정 보 보 호 학 회 지
제26권 제4호, 2016. 8

사이버 레질리언스 국제표준화 동향과 이슈

김 정 덕*, 진 철 구**

요 약

사이버 위협이 고도화, 지능화함에 따라 사이버 보안사고를 사전에 예방하는 것에는 한계가 있으며, 이제는 보안사고 발생을 기정 사실화 하고 이로부터 얼마나 신속하게 사고를 탐지하고, 복구할 수 있는 역량을 구축하는 것이 필요하다. 이러한 현실적 필요성으로 인해 2010년경부터 레질리언스(resilience) 개념을 정보보안에도 접목시키려는 노력이 있었으며, 2016년 4월 템파에서 개최된 SC 27 회의에서도 사이버 레질리언스에 대한 국제표준화 작업이 많은 관심 속에서 논의되었다. 본 논문에서는 사이버 레질리언스에 대한 개념을 정리하고, 사이버 레질리언스 주요 모델과 구현 과제를 기술한다. 마지막으로 사이버 레질리언스 국제표준화 작업에서의 주요 이슈와 활동을 소개한다.

Ⅰ. 서 론

인터넷 사용자의 증가뿐만 아니라 ICBM(IoT, Cloud, Big data, Mobile)으로 대표되는 혁신적 기술발전으로 인해 새로운 유형의 디지털 비즈니스 모델이 개발되고 있다. 그러나 이러한 급격한 변화와 더불어 사이버상의 위협은 그만큼 높아지고 있다. 온라인 상의 공격은 매일 천만 건 이상 발생하고 있으며 연간 1천억 불 이상의 손실을 초래하고 있다. 사이버 레질리언스(cyber resilience)는 사이버 상의 부정적 사건 및 위협에도 불구하고 조직의 목표 성과(outcome)를 전달할 수 있는 역량(ability)을 의미한다. 조직 내 보안 활동이 시스템, 소프트웨어 또는 IT 부서만의 책임이 아님을 인식하고, 인간으로 부터의 위험에 대응하여 인텔리전스를 활용한 예방 조치와 교정 작업을 실천할 수 있도록 지원하는 활동을 의미한다.

사이버 레질리언스란 용어는 2012년 다보스에서 개최된 세계경제포럼(World Economic Forum, WEF)에서 사이버 레질리언스란 처음 사용한 이후, 개인, 기업, 국가 사회 전반에서 그 중요성이 점차 인식되고 있을 뿐만 아니라, 관심과 활용이 많아지고 있다[1]. 아직 학계에서는 관련 연구가 초기 단계라고 할 수 있으나 정치 또는 비즈니스 리더 사이에서 레질리언스란 용어가 많이 사용되고 있다. 2015년 10월 인도에서 개최된 JTC 1 SC 27 회의에서 사이버 레질리언스에 대한 국제표준화 준비 작업이 시작된 이후 표준 전문가의 많은 관심 속에서 진행되고 있다.

본 논문에서는 사이버 레질리언스에 대한 정의, 특성, 원칙 등에 관한 기존 연구들을 비교 분석하여 개념을 명확히 하고, 대표적 사이버 레질리언스 모델을 분석하여 레질리언스 구현을 위한 필요 요건 및 과제를 제시하고자 한다. 또한 사이버 레질리언스 국제표준화 노력에서의 이슈를 기술하고 향후 활동계획을 소개한다.

