차단된 랜섬웨어 공격은 총 397만 4,658건으로 나타났으며 랜섬웨어 공격은 해마다 과격해지고 위험해지면서 보안 위협도 덩달아 높아졌다[1]. 이러한 위험은 금융 산업에도 큰 위협이 될 수 있어 대책이 필요한 상황이다.

또한 2017년 5월 13일을 시작해 전 세계를 대상으로 워나크라이 랜섬웨어가 배포되었으며 한국에도 공격이 진행되고 있다.

이러한 보안이슈들에 대해 대응하기 위해 대표적으로 정보보호 관리 체계인 ISMS (Information Security Management System)가 사용하고 있지만 피해가 발생 했을 시 발생하는 피해규모를 산정할 수 없어 경영진이 피해 현황에 대한 의사결정을 하는 것에 어려움이 있다. 이에 리스크에 대한 합리적인 피해규모 산정 방법이 필요했다.

랜섬웨어의 특성상 근본적인 차단은 사실상 힘들고 파일들을 암호화하기 때문에 대응 방법으로 유입경로 차단 및 감염 후 대응하는 방안이 있다. 하지만 랜섬웨어의 경우 사전에 차단하는 것이 사실상 힘들며 돈을 직접적으로 요구하는 특성상 감염 후 대응이 주를 이룬다. 즉, 기업의 입장에서는 감염 후 대책을 산정할 때 실제 비트고인을 지불하는 방안보다 저렴하며 투자를 통해 피해를 사전에 줄일 수 있는 대책을 찾을 필요가 있다.

본 연구에서는 리스크 분석 방법론인 FAIR (Factor Analysis of Information Risk)를 통해 ISMS에서 부족하다고 여겼던 피해규모 산정을 진행하였다.

해당 프로세스에서 랜섬웨어를 기반으로 피해규모 산정 모델을 제시한 이유는 문재 발생 후 피해를 줄여야 하는 특성과 악성코드의 특성을 가졌기 때문이다. 즉, 다른 악성코드 및 보안 사고에 의한 문재 발생 시 본 모델을 바탕으로 유동적이며 객관적으로 각 케이스의 피해를 산정하여 추후 사고에 대한 대비 및 문재의 대응 방법에 대한 의사결정 진행 시 합리적인 지표로 작용 할 수 있을 것이다. 실제 랜섬웨어 관련 피해 사례를 통해 금융 산업에 적합한 피해규모산출 방법을 제시하여 금융 산업에 끼칠 수 있는 리스크를 실제 실무에서 활용할 수 있도록 순차적, 객관적으로 분석하고 손해금액을 산정하는 방법론을 제시한다. 또한 A 금융사에 시도되는 공격에 대한 실 데이터를 활용하여 방법론의 신뢰성을 높이었다.

본 연구에서는 리스크에 대한 피해규모의 파악 및 합리적인 피해규모 산정을 통해 금융 산업에 랜섬웨어 공격이 미칠 수 있는 손실 및 위험을 확인하며 ISMS를 수정하는 것이 아닌 현재 적용되어 있는 ISMS 및 ISO 27001의 통제항목을 적용하여 손해금액을 낮출 수 있는 방안을 제시한다.

1.2 연구 대상 및 방법

본 연구에서는 리스크에 대한 피해규모의 파악 및 합리적인 피해규모 산정을 통해 랜섬웨어가 미칠 수 있는 손실 및 위험을 확인하며 ISMS를 수정하는 것이 아닌 ISMS 및 ISO 27001의 통제항목 적용을 통해 손해금액을 낮출 수 있는 방안을 제시한다.

2장에서는 본 연구에서 활용될 FAIR 방법론에 대한 선행 연구 분석과 현제 사용되고 있는 ISMS에 대한 분석이 진행되었다.

3장에서는 FAIR를 통한 금융권의 랜섬웨어 피해 시 손해금액 산정 및 위험 분석이 진행된다.

4장에서는 A 금융사에서 제공한 자사에 가해지는 공격들에 대한 실제 데이터를 시나리오에 적용해 본 방법론을 검증한다.

5장에서는 본 논문에 대한 결론을 제시한다.

II. 관련 연구

중요 기반시설에 대한 공격, 클라이언트 S/W에 대한 공격, 제어시스템 대상 공격 등 최근 사건에 사용된 공격 기술들이 점점 더 정교화 되고 있으며 금융권에 대한 공격도 다양해지고 있다[2]. 즉, 해당 분야에 대한 예상 손해 및 피해를 연구해 볼 필요가 있다.

2.1 ISMS 연구

ISMS(Information Security Management System)를 흔히 정보 보안 경영 시스템이라고 해석한다. BSI에서는 기업이 민감한 정보를 안전하게 보존하도록 관리할 수 있는 체계적 경영 시스템이라고 정의한다.

