정 보 보 호 학 회 지
제25권 제4호, 2015. 8

자율규제 환경에서의 정보보호 혁신을 위한 고려사항

김 정 덕*, 김 보 경**, 박 수 형**, 김 건 우***

요 약

IT 기술의 발전과 법·규제 등 비즈니스 환경의 변화에 따라 기존의 정보보호 접근방법에 대한 변화의 필요성이 대두되고 있다. 다양한 정보보호 노력에도 불구하고 정보보호의 발전 속도는 IT 기술의 급속한 변화를 따라가기 어려운 실정이며, 끊임없이 발생하는 보안사고는 예방 중심 보안체계의 한계를 보여주고 있다. 최근 금융권에서부터 자율규제에 대한 논의가 이루어지고 있으며, 이러한 변화에 따라 정보보호의 효율성과 효과성뿐만 아니라 비즈니스의 지속가능성을 동시에 만족시키기 위한 혁신적인 관점에서의 새로운 접근방법이 요구되어진다. 본 고에서는 정보보호 혁신 모델을 통하여 자율규제 환경에서의 정보보호의 새로운 접근방법 구현을 위해 고려해야 할 사항들을 제시한다.

Ⅰ. 서 론

IT 환경이 급속도로 변화하는 현재의 디지털 융·복합 시대에서 금융과 ICT의 결합을 통해 등장한 핀테크(FinTech)에 대한 관심이 고조되고 있다. 또한 미래창조과학부에서 발표한 “2015년도 과학기술· ICT 분야 연구개발사업 종합시행계획”에 따르면 데이터 경제 시대의 새로운 성장 동인인 ICBM(IoT, 클라우드, 빅데이터, 모바일)이 향후 ICT산업 성장을 견인할 것으로 기대하고 있다[1]. 따라서 ICT 환경의 변화는 비즈니스 환경의 변화에 기인할 것이며, 데이터 처리 및 업무 방식의 변화는 새로운 정보보호 접근방법으로의 변화를 요구한다고 할 수 있다.

전 세계적으로 정보보호 산업은 지속적으로 증가하는 추세를 보이지만 여전히 기술적 솔루션에 대한 의존도가 높은 것으로 나타났다. Gartner의 조사에 의하면, ‘15년도 전 세계 정보보호 산업 규모는 전년도 대비 8.2% 증가된 약 760억불이며, 정보유출 방지를 위한 솔루션 중에 하나인 DLP(Data Loss Prevention)는 18.9% 증가할 것으로 예상하고 있다[2]. 이것은 여전히 정보유출 등의 보안사고를 우려한 나머지 예방 중심의 기술적 보안대책에 대한 구매에 초점이 맞춰져 있기 때문이다. 그럼에도 불구하고 보안사고가 지속적으로 발생함에 따라 기존의 정보보호 접근방법의 실패론까지 대두되고 있다[3].

한편 APT와 같은 지능화된 보안위협 또한 증가하고 있으며, 정보보호에 대한 많은 노력에도 불구하고 정보보호의 발전 속도는 IT의 급속한 발전과 환경 변화를 따라가기 어려운 실정이다. 또한 보안 위협의 대상은 조직의 정보자산 뿐만 아니라 개인에게까지 확대되고 있으며, 향후에도 점차 고도화된 보안위협이 지속적으로 나타날 것으로 예상된다. 이로 인한 보안사고는 완전히 예방할 수 없으며, 신속한 탐지 및 대응의 중요성이 부각되는 것이 최근의 추세이다[4].

우리나라의 경우, ‘13년 3.20 대란, ‘14년 카드사 개인정보 유출사고 등 매년 대형 보안사고가 발생하고 있으며, 이것은 법률에서 요구하는 최소한의 보안활동, 예방 중심의 기술적 보안솔루션 운영에 한계가 존재함을 의미한다. 이러한 문제와 더불어 최근 금융권에서 이슈화되고 있는 자율규제는 능동적이고 지속가능한 정보보호 접근방법의 필요성을 요구하고 있다. 결국 균형 잡힌 정보보호를 위해서는 지속적인 위험 탐지와 신속한 복구역량을 강화함으로써 다양한 보안위험에 대한 대응력을 확보할 수 있다는 것이다.