Ⅱ. 사이버 레질리언스 개념

2.1 정의

사이버 레질리언스에 대한 정의는 많은 전문가에 의해 다양하게 논의되고 있지만 가장 일반적이고 보편적인 정의는 다음과 같다[2][3]. ‘사이버 레질리언스는 부정적인 사이버 이벤트에도 불구하고 의도한 성과/결과물을 지속적으로 전달할 수 있는 능력(ability)을 의미한다’ 여기에서 주목할 것은 사이버 레질리언스는 능력이라는 점이며 이는 정보시스템, 비즈니스 기능, 조직, 지역 또는 도시, 국가 또는 사회, 또는 국제적 수준 등 다양한 차원에서의 능력을 의미할 수 있다. 지속적으로 전달한다는 것은 정상적인 전달 메커니즘이 실패하였을

* 중앙대학교 경영경제대학 산업보안학과 교수(jdkimsac@cau.ac.kr)
** 중앙대학교 일반대학원 융합보안학과 석사과정(raminez69@gmail.com)

때, 즉 위기 상황이거나 보안사고 발생 후에도 의도한 결과물을 제공할 수 있어야 함을 의미한다. 이는 정상으로의 복구도 포함한다. 부정적 사이버 이벤트는 자연재해 또는 인위적인 원인에 의해 네트워크로 연결된 IT 시스템, 관련 정보와 서비스의 기밀성, 무결성, 가용성에 부정적 영향을 미치는 모든 사건을 의미한다. 바로 이점에서 비즈니스 레질리언스와 구분을 할 수 있다. 사이버 레질리언스는 사고가 발생한 후 정상상태로의 조속한 복구 역량(회복력)도 중요하지만, 이를 위한 조직 내의 관련 부서(예: IT 운영부서, 보안부서, BCM 부서 등)간의 업무 협조를 기반으로 조직에 악 영향을 줄 수 있는 위협요인에도 사고가 발생하지 않도록 하고, 설령 사고가 발생해도 조속히 탐지해서 정상상태로 복귀할 수 있는 역량(면역력)을 강조하고 있다. 따라서 사이버 레질리언스는 곧 '사이버 면역·회복력'이라고 번역하는 것을 제안한다.

2.2 속성

사이버 레질리언스의 주요 속성을 파악하기 위해서는 사이버 보안과의 차이를 비교할 필요가 있다. 두 개념을 비교하면 [표 1]과 같다[2].

사이버 보안과 사이버 레질리언스를 구분 짓는 주요 속성 중 하나는 사이버 보안이 IT시스템 보호에 초점을 맞춘다면 사이버 레질리언스는 궁극적으로 비즈니스 결과물을 전달(business delivery)하고자 하는 데 있다. 따라서 사이버 레질리언스 노력은 정보기술보다는 비즈니스를 출발점으로 한다는 점이 극명하게 차이를 나게 하는 것이다. 위의 목표와 관련하여 바람직한 시스템의 속성을 보면, 사이버 보안은 실패를 허용하지 않는 시스템을 설계한다면, 사이버 레질리언스는 실패할 수 있음을 가정하고 그럼에도 불구하고 소기의 목표를 달성할 수 있도록 통제된 상황 속에서 실패도 극복할 수 있도록 설계한다.

〔표 1〕 Characteristics of cybersecurity vs. cyber resilience

	Cybersecurity	Cyber Resilience
Objective	Protect IT systems	Ensure business delivery
intention	Fail-safe	Safe-to-fail
Approach	security from the outside	Build security from within
Scope	One organization	Network of organizations

사이버 레질리언트하기 위해서는 해당 조직 뿐만 아니라 주위 환경에 대한 고려도 필요하다. 비즈니스와 IT 시스템을 주위 환경과 상호 연결된 네트워크로 보고 이를 단순히 위협의 원천으로 보기 보다는 강점과 약점을 보는 관점의 변화가 필요하다.

결국 사이버 레질리언스를 구축함으로써 위험 중심의 보안관리 역량을 강화하고, 평상시 보안 프로세스의 내재화를 통한 보안운영 역량, 비상시 신속한 대응과 정상으로의 복구를 위한 위기관리 역량이 요구된다고 할 수 있다.