ISO 27001에서는 PDCA 모델을 통해서 ISMS를 발전시켜 나갈 수 있다고 말하고 있는데, 여기서 PDCA는 계획(Plan), 수행(Do), 점검(Check),

조치(Act)를 순환 반복적으로 수행하는 모델이다. 계획: ISMS 수립(Establishing ISMS), 수행 : ISMS 구현과 운영(Implement and Operate the ISMS), 점검 : ISMS 모니터링과 검토(Monitor and Review the ISMS), 조치 : ISMS 관리와 개선(Maintain and Improve the ISMS)의 단계를 거친다[3].

민감한 정보를 안전하게 보존하도록 관리할 수 있는 체계적 경영 시스템이라고 정의하고 있지만 실제 피해발생시 의사결정에 도움을 줄 수 있는 지표는 없는 상태이다. 본 문재에 대한 대응으로 임시로 공식을 만들어 피해액 및 피해 정도를 산출 하는 임시방편적이 공식 및 대책이 제시되고 있지만 실무진의 인터뷰 결과 실질적으로 사용되고 있는 것은 없는 상황이다.

2.2 FAIR 방법론에 대한 사전 연구

2.2.1 FAIR 방법론

FAIR(Factor Analysis of Information Risk)는 2005년 Risk Management Insigh사의 Jack Jones에 의해서 처음 제안 되었으며 FAIR의 기본은 "FAIR ISO/IEC 27005 cook book"에 방법론이 소개되고 있다[4][5]. FAIR는 리스크가 발생할 수 있는 가능성을 시나리오 기반으로 분석하여 정량적으로 측정할 수 있도록 하였다. 이를 바탕으로 기업에서 피해에 대한 사전 대책 수립 시 실용적인 의사결정 수단으로 활용 가능하도록 설계 되었다.

2.2.2 FAIR 방법론관련 연구

FAIR 방법론을 사용하여 각 분야의 리스크를 분석한 최신 동향을 연구 하였다.

윤장호(2016)는 개인정보 유출사고 발생에 따른 손실 측정을 FAIR 방법론을 통해서 분석하였다. 본 논문에서는 투자의 의사결정을 위한 손실측정을 사전에 분석하는 방법으로 리스크를 분석하였다[6].

김정규(2017)는 개인정보 유출사고에 대한 기업의 리스크와 손해금액 산출을 위해, FAIR 방법론을 사용하여 실제 개인정보 유출 사고 기업의 손해금액을 분석하고 산출하는 방법론을 제시 하였다[7].

Anhtuan Le(2017)는 FAIR을 확장 한 베이지안 네트워크를 구축하는 방법을 제안한다. 높은 입상성의 정량적 LEF 결과를 얻기 위해, 퍼지 입력의 경우에도 추적 가능하고 반복 가능한 프로세스를 사용하였고 퍼지 입력의 변화가 LEF에 어떻게 기여하는지 보여줌으로써 FAIR의 다양한 활용을 보여준다[8].

앞선 두 연구의 경우 포괄적인 개인정보 유출사고에 대한 연구를 진행하였고 Anhtuan Le의 경우 지표를 빅 데이터를 통해 설정하는 방안을 제시하고 있지만 구체적인 공격에 대한 연구는 부족한 상황이며 해당 방법론에 대한 실용성 또한 검증되지 않은 상황이다.

본 논문에서는 사고 발생 후 대책에 대한 기준점으로 랜섬웨어에 대한 방법론을 제시하며 실제 데이터를 통해 효용성을 증명하였다.

2.3 금융 산업의 보안 취약점 및 보안사고 동향

금융권에 가해지는 공격은 증가하고 있는 추세이며 새로 이슈가 되고 있는 랜섬웨어 공격 또한 뜨거운 감자로 오르고 있다.

2016년에 발생한 다양한 사이버 범죄의 공격자들의 특징 중 하나는 금전목적의 공격성향이 강해진 점을 들 수 있다. 랜섬웨어의 경우 금전목적의 대표적인 사례라고 볼 수 있다. 공격자들이 피해자에게 직접적인 금전탈취를 통해 수익을 창출하게 되면서 금융권의 직접적인 공격이 증가하고 있다[9].

III. FAIR를 통한 랜섬웨어에 대한 피해 예측 모델

본 단락에서는 FAIR 분석방법론을 통해서 랜섬웨어에 인한 손해금액의 산정모델을 제시하여 사고 발생 후 발생하는 피해 금액으로 확인 할 수 있는 가이드라인을 제시하며 추후 ISMS에 적용 가능하도록 한다.