따라서 ICT 및 비즈니스 환경변화에 신속히 대응하기 위해서는 법·규정 등에 대한 컴플라이언스 기반의

본 연구는 미래창조과학부 및 한국인터넷진흥원의 “고용계약형 정보보호 석사과정 지원사업”의 연구결과로 수행되었음
* 중앙대학교 경영경제대학 산업보안학과 교수(jdkimsac@cau.ac.kr)
** 중앙대학교 일반대학원 산업융합보안학과 석사과정(skybluebk88@gmail.com, suhyung77@gmail.com)
*** 중앙대학교 일반대학원 융합보안학과 박사과정(kunwoo.kim317@gmail.com)

최소한의 보안활동이 아닌 비즈니스와 연계된 위험 기반 자율적 정보보호 체계 수립이 필요하다고 할 수 있다. 이에 본 고에서는 현재의 정보보호 접근방법의 한계를 극복하고, 나아가 정보보호 혁신을 위한 고려사항을 제시하고자 한다.

Ⅱ. 정보보호 혁신을 위한 접근방법

2.1. 혁신 이론

혁신이란 기존의 틀이나 형식을 바꾸어 새롭게 한다는 의미로, 기존 방법의 개선이 아닌 새로운 접근방법을 시도해야 한다는 것이다. 혁신에 대한 연구는 1934년 Schumpeter에 의하여 시작되었으며[5], 이후 시장지향 관점과 자원지향 관점으로 나누어 연구되었다. 특히 Rothwell & Zegveld는 시장 견인(Market Pull)과 기술 공급(Technology Push)의 결과를 혁신으로 해석하고 있으며[6], Kelly & Kranzberg는 혁신을 필요에 대응하는 종속적인 상황, 참신한 창의 활동 등을 포함하는 관리 과정으로 설명하고 있다[7]. 위와 같은 연구는 혁신에 대한 개념 및 구성요소 간의 관계에 대하여 중점적으로 연구한 반면에 혁신이 어떠한 계기로 필요하게 되었는지, 구체적으로 어떠한 방법으로 달성할 수 있는지에 대한 설명이 부족하다고 할 수 있다.

한편 2005년 ISPIM(International Society of Professional Innovation Management)에서 소개된 혁신 큐브(Innovation Cube)는 혁신의 계기와 목적으로부터 기회를 도출하는 TDE(Trigger, Driver, Enabler)접근방법을 통하여 혁신의 메커니즘을 설명하였다[8]. 예를 들어, 시장 상황의 변화와 파괴적 기술의 등장은 혁신의 계기가 되고, 조직의 목적인 경쟁우위를 점하기 위한 방법으로써 가격과 신속성이라는 기회를 도출할 수 있다. 그리고 결국 조직은 역량과 자원을 투입하여 기회를 구체화함으로써 혁신을 달성할 수 있다. 따라서 상기와 같은 접근방법을 통해 현재의 정보보호 환경을 분석하여 정보보호 혁신을 위한 고려사항을 도출 할 수 있다.

2.2. 정보보호 혁신 모델

혁신을 위해서는 우선적으로 혁신의 기회를 찾아야 하고 그 다음 이를 가능하게 하는 메커니즘을 도출해야 한다. 본 고에서는 혁신의 기회를 찾고 이를 구현하기 위한 요소를 도출하기 위해 TDE(Trigger, Driver, Enabler)접근방법을 사용하였다[8]. 즉 정보보호의 혁신을 위해서는 현재의 정보보호 접근방법의 변화를 유도하는 계기 또는 환경 변화요인(Trigger)과 정보보호가 궁극적으로 달성하고자 하는 목적(Driver)을 고려하여 혁신의 기회를 도출할 수 있다. 즉 정보보호 목적 달성을 위해 정보보호 환경변화가 어떠한 혁신의 가능성을 제공하느냐하는 점을 파악해야 하고 도출된 혁신 기회를 구현하게 하는 메커니즘(Enabler)을 제시해야 한다.

Trigger는 환경 변화로 인해 혁신의 필요성을 나타나게 하는 요인으로서 대표적 환경인 기술과 시장 환경의 변화를 고려할 수 있다. 우선 기술 환경은 ICBM으로 대표되는 파괴적 기술(Disruptive Technology)의 출현을 고려해야 할 것이다. 이러한 신기술 출현에 따라 기존에 없었던 새로운 정보보호 위험을 초래하기도 하지만 이러한 신기술을 활용함으로써 새로운 정보보호 대책도 가능하게 할 수 있는 기회를 고려해야 한다. 즉 클라우드 기술을 적용한 SecaaS(Security as a Service), 빅데이터 분석기술을 활용한 보안분석(Security Analytics) 등 새로운 보안대책도 개발 가능하다.