2.3 원칙

디지털 비즈니스에서 사이버 레질리언스를 구현하기 위해서는 가트너에서는 다음과 같은 6가지 원칙을 제시하고 있다[5]. 첫째, 위험기반 의사결정을 채택하라는 것이다. 기존의 컴플라이언스 기반의 접근방법으로는 디지털 위험에 대응하기에 한계가 존재하기 때문에 위험을 최소화하기 위해서는 위험기반의 접근방법이 요구된다. 위험관리 대상은 정보자산에 대한 위험뿐만 아니라 비즈니스에 대한 영향까지의 분석을 포함하고 있다. 둘째, 비즈니스 성과 관점에서의 보안 노력이 요구된다. 디지털 비즈니스 환경에서는 IT 인프라 뿐만 아니라, 조직의 경영성과를 고려한 보안전략을 수립하여야 한다. 셋째, 능동적 조력자(facilitator) 역할 수행이 필요하다. 기존의 보안활동이 수동적인 보안관 역할에서 조직의 보안과 경영성과간의 균형을 유지하기 위한 능동적 조력자 역할로 변화하여야 한다. 넷째, 정보흐름을 이해하고 결정하여야 한다. 즉 디지털 비즈니스 환경에서 조직의 정보는 협력사, 디바이스, 네트워크 등에 분산되어 있기 때문에 모든 정보를 통제하는 것은 한계가 있다. 따라서 조직의 정보 흐름을 결정하고 이에 대해 지속적 경계와 능동적 대응이 필요하다. 정보유통 분석을 통해 정보에 대한 책임 권한 식별 및 할당이 가능하다. 다섯째, 인간 중심의 보안이 필요하다. 단순히 기술적 솔루션만으로 디지털 위험을 최소화하기에는 한계가 존재하며, 개인의 권한과 관련 책임을 중심으로 신뢰 기반의 인간 중심 보안 접근방법이 요구된다. 여섯째, 신속한 탐지 및 대응 전략을 수립하고 투자하여야 한다. 빠르게

변화하는 디지털 비즈니스 환경에서 모든 공격 유형에 대한 보안 조치를 구축 운영한다는 것은 현실적으로 불가능하며 오히려 손실 최소화를 위한 신속 탐지와 정상 복구 역량 구축을 위한 전략 수립과 관련 시스템에 투자해야 한다.