FAIR를 기반으로 한 연구들은 단순한 모델을 예측하고 결론짓는다. 하지만 랜섬웨어의 경우 실시간 대처가 무엇보다 중요하고 직접적인 공격에 의한 피해보다는 공격으로 인해 발생하는 2차 피해가 주를 이룬다. 금융 산업은 기반시설 중 하나며 공격 시 사람들의 생계에 직접적으로 영향을 줄 수 있다. 즉, 최신의 데이터를 통해 피해를 줄이는 것이 중요한데 본 논문에서는 아닌 실제 금융회사의 데이터를 이용함으로서 금융산업 및 랜섬웨어에 적합함을 보여주었다.

본 연구에서는 FAIR 모델을 단계적으로 랜섬웨어

공격에 대한 실제 금융 산업이 가질 수 있는 리스크를 객관적으로 분석하고 손해금액을 산출하는 방법을 제시하여 기관의 정보보호 관리체계에서 발생 될 수 있는 피해를 확인 할 수 있게 하였다.

따라서 본 연구를 통해 금융 산업 실무자들은 랜섬웨어가 감염 되었을 때 발생 할 수 있는 손해금액 산출을 FAIR를 통해 확인하게 된다. 또한 시나리오를 기반으로 어떤 사고조치가 타당한 조치인지 논리적인 근거를 확보할 수 있다.

3.1 ISMS에 FAIR 적용

Fig 1의 경우 ISMS를 ISO 27001에서 제안하는 PDCA 모델을 통해 운영하는 그림이다. ISMS의 경우 리스크에 대한 합리적인 피해규모의 산정이 어렵다. FAIR의 경우 피해의 정량적 확인이 가능해 ISMS의 PDCA의 관리와 개선 단계에 적용하여 ISMS의 고질적인 문제인 리스크에 대한 피해규모 파악 및 합리적인 피해규모 산정이 가능하다.

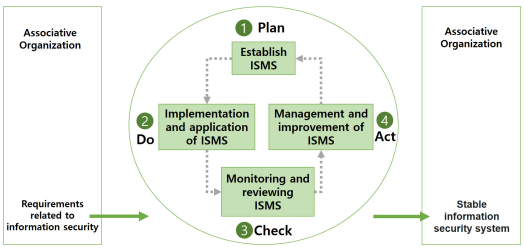

Fig. 1. Applying PDCA on ISMS[3]

3.2 FAIR의 단계별 분석 방법

본 연구에서는 Measuring and Managing Information Risk: A FAIR Approach에서 제시하는 방법론 및 용어를 통해 FAIR 분석 하였다

FAIR 방법론은 각 컴포넌트에 대한 분석을 Very Low 부터 Very High까지 5단계로 구분되어 평가된다. Fig 2 은 FAIR의 전체 프로세스를 나타낸 그림이다[10].

첫 랜섬웨어 사고 시나리오 구성, 자산식별 단계에서는 사고가 발생 할 수 있는 자산 및 사고 발생 위협을 식별하는데 본 논문에서는 랜섬웨어에 의해 발생한 피해유형과 공격 대상을 식별해 실제 발생 가능한 시나리오를 구성한다.

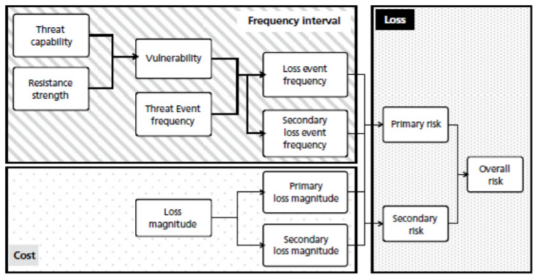

Fig. 2. FAIR risk analysis process

랜섬웨어 사고에 대한 LEF (Loss event Frequency) 및 SLEF (Secondary Loss Event Frequency)를 구하기 위해 TEF(Threat Event Frequency), TCAP (Threat Capability), RS (Resistance Strength)를 산출하고 결과를 통해 VUL(Vulnerability)를 산출해 취약점을 파악한다.

세 번째 랜섬웨어 사고에 대한 Risk 산출 단계는 PLM(Primary Loss Magnitude) 과 SLM(Secondary Loss Magnitude)을 산출해 사건에 대한 PR(Primary Risk)와 SR(Secondary Risk)을 산출하여 마지막 OR(Overall Risk) 산출을 통해 손해금액을 산정한다.