시장 환경의 변화에서 가장 주목할 만한 현상은 자율규제 등장에 따른 규제의 중심이 사전 규제에서 사후규제로 변화되고 있다는 점이다. 전통적인 정보보호 접근방법으로는 보안사고를 예방하기 위한 정부차원에서의 규제 강화가 심화되었으며, 기업 차원에서는 이를 준수하기 위한 기술적 솔루션 중심의 보안통제 구축이 주를 이루었다. 그러나 이는 사용자의 불편을 야기하였으며, 업무 효율성과 상충되는 경우가 많았다. 또한 이러한 상황에서도 보안사고는 계속해서 발생하고 있기 때문에 민간 중심의 자율적인 보안체계 구축의 필요성이 대두되고 있으며 이것이 곧 자율규제의 핵심이라고 할 수 있다. 이러한 환경의 변화는 비즈니스의 변화에 기인하고 결국 정보보호 혁신을 요구하는 계기가 될 것이다.

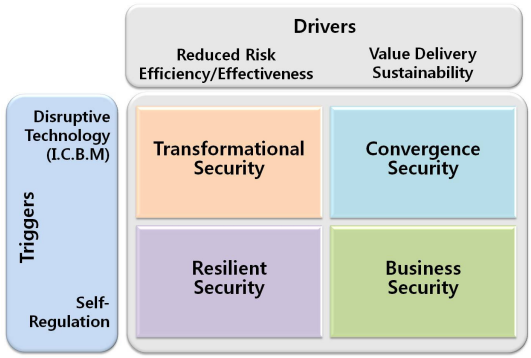
Driver는 정보보호를 통해 궁극적으로 달성하고자 하는 목적 또는 존재 이유(Reason of Being)로서 다음과 같은 스펙트럼 상에서 두 가지 목적으로 구분할 수 있다. 즉 정보보호 활동을 통해 보안사고로 인한 손실(위험)의 가능성을 최소화하며 이를 위한 정보보호 운

영의 효율성과 효과성을 도모하는 것이다. 이는 전통적이면서 비교적 수동적 입장에서의 정보보호 목적이라고 할 수 있다. 다른 측면은 정보보호 활동을 통해 비즈니스에 가치를 창출, 전달하고 이를 통해 기업의 지속가능성을 지원하는 것이다. 최근 디지털 비즈니스가 확대됨에 따라 정보보호가 고객의 신뢰와 자신감을 높임으로써 새로운 고객 유치 수단으로서 활용되고 있으며, 지속적 경영을 위한 노력에 중요한 부분을 담당하고 있는 추세가 곧 이러한 긍정적 가치 전달의 좋은 예라고 할 수 있다.

이러한 기술 및 시장 환경의 변화와 정보보호의 목적이라는 관점에서 보면 Fig. 1.과 같이 4 가지 혁신 기회인 변혁적 보안(Transformational Scurity), 융합보안(Convergence Security), 레질리언트 보안(Resilient Security), 비즈니스 보안(Business Security)을 도출할 수 있다.

첫 번째 혁신 기회인 변혁적 보안은 기술 환경 변화에 따른 효과적인 위험 완화를 위한 접근방법이다. IT 기술의 발달에 따라 예방 중심의 보호대책은 한계가 존재하기 때문에 효과적인 위험 완화를 위하여 신속한 탐지 및 대응 관점에서 접근해야 할 필요가 있다. 현재의 모바일, 클라우드 환경 하에서는 과거와는 비교할 수 없을 정보도 많은 데이터가 생성되고 처리된다. 이와 같은 환경에서는 빅 데이터 기법을 활용하여 과거와는 비교가 안 될 정도의 대규모 정보를 빠른 시간 안에 분석하는 것이 가능하며, 이를 통하여 새로운 보안위협을 사전 예측하는 것이 가능할 것이다[9].

두 번째 혁신 기회인 융합보안은 기술 환경 변화에 따른 지속적이고 안정적인 환경, 제품 및 서비스를 제공하기 위한 접근방법이다. IoT와 핀테크의 등장으로 융·



〔그린 1〕 Security Innovation Opportunities Model

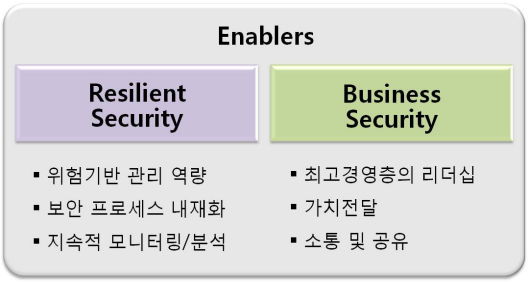
복합적인 보안 위협도 등장하고 있으며, 이러한 위협은 과거 조직의 정보자산을 포함하고 점차 개인적인 피해로 확대될 수 있다. 따라서 효과적인 융합보안 체계를 구축하여 안전한 환경에서 근무하고, 고객이 신뢰할 수 있는 제품과 서비스를 제공하는 것은 기업의 지속경영을 위해 정보보호가 제공하는 궁극적인 가치라고 할 수 있다.