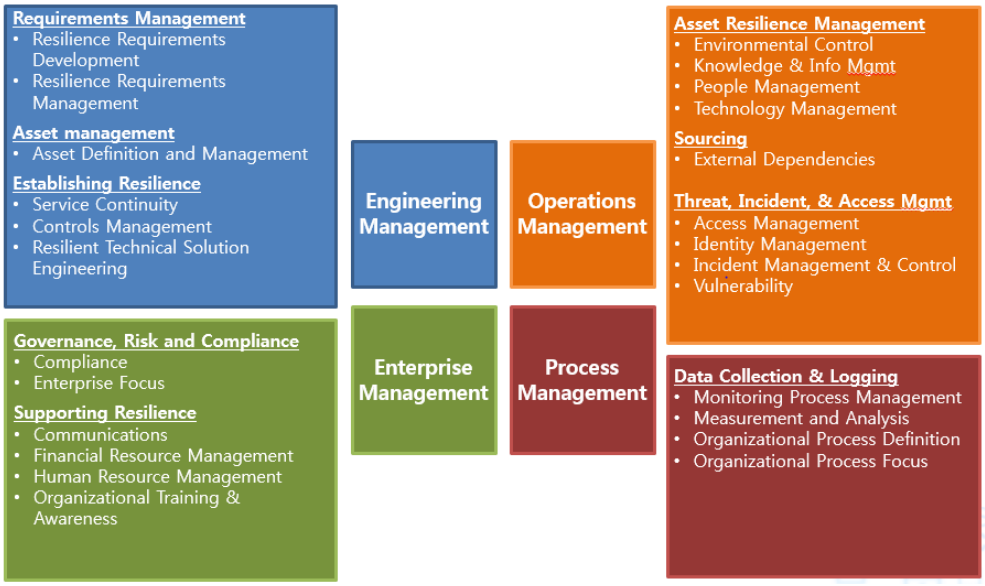
Ⅲ. 사이버 레질리언스 모델

사이버 레질리언스에 관한 대표적 모델은 카네기 멜론 대학의 CERT-Resilience Management Model (CERT-RMM)이다[6]. RMM의 범위는 기업의 핵심 자산인 인적자원, 정보(업무절차), 기술 및 시설을 포함한 레질리언스를 강조하고 있다. RMM은 통합적 관점에서 핵심 자산의 보호(protection)와 지속성 (sustainability) 보장을 위한 목표로 하고 있다. 레질리언스는 사전적 예방 성격의 보안대책과 신속한 탐지 및 사후적 복구 성격의 보안 대응이 융합되어 정보보호 면역·회복 체계를 구축하고, 이를 통해 조직의 미션을 달성하고자 한다.

RMM은 [그림 1]과 같이 4개 분야(엔지니어링 관리, 엔터프라이즈 관리, 운영 관리 및 프로세스 관리), 26개 프로세스 영역으로 구성되어 있다. 엔지니어링 관리 분야는 자산 및 비즈니스 프로세스, 서비스에 대한 레질리언스 수립과 구현을 위한 프로세스 영역으로, 요구사항 관리, 자산관리, 서비스연속성관리로 구성되어 있다. 엔터프라이즈 관리 분야는 거버넌스, 위험관리, 컴플라이언스, 재무관리, 인적자원관리 등 전사적인 차원의 관리 프로세스를 포함한다. 운영 관리 분야에는 접근관리, ID 관리, 사고관리, 취약점 관리, 아웃소싱 관리 등 보안운영 프로세스와 지식관리, 기술관리, 환경통제 등 전반적 자산의 레질리언스를 강조한다. 프로세스 관리 분야는 모니터링, 측정 및 분석, 조직 프로세스 정의 등 레질리언스 관리 프로세스의 측정, 관리 및 개선을 보장하기 위한 프로세스 영역들로 구성되어 있다. 프로세스 관리 분야의 목표는 레질리언스의 지속적인 개선이며, 이를 위해 각 프로세스 영역이 반복적으로 수행된다.

미국 연방정부에서는 CERT-RMM 모델을 기반으로 Cyber Resilience Review(CRR)를 개발하여 국토안보부(DHS) 주도로 연방정부에 적용하고 있다[7]. CRR은 10개의 영역(자산관리, 보안대책관리, 구성 및 변경관리, 취약점관리, 사고관리, 서비스연속성관리, 위험관리, 외부의존도관리, 훈련 및 인식제고, 대내외환경 분석)에 기초하여 총 42개의 목표(goal)과 167개의 실천사항(practices)들이 포함되어있다. 각 도메인별로 달성하고자 하는 목적이 명시되어 있으며 특정 목표와 관련된 실천사항들을 통해 조직의 사이버 레질리언스 역량들을 측정할 수 있도록 한다.

측정 방법은 우선적으로 각 도메인별 실천사항에 대한 수행 여부를 “예”, “아니오”, “일부 수행”으로 구성



〔그림 1〕 Domains of CERT-RMM Processes

된 3가지의 답변을 통해 수치화 한다. 이를 기반으로 각 목표별 해당 질문 수 대비 실천사항 수행 여부를 “달성”, “달성하지 못함”, “일부 달성”으로 답변하여 결과를 도출한다. 최종적으로 각 목표별 달성 결과를 성숙도 지표 수준(maturity indicator level, MIL)으로 조직의 사이버 레질리언스 역량에 대한 수준을 정의한다. 이때, 상위 단계 요구사항을 만족하더라도 하위 단계 요구사항을 충족시키지 못한다면 낮은 수준을 적용한다. CRR을 수행한 조직은 정의된 수준을 활용하여 문제점을 식별하고 gap분석을 통해 선결과제를 우선 순위화하며 이를 개선하기 위한 계획을 세울 수 있다.