3.3 랜섬웨어 공격에 대한 단계별 분석을 위한 지표 설정

3.3.1 랜섬웨어 사고 시나리오 구성, 자산식별 단계

랜섬웨어 사고에 대한 시나리오 구성 및 자산식별을 진행하기 위해 2016년 인도에서 3개의 은행과 1개의 제약회사가 랜섬웨어 공격에 노출되어 컴퓨터당 1 비트코인을 요구 받은 랜섬웨어 공격 사례를 이용하였다. 해당 케이스를 지표설정에 사용한 이유는 실제 랜섬웨어에 감염이 된 케이스이며 랜섬웨어를 유포한 단체가 요구한 금액이 구체적으로 알려졌기 때문이다. FAIR의 경우 실제 발생하였던 이전 사고의 피해금액을 기준으로 미래의 피해액을 산출하기 때문에 유사 기관에서 발생한 랜섬웨어 관련 구체적인 피해금액을 활용하는 것이 중요하다. 추후 관련 기관에서 많은 유사 피해가 발생하여 피해금액은 변경 될 수 있으나 ISMS의 경우 사이클을 통한 개선을 추구하고 있다는 점에서 수정은 긍정적이며 추후 수정 시 본 분석이 기준이 될 수 있다.

3.3.1.1 랜섬웨어 사고 관련 자산 식별

인도에서 발생한 공격 및 A 금융회사의 문서보존기간 표를 바탕으로 Table 1.을 식별하였다.

Table 1.에서 언급되고 있는 자산은 인도의 사례와 A 금융회사에서 제공한 사내 문서 중요도에 따른 문서보존기간을 바탕으로 식별 되었다.

Table 1. List of asset

Classification	Description
Management Plan Document	Management strategy, Finance, Accounting, ect.
Management Support Document	Personnel Management, Training, General Affairs, Manager, ect
Business Document	Product, Financial Instrument, contract, Personal Information, ect
General Document	Risk Management

3.3.1.2 위협원 분석

위협원을 분석하기 위해 한국의 기반시설을 대상으로 발생한 공격과 인도 은행에 대한 공격을 참고하였다.

Table 2. Intimidator analysis

Intimi-dator	Cyber criminal			Country		
Reason for Selection	There has been attack through Ransomeware are increasing			Cyber terrorist attacks have occurred on major facilities of Korea		
Motiva-tion	Financial			Nationalism		
Major Intention	Participate in practice legitimate or illegal activities to maximize financial benefit			New tactics of gathering information / Making country's financial base and information hostage		
Preferred Target	Financial and private information			Critical financial infrastructure		
Ability	Well-trained and has professional skills			Acquired high skills through training and open to unlimited resources		
Degree of Danger	Min	Ave	Max	Min	Ave	Max
	H	VH	VH	VH	VH	VH

공격에 대한 위험 정도를 기존의 matrix를 기반으로 위 S케이스는 숙련된 능력을 요구하며 평균 및 최대 위험도는 조직적이고 숙련된 사람에 의해서 실행되기에 최고 점수를, 최소 위험도는 사이버 범죄자의 경우에는 공격에 대한 강제성이 부여되지 않아 한 단계 낮은 등급을 부여하였다.

3.3.2 랜섬웨어 사고에 대한 LEF (Loss event Frequency) 산출을 위한 지표

3.3.2.1 TEF, TCAP 산출을 위한 지표

TEP를 산출하기 위해 실제 A 금융회사에 5개월 동안 있었던 3757건의 공격 시도의 악성코드 및 공격 기법을 분석하여 Table 3.의 결과를 얻었다.

TCAP 산출을 위해 위협원을 참고하여 공격자의 능력이 중요하다는 것을 알 수 있었던 점에서 Gilbert Alaberdian 해커등급을 사용하였다[11].

Table 3. Table of criteria for TEF

Rating	Description (Monthly)
Very High(VH)	over 100 times
High(H)	30~99 times
Moderate(M)	10~29 times
Low(L)	1~9 times
Very Low(VL)	less then 1 or nothing happens

Table 4. Table of criteria for TCAP

Rating	Description (Hacker level)
Very High(VH)	Discover new vulnerability, Able to implement scripts
High(H)	Able to apply known scripts to targeting system
Moderate(M)	Able to modify scripts and understand hacking method
Low(L)	Able to attack as existing scripts are created for
Very Low(VL)	Able to execute simple hacking command and hacking program

3.3.2.2 RS 및 VUL 산출을 위한 지표

Table 5.는 A 금융회사의 보안체계를 기반으로 발생한 공격을 분석한 결과이며 VUL 산출을 위해서는 TCAP과 RS의 결과를 종합하여 산출하게 된다.

Table 5. Table of criteria for RS

Rating	Description (% passed among trial)
Very High(VH)	less then 2%
High(H)	3~10%
Moderate(M)	11~20%
Low(L)	21~30%
Very Low(VL)	31%

3.3.2.3 LEF 및 SLEF 산출을 위한 지표

LEF는 VUL에 의해 시나리오에 따라 지표의 변화가 필요하다. SLEF는 TEF와 SLE (secondary Loss Event)의 발생 확률이며 하루에 각 DDEI, Fire eye, V3를 통과한 수를 기반으로 산출하였다.