세 번째 혁신 기회인 레질리언트 보안은 자율규제 환경에서 효과적인 위험 완화 및 정보보호 운영 탁월성을 위한 접근방법이다. 정부주도의 사전규제에서 자율규제로 경영환경이 변화함에 따라 기존의 규제 중심의 정보보호 활동에서 벗어나, 기업 고유의 위험에 대응하기 위한 자율역량이 요구되어지며, 신속한 탐지 및 정상 복구를 강조하는 면역·회복력(Resilience) 관점에서의 접근이 필요하다. Resilience는 원래의 상태로 되돌아가려는 특성을 의미하는데, 신속한 회복력도 중요하지만 정상상태를 유지하고 재발방지를 위한 면역체계도 함께 고려되어야 한다. 즉, 위험 중심의 자율통제를 위한 관리역량을 강화하고, 평상시 운영의 탁월함을 위한 정보보호 프로세스의 내재화, 비상시 신속한 대응과 정상으로의 복구를 위한 위기관리 역량이 요구된다.

네 번째 혁신 기회인 비즈니스 보안은 자율규제 환경에서 지속적으로 정보보호의 가치를 전달하기 위한 접근방법이다. 이를 위하여 최고경영층의 리더십을 기반으로 비즈니스와 연계된 정보보호 활동을 위한 전사적인 차원에서의 거버넌스 체계 수립이 필요하다고 할 수 있다. 그리고 비즈니스의 연계, 주기적인 보호대책의 효과성 평가를 통해 정보보호의 긍정적인 가치를 전달할 수 있을 것이다. 비즈니스와의 연계는 정보보호 조직의 노력만으로 달성할 수 없다. 내부적으로는 위험관리 현황, 정보보호 수준 등에 대한 소통 및 공유, 협업의 정보보호 활동 참여가 필요하며, 외부적으로는 전문기관과의 긴밀한 협력체계를 구축하여 보안사고 발생 시 효과적으로 대응함으로써 비즈니스 연속성 유지에 기여할 수 있을 것이다.

Ⅲ. 자율규제 환경 하에서의 정보보호 혁신을 위한 고려사항

자율규제 환경에서의 혁신 기회인 레질리언트 보안과, 비즈니스 보안을 가능하게 하기 위해서는 Fig. 2.와 같은 Enabler를 고려해야 한다.



〔그림 2〕 Enablers for Resilient & Business Security

3.1. 레질리언트 보안

자율규제 환경에서 균형 잡힌 정보보호를 위해서는 무엇보다도 조직과 관련된 위험 기반의 정보보호 활동을 위한 관리역량이 필요하다. 즉, 기존의 정보보호 조직 또는 IT조직이 수행하던 정보자산 중심의 위험관리가 아닌 서비스 차원의 위험이 식별되고 이와 관련된 정보자산을 활용하는 현업이 위험관리 프로세스에 참여해야 하고, 이와 관련된 대내외 요구사항에 따라 보호대책을 수립해야 효과적인 위험관리가 가능할 것이다. 또한 정보보호 활동을 위한 조직 및 인력에 대한 제도화를 통해 정보보호 활동에 대한 평가, 교육 프로그램 수립과 효과성 측정, 보호대책의 적합성 평가 등을 통해 레질리언트 보안의 기반이 될 수 있는 관리역량을 확보하고, 정보보호 수준의 지속적인 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 지속 발생하는 경우가 존재한다. 따라서 건실한 면역체계를 구축하기 위해서는 자동화 및 상호운영성을 기반으로 역량 있는 담당자가 적절한 업무절차에 따라 필요한 도구/SW를 활용하여 업무를 처리하는 운영업무 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 이상징후를 신속하게 탐지하여 대응하기 위해서는 지속적인 모니터링과 분석 활동이 반드시 수반되어야 한다. 자율규제 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 이슈가 되는 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.