Ⅳ. 사이버 레질리언스 과제

디지털 비즈니스 환경에서 사이버 레질리언스를 위해서는 무엇보다도 조직과 관련된 위험 기반의 보안 활동을 중심으로 하는 관리역량이 필요하다. 즉, 기존의 정보보호 조직 또는 IT조직이 수행하던 정보자산 중심의 위험관리가 아닌 서비스 차원의 위험이 식별된다. 따라서 정보자산을 활용하는 현업부서가 위험관리 프로세스에 참여해야 하고, 이와 관련된 대내외 요구사항에 따라 보호대책을 수립해야 효과적인 위험관리가 가능할 것이다. 또한 전사적 정보보호 활동을 위해 조직 및 인력의 정보보호 활동에 대한 평가, 교육 프로그램 수립 및 효과성 측정, 보호대책의 적합성 평가 등을 제도화하여 레질리언트 보안의 기반이 될 수 있는 관리역량을 확보하고, 정보보호 수준의 지속적 개선을 유도해야 한다.

기존의 시스템에 대한 접근통제, 물리적 보호조치 등과 같은 예방적인 정보보호 통제는 기술적 솔루션 도입에 초점이 맞추어져 이행점검과 같은 일상적인 운영활동에 미흡한 부분이 많았다. 이 때문에 일부 조직에서는 보안사고가 발생하였는지 인지가 어렵거나, 동일한 유형의 보안사고가 반복 발생하는 경우가 존재한다. 따라서 건실한 면역체계를 구축하기 위해서는 자동화 및 상호운영성을 기반으로 역량 있는 담당자가 적절한 업무절차에 따라 필요한 도구/SW를 활용하여 업무를 처리할 수 있는 운영 프로세스가 정립되고 내재화되어야 한다.

보안사고를 사전에 완벽히 예방하는 것이 불가능하다면, 보안사고 발생 시 이를 신속히 탐지하고, 원래의 상태로 회복하는 것이 중요하다고 할 수 있다. 조직의 보안위협, 취약성에 따른 이상 징후를 신속하게 탐지하고 대응하기 위해서는 지속적인 모니터링과 분석 활동이 반드시 수반되어야 한다. 디지털 비즈니스 환경에서는 업무 효율성 및 사용자의 편의성을 제한하는 보안 솔루션의 적용이 어려우므로, 최소한의 예방 통제와 신속한 탐지 및 대응체계가 함께 고려되어야 한다. 이때 외부의 전문기관과의 협력관계 및 집단지성(collective intelligence)를 통해 최근 위협 및 취약점 유형, 공격방법 등에 대한 다양한 정보를 제공받을 수 있으며, 보안사고에 대한 증거확보 및 법적 대응이 가능할 것이다. 결국 위와 같은 활동들은 조직의 위기 및 재난관리 프로그램과 연계되어야 보안사고 발생 시 조직의 비즈니스 연속성을 유지할 수 있을 것이다.

Ⅴ. 사이버 레질리언스 국제표준화 이슈

급격한 비즈니스 및 기술 환경 변화로 인한 사이버 레질리언스 구현에 대한 요구사항이 점차 확대됨에 따라 사이버 레질리언스의 범위, 개념, 구현모델, 구현 메커니즘 등에 연구 및 표준화 작업이 필요하다.

이에 따라 JTC 1 SC 27 WG 1에서는 사이버 레질리언스 국제표준화 작업에 대한 준비단계를 진행하고 있다. 2015년 10월 인도회의에서 사이버 레질리언스 국제표준화 작업이 논의되기 시작되어 2016년 4월 미국 탬파회의에서는 스웨덴을 위시한 유럽, 미국, 일본, 한국 등 많은 전문가들의 기고문을 바탕으로 용어 정의 및 표준화 전략 등을 논의하였다. 회의 결과, 3명의 Rapporteur가 선임되었고 2017년 4월까지 SP(study period)를 연장하여 충분한 논의를 진행 중에 있다. 다음 10월 회의를 위해 전문가 기고 요청사항으로는 사이버 레질리언스의 용어 정의 및 수준, 부정적 영향을 주는 위협요인 식별, 관련 국제표준 중 참고해야 하는 표준의 식별과 향후 사이버 레질리언스 국제표준화 전략에 대한 전문가 의견을 요청하고 있다.