Table 6. Table of SLEF range

Rating	Range Low End	Range High End
Very High (VH)	90%	100%
High (H)	70%	90%
Moderate (M)	30%	70%
Low (L)	10%	30%
Very Low(VL)	0	10%

3.3.3 랜섬웨어 사고에 대한 Risk 산출 단계

3.3.3.1 PLM SLM 산출을 위한 지표

PLM과 SLM은 국내외 금융권의 정보보안 동향과 전망을 분석하여 다음 Table 7,8를 도출 하였다[12].

Table 7. Content of PLM for estimating loss amount

Loss Type	Cost
productivity	Productivity loss due to loss event
Response	Time spent in investigating and dealing with the event
Replacement & Restore	Replacement of systems or data might be required

Table 8. Content of SLM for estimating loss amount

Loss Type	Cost
Management	Incident involving sensitive customer information, management of costumer, business parter and ect.
Investment	In order to decrease the further attacks, additional investment is mandatory
Reputation	Reputation damage is a potential outcome from any breach of sensitive customer information

PLM의 손해 규모를 파악하기 위해 실제 랜섬웨어 공격에 의해 발생한 피해액을 기반으로 산출하였고 SLM 규모의 경우 랜섬웨어 공격 발생 시 대응하기 위한 금액을 기준으로 규정하였고 실제 과거 금융권에 대한 공격 발생 시 대응했던 영역을 산정 하였다. Table 9.과 같이 산출된다.

Table 9. PLM/SLM loss amount [unit: BTC]

Rating	Range Low End	Range High End
Very High (VH) (group)	153.1	-
High (H) (department)	51.1	153
Moderate (M) (team)	15.4	51
Low (L) (same work)	5.2	15.3
Very Low(VL) (person)	0.5	5.1

3.4 시나리오 별 OR(Overall Risk) 산출

Table 1.를 기반으로 4가지 시나리오를 구성하여 3.3에서 산출된 지표들을 기반으로 랜섬웨어 공격에 대한 OR을 산출하였다.

3.4.1 가능한 위험분석 시나리오

Table 10에서 CC는 Cyber Criminal이며 외부자, AP는 Authorized Personal이며 권한 있는 내부자, Threat type에서 MA는 Malicious Action이며 해킹 및 정보습득을 의미한다. Threat effect에서 A는 Availability이며 문서 암호화를 의미한다.

Table 10. Possible risk scenario's

NO	Risk Asset	Intimidator	Threat type	Threat effect
1	Management Plan Document	CC	MA	A
2	Management Support Document	CC	MA	A
3	Business Document	AP	MA	A
4	General Document	AP	MA	A

3.4.2 지표 적용을 통한 OR 산출

시나리오 1번의 TEF의 경우 월간 1~9회의 빈도를 보여 L이며 TCAP의 경우 해당 문서에 도달하기 위해서는 높은 수준의 실력이 요구되기 때문에 VH이다. 실제 5월 1달간 유입된 공격 457건을 분석하면 총 55건이 기본 보안 시스템을 통과하였고 이는 약 12.03%로 M이다. 이를 바탕으로 VUL을 산출한 결과 Table 11가 산출되었고 VUL은 VH로 책정 되었다.

LEF를 도출하기 위해 VUL과 TEF를 적용 하였을 때 Table 12과 같이 L이 도출된다.

LEF의 실제 통과된 공격들을 공격 유형별로 분석한 결과 피해 발생률이 2%로 산출되어 SLE%는 L로 측정되고 SLEF는 Table 13.와 같이 VL가 도출된다.

Table 11. Matrix method of VUL

TCAP	**VH**	VH	VH	VH	H	M
	H	VH	VH	H	M	L
	M	VH	H	M	L	VL
	L	H	M	L	VL	VL
	VL	M	L	VL	VL	VL
VUL		**VH**	**H**	**M**	**L**	**VL**
		RS				

Table 12. Matrix method of LEF

TEF	**VH**	M	H	VH	VH	VH
	H	L	M	H	H	H
	M	VL	L	M	M	M
	L	VL	VL	L	L	L
	VL	VL	VL	VL	VL	VL
LEF		**VH**	**H**	**M**	**L**	**VL**
		RS				

Table 13. Matrix method of LEF

LEF	**VH**	M	H	VH	VH	VH
	H	L	M	H	H	H
	M	VL	L	M	M	M
	L	VL	VL	L	L	L
	VL	VL	VL	VL	VL	VL
SLEF		**VH**	**H**	**M**	**L**	**VL**
		SLE%				

PLM은 인도 은행의 1개의 지점에 공격 발생 시 실제 발생한 대응 금액인 52 비트코인을 적용 하였고 SLM은 랜섬웨어 공격 발생 시 해당 문제의 추후 방지를 위한 컨설팅 비용을 책정 하였고 본 금액은 롯대 케미컬의 액시올 M&A 인수 실패로 인한 피해금액인 컨설팅 비용 3억을 기준으로 하여 375 비트코인을 산정 하였다. Table 9.을 통해 PLM은 H, SLM은 VH로 책정 되었다.