레질리언스 관련 표준은 SC 27에서 27001, 27002, 27013, 27031, 27035, 27036-1 등이 관련되어 있으며, ISO/TC 292에서의 표준인 ISO 22301을 비롯하여 ENISA, NIST, DHS, CERT-RMM, ASIS SPC.1-Organizational resilience: Security 등이 있다[8-19]. 이 중 본 프로젝트에 필요한 표준은 어떤 것이며, 어떻게 이를 활용할 것인가, 또한 기존 표준과 어떻게 차별화할 것인가에 대한 기고문 개발이 필요하다.

본 프로젝트의 중요성에 따라 국내에서도 적극적인 기고문 활동과 국제표준회의 참가를 통해 사이버 레질리언스에 대한 글로벌 선진사례를 적극 수용하면서 한국 측 의견을 반영할 수 있어야 하겠다.

참 고 문 헌

[1] World Economic Forum, “Partnering for Cyber Resilience”, 2012

[2] Fredrik Bjorck, et al, “Cyber Resilience-Fundamentals for a Definition”,Advances in Intelligent Systems & Computing, 2015

[3] Ernst & Young, “Achieving Resilience in the Cyber Ecosystem”, 2014

[4] Springer, “New Contributions in Information Systems and Technologies”, pp.313-315, 2015

[5] Gartner, “Use Six Principles of Resilience to Address Digital Business Risk and Security”, 2015

[6] Carnegie Mellon, “CERT® Resilience Management Model, Version 1.0”, 2010

[7] Dept. of Homeland Security, “Cyber Resilience Review(CRR):Method Description and Self-Assessment User Guide”, 2016

[8] ISO/IEC 27001:2013, ”Information Security Management Systems - Requirements”, 2013

[9] ISO/IEC 27002:27013, “Code of Practice for Information Security Controls”, 2013

[10] ISO/IEC 27013:2015, “Guidance on the Integrated Implementation of ISO/IEC 27001 and ISO/IEC 20000-1”, 2015

[11] ISO/IEC 27031:2011, “Guidelines for Information and Communication Technology Readiness for Business Continuity”, 2011

[12] ISO/IEC 27035:2011, “Information Security Incident Management”, 2011

[13] ISO/IEC 27036-1:2014, “Information Security for Supplier Relationships – Part 1: Overview and Concepts”, 2014

[14] ISO 22301:2012, “Societal Security – Business Continuity Management Systems – Requirements”, 2012

[15] ENISA, “Security and Resilience in eHealth, Security Challenges and Risks”, 2015

[16] ENISA, “Security and Resilience of Smart Home Environments, Good Practices and Recommendations”, 2015

[17] NIST, SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations”, 2013

[18] NIST, “NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide”, 2012

[19] ASIS SPC.1-2009, “Organizational Resilience: Security, Preparedness, and Continuity Management Systems-Requirements with Guidance for Use”, 2009

〈저 자 소 개〉

김 정 덕 (Jungduk Kim)
종신회원

1979년 2월 : 연세대학교 정치외교학과 졸업
1981년 8월 : 연세대학교 경제학과 석사
1986년 5월 : University of S. Carolina, MBA
1990년 12월 : Texas A&M University, Ph.D. in MIS
1995년 3월~2014년 8월 : 중앙대학교 정보시스템학과 교수
2014년 9월~현재 : 중앙대학교 산업보안학과 교수
<관심분야> 디지털 비즈니스 보안, 사이버보안 거버넌스 및 관리

진 철 구 (Chulgu Jin)
학생회원

2009년 2월 : 중앙대학교 정보시스템학과(학사)
2015년 3월~현재 : 중앙대학교 융합보안학과(석사과정)
<관심분야> ICT 공급망 보안, 사이버보안 거버넌스 및 관리