PLM, SLM, LEF, SLEF를 matrix에 적용하게 되면 Table 14.와 같이 PR과 SR은 M이 산출된다.

Table 14. Matrix method of PR/SR

P/SLM	**VH**	*M*	H	VH	VH	VH
	H	L	*M*	H	VH	VH
	M	VL	L	M	H	VH
	L	VL	VL	L	M	H
	VL	VL	VL	VL	L	M
PR(Light grey)/SR (Dark grey)		**VH**	**H**	**M**	**L**	**VL**
		LEF/SLEF				

Table 15. Matrix method of OR

SR	**VH**	VH	VH	VH	VH	VH
	H	H	H	H	VH	VH
	M	M	M	H	H	VH
	L	L	L	M	H	VH
	VL	VL	L	M	H	VH
OR		**VH**	**H**	**M**	**L**	**VL**
		PR				

Table 16. 4 Scenario result

No	TEF	TCAP	RS	VUL	LEF	SLEF	PLM	SLM	PR	SR	OR
1	L	VH	M	VH	L	VL	H	VH	M	M	H
2	VH	H	H	M	VH	M	VL (1 server)	VH (24 billion won) (3000 BCT)	M	VH	VH
3	VH	VL	VL	M	VH	VH	H (Thirty thousand won)	VL (177,152 won) (,0.2 BTC)	VH	M	VH
4	VH	VH	M	VH	VH	VL	VL (1 server)	VH (24 billion won) (3000 BCT)	M	M	H

산출된 PR과 SR을 바탕으로 OR을 산출하게 되면 Table 15.과 같이 H가 산출이 된다. 나머지 3개의 시나리오도 해당 방법을 통하며 OR을 산출하게 되면 Table 16과 같은 결과가 산출된다.

3.4.3 정량적 손해 금액 산출

정량적인 Risk를 산출하기 위해서는 FAIR 방법론에서 제공하는 Table 17, 18.를 통하여 산출한다.

즉, 시나리오 1-4를 해당 손해금액 산출식을 통하여 도출하면 Table 19.이 도출된다.

FAIR를 통해서 랜섬웨어가 금융 산업에 미칠 수 있는 사고를 논리적으로 분석하고, 발생 가능한 사고 손해 금액의 최솟값, 최댓값을 도출하였다.

Table 17. Method for estimating loss amount

Item	Amount	probability range		Expected value of damage
PLM	A	max	α	Axα
		min	β	Axβ
SLM	B	max	α'	Bxα'
		min	β'	Bxβ'

Table 18. Method for estimating final loss amount

Maximum value	Minimum value
(A×α) + (B×α')	(A×β) + (B×β')

본 연구결과에 따라 금융권의 리스크를 객관적으로 설명하여 실질적인 현황 파악 및 소통이 이루어 질 수 있다. 또한 공격에 따른 손해금액 발생구간을 예측하여 대책을 수립할 수 있다.

IV. 응용 및 검증

앞선 단계를 통하여 문재 발생 시 발생 가능 패해 금액을 확인하였다. 앞서 밝힌바와 같이 해당 기준을 통해 ISMS를 수정하는 것이 아닌 ISMS와 ISO 27001에서 제공하는 통제항목을 합리적인 의사결정을 통해 적용함으로서 패해 금액을 줄일 수 있다는 것을 검증 할 것이다. A 금융사에서 제공한 데이터 및 정보를 바탕으로 사내에 적용되고 있는 ISMS와 결합해 손해금액을 줄일 수 있는 방안을 확인해 본다.

Table 19. Final loss amount for each scenario

No	Risk type	Probability Range	Loss	Min Loss	Max Loss	Min Loss Total	Max Loss Total
1	primary	0.1~0.3	52	5.2	15.6	5.2	53.1
	secondary	0~0.1	375	0	37.5		
2	primary	0.9~1	5.1	4.59	5.1	904.59	2105.1
	secondary	0.3~0.7	3000	900	2100		
3	primary	0.9~1	57.13	51.417	57.13	51.867	57.63
	secondary	0.9~1	0.5	0.45	0.5		
4	primary	0.9~1	5.1	4.59	5.1	4.59	305.1
	secondary	0~0.1	3000	0	300		

4.1 금융업계의 현황

회사의 손해금액을 줄일 수 있는 방안을 모색하기 위해 대상 회사의 정보보안수준을 확인 한 결과 과거 금융업계에서 발생한 대규모 개인정보 유출 사태 이후 금융사들은 정보보호를 위해A 금융사는 많은 투자를 통해 정보보호 관리체계를 정착하였다. 실시간 공격에 대한 지속적인 분석을 통하여 변화하는 공격의 대책을 제시하고 지속적인 교육을 통해 위협에 방어 할 수 있도록 해 새로운 위협에 대응하고 있다. 그리고 전자센터와 백업센터를 통해 보유하고 있는 자산을 보호하며 수준급 보안 시스템을 구성하고 있다.

하지만 ISMS를 통한 보안의 경우 단순한 기준을 충족하기 위한 설비 증축, 정책 수립 및 교육 등이 진행 될 뿐 사이클의 본 목적인 ISMS의 발전은 이루지기 힘든 상황이며 이와 더불어 기존에 있는 통재의 활용이 아닌 새로운 기술이나 방법을 찾기 급급하다. 이러한 조치들은 과거에 발생하였던 정보유출 케이스만을 기반으로 구축되었으며 당시 대규모 투자를 통해 구축 가능한 기술적인 보안 기능은 다 설치했다고 볼 수 있다. 하지만 추후 유사 및 다른 유형의 문제가 발생 했을 시 이전과 같이 대규모의 무분별한 구매 및 설치는 이루어지기 힘들며 현재 초치들은 기술적인 조치에만 치우쳐 있다. 즉, 추가로 투자하지 않아도 되는 분야 에만 무분별하게 돈이 사용될 수 있고 이는 다양한 보안 이슈에 대한 보안이 아닌 기술적인 보안에서 그칠 수 있는 상황이 발생 할 수 있다.

앞서 도출된 피해금액을 바탕으로 운영진은 어떤 분야에 투자를 진행 시 최소의 금액으로 최대의 안전을 확보 할 수 있는지 결정을 할 때 하나의 의사결정 도구로서 사용 할 수 있음을 보일 것이다. 그리고 새로운 통제를 산정하지 않고도 FAIR를 통한 피해금액 산정 방법에 의해 산출된 내용을 기반으로 피해금액을 줄일 수 있음을 보인다.

4.2 손해금액 감축 방안

손해감소를 위해 Table 16.의 결과에 Table 20. 의 통합 통제 항목을 각각 적용해 H이상의 항목을 낮추는 방법을 사용 하였다. 시나리오 별 영향이 큰 항목을 통제 할 수 있는 도메인을 선정하였고 가장 많은 위험 등급을 보유한 영역에 통제항목을 적용하였다. 예로 적용된 항목의 경우:

1. 정보보호정책 (Information Security Policies):

Table 20. ISMS/ISO27001 integrated control item

No	Control item (ISMS)	Control item(ISO 27001)
1	Information security policy	Information security policy
2	Information security organization	Information security organization
3	Outsider security/Education and Training/Personal security	Human resources security
4	Information asset classification	Asset management
5	Access control	Logical security / access control
6	Cryptographic control	Encryption
7	Physical security	Physical and environmental security
8	Operation system/Review, monitor and audit	Operation system security
9	Electronic commerce security	Communication security
10	System development security	System introduction, development and maintenance
11	-	Supplier relationship
12	Security accident management	Information security incident management
13	Business continuity management	Business Continuity
14	-	Compliance to law

게시판 및 이메일 사용 시 보안 정책 준수,

8. 운영보안/악성코드 통제 (Operations security /Controls against malware): 각종 malware 탐지 분석 및 차단 시스템 구축을 통한 제어 ,
8. 운영 보안/정보 백업 (Operations security /Information Backup): 주요 문서 파일에 대한 백업 실시 항목을 적용하였다.

Table 21. Result after applying controls

No	Min loss total	Max loss total	Make secondary loss to 0	Min loss total	Max loss total
1	5.2	53.1		5.2	15.6
2	904.59	2105.1		4.59	5.1
3	51.86	57.63		51.41	57.13
4	4.59	305.1		4.59	5.1

정보보호 정책 및 악성코드 통제를 적용 하였을 시 가장 큰 피해액이 발생한 시나리오의 금액감소가 이루어지지 않았다. 이 이유는 랜섬웨어의 특성이 감염 후 패해가 주를 이룬다는 것인데 이는 주로 secondary loss 영역에 들어간다. 하지만 백업 구축 통제항목을 적용한 결과는 Table 21.과 같다.

Table 21.에서 볼 수 있듯이 통제 항목을 적용해 secondary loss를 0으로 만든 결과 손해금액이 대폭 감소하였다. Secondary Loss가 감소한 이유는 랜섬웨어에 감염이 된 후 문제가 발생하기 때문이다. 해당 결론이 실용적인 이유는 전체설비의 변경 및 이룰 수 없는 방법을 통해서 피해를 줄이는 것이 아니라 실제 가능한 통재항목 및 변화를 통해 문제를 어느 정도 해결 할 수 있다는 것이다. 즉, 백업 시스템의 구축을 통해 랜섬웨어에 대해 대비 할 수 있다고 볼 수 있다.

V. 결 론

랜섬웨어가 확산됨에 따라 공격 대상이 개인에서 단체로 변하게 되었다. 이에 랜섬웨어의 위협은 더 이상 무시 할 수 없게 되어 기존의 정보보호 관리체계를 보유한 회사들이 랜섬웨어 피해에 대한 예측을 하는 것이 필요했었다. 하지만 사고 발생 시 발생할 수 있는 피해액에 대한 분석방법론이 부재한 정보보호 관리체계의 한계로 인해 어떤 대응이 필요한지에 대한 고민만이 아닌 심지어 현재 보안체계가 이러한 공격에 대해 효율적인지 판단하는 것조차 힘든 상황이다. 따라서 본 논문에서는 시나리오를 기반으로 진행되는 FAIR 기반의 손실 측정모델을 통해 금융 산업에 랜섬웨어 공격이 미칠 수 있는 손실 및 위험을 확인하고 ISMS 및 ISO27001에서 제공하는 통제를 통해 백업 시스템의 구축이 secondary loss를 막아 손실금액을 줄여줄 수 있다는 사실을 확인 하였다.

이에 ISMS를 보유한 회사가 랜섬웨어의 리스크에 대한 피해규모 파악 및 합리적인 피해규모 산정이 가능하여 대비 할 수 있다는 점에서 의의가 있다.

References

[1] Naver encyclopedia of knowledg, . http://terms.naver.com/entry.nhn?docId=932418&cid=43667&categoryId=43667

[2] Kangyu Cho, Sangshik Min, Jaemo Seung, "Measures to promote countermeasures against electronic financial security threats," *KIISC*, 23(6), pp. 49-53, Dec. 2013

[3] Naver encyclopedia of knowledg, . http://terms.naver.com/entry.nhn?docId=3432095&cid=58437&categoryId=58437

[4] The Open Group, "Technical Guide FAIR - ISO/IEC 27005 Cookbook," Thames Tower 37-45 Station Road Reading Berkshire, RG1 1LX United Kingdom, pp. 1-52, Oct. 2010

[5] Jack Jones, "An Introduction to Factor Analysis of Information Risk (FAIR), Risk Management Insight", pp. 1-59, 2005

[6] Jang Ho, Yun, "FAIR-Based Loss Measurement Model for Enterprise Personal Information Breach," Advances in Computer Science and Ubiquitous Computing, Springer Singapore, pp. 825 - 833, Feb. 2015

[7] Jeong-Gyu Kim., Kyung-Ho Lee, "FAIR-Based Loss Measurement Caused by Personal Information Breach of a Company," *KIISC*, 27(1), pp 129-145, February 2017

[8] Le A., Chen Y., Chai K.K., Vasenev A., Montoya L. "Assessing Loss Event Frequencies of Smart Grid Cyber Threats: Encoding Flexibility into FAIR Using Bayesian Network Approach," LNICST vol 175, 2017

[9] Kim Mihee, "Major Security Vulnerabilities and Security Accident Trends in 2016," *Igloo Security*,

http://www.igloosec.co.kr/, Jan. 2017
〔10〕 J. Freund; J. Jones, "Measuring and Managing Information Risk: A FAIR Approach," book, pp. 17-201, 2015
〔11〕 Gilbert Alaberdian, "Hacker Society", *Neo Corporation,* Aug. 2000
〔12〕 kisong Lee, "Recent Trends and Prospects of Information Security in Domestic and Foreign Financial Sectors"", *KB Financial Group*, Mar. 2015
〔13〕 "What is Capability Maturity Model (CMM)? What are CMM Levels?",ISTQB EXAM CERTIFICATION

〈저자소개〉

윤 현 식 (Hyun-sik Yoon) 정회원
2014년 8월: 고려대학교 컴퓨터 통신 공학부 학사
2014년 9월~현재: 고려대학교 정보보호대학원 석사 과정
〈관심분야〉 위험관리, 정보보호 컨설팅, 정보보호 및 개인정보보호정책

송 경 환 (Kyung-hwan Song) 정회원
1997년 2월: 고려대학교 수학과 학사졸업
1997년 1월~현재: 국민은행 재직 중
2015년 9월: 고려대학교 정보보호대학원 석사 졸업
2015년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 정보보호, 금융보안, 시스템 및 네트워크 보안

이 경 호 (Kyung-Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사 졸업
2009년 8월: 고려대학교 정보경영대학원 박사 졸업
1994년 2월~2013년 12월: 삼성그룹, 네이버(주), 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 조교수, 부교수
〈관심분야〉 위험관리, 정보보호 컨설팅, 정보보호 및 개인정보보호정책