3.2. 비즈니스 보안

정보보호의 역할이 비즈니스 목표 달성을 지원하는 것이라면, 비즈니스에 긍정적인 가치를 제공하지 않는 정보보호는 의미가 없을 것이다. 다른 한편으로는 정보보호 활동이 단순히 업무에 대한 지원에서 벗어나 비즈니스에 전략적 우위를 창출하고, 신사업을 가능하게 하는 긍정적 영향 또는 가치를 제공할 수 있는 기회를 실현시켜야 할 필요가 있다. 정보보호 활동이 업무와 연계됨으로써 전사적 보안을 실현하고 궁극적으로는 긍정적인 정보보호 문화를 정착시킬 수 있을 것이다. 비즈니스와 정보보호의 연계는 거버넌스 차원의 이슈이며, 정보보호 거버넌스의 핵심 주체인 최고경영진의 리더십이 필수라고 하겠다. 이를 위해서 거버넌스 활동의 핵심인 CISO의 책무가 정의되어야 하고, CEO의 책임 하에 CIO 등 정보보호 관련 임원들의 명확한 역할 및 책임 정의가 가장 우선적으로 수행되어야 하며, 현업 임원들이 참여한 최고경영층의 리더십을 통해 정보보호활동을 경영전략에 연계시키기 위한 노력이 필요하다.

정보보호의 가치는 재무적 또는 비재무적으로 평가되어야 하며, 이를 통해 궁극적으로 정보보호가 비즈니스에 제공하는 긍정적인 가치를 도출할 수 있다. 따라서 비용 효과적 정보보호를 위한 객관적인 투자 타당성 평가, 계획에 따른 예산 편성 및 적절한 자원할당이 수반되어야 하며, 이를 기반으로 한 정보보호 활동은 주기적으로 평가되어야 하고 경영 성과체계에 반영되어야 한다.

기존의 정보보호 활동이 정보보호 전담부서, IT 부서 위주로 수행되었다면, 비즈니스와 연계된 전사차원의 정보보호를 위해서는 현업의 참여 및 긴밀한 소통과 정보보호 현황공유가 필수적이라 할 수 있다. 조직 내부

적으로는 최고경영층으로 구성된 위원회의 역할 및 운영이 필요하며, 조직 외부적으로는 복잡해지는 비즈니스 환경을 고려한 다양한 파트너사와의 협업체계 구축이 필요하다. 특히 최고경영층으로 구성된 위원회는 전사적 정보보호 활동 수행 시 발생 가능한 다양한 이해갈등을 조정하고, 현업 관리자의 참여를 유도하기 위한 핵심적인 거버넌스 기능을 수행한다고 할 수 있다. 또한, 정보보호 포털시스템 등과 같은 채널을 이용하여 경영층을 포함한 모든 임직원이 정보보호 현황을 공유하고, 자신의 업무와 관련된 보안위험을 인지하여 능동적인 정보보호 활동을 가능하게 해야 한다. 이러한 비즈니스 보안을 구축함으로써 긍정적인 정보보호 문화를 정착시킬 수 있을 것이다.

Ⅳ. 결 론

본 고에서는 TDE(Trigger, Driver, Enabler) 접근방법을 통하여 자율규제 환경에서의 정보보호 혁신을 위한 고려사항을 제시하였다. IT의 급속한 변화와 비즈니스 환경의 변화에 따라 기존의 정보보호 접근방법에는 한계가 존재하며 새로운 관점에서 접근할 필요가 있다. 예방 중심의 보호대책은 기술적인 보안 솔루션 구축 및 운영에 비용 측면의 부담이 될 수 있으며, 업무 효율성 및 고객 편의성에 부정적인 영향을 줄 수 있다. 또한 법·규정 등 외부 요구사항에 대한 컴플라이언스 기반의 보호대책은 비즈니스 상에 존재하는 다양한 보안위험을 모두 반영하기에 한계가 있으며, 이러한 단편적인 보호대책은 지속적인 개선이라는 정보보호의 철학과도 차이가 존재한다.

따라서 앞으로 다가올 자율규제 환경에서는 조직에 특화된 위험 기반의 접근방법과 비즈니스와 연계된 보호대책 수립이 요구되어진다. 효과적인 위험관리를 위해서는 정보보호 운영 프로세스를 내재화하여 지속적으로 정보보호 활동을 평가해야 하며, 이때 정보자산과 비즈니스 프로세스를 통합한 관점에서 식별된 위험은 지속적으로 모니터링 되어야 한다. 효과적인 정보보호 및 비즈니스와의 연계를 위하여 최고경영층의 정보보호 활동 참여가 필수적이며, 리더십을 발휘하여 다양한 갈등을 조정하고 지속적인 소통 및 공유를 통해 현업의 참여를 독려해야 한다. 또한 주기적인 정보보호 활동의 성과평가를 통해 정보보호가 비즈니스에 긍정적인 가치를 제공하고 있음을 보증해야 한다. 혁신이란 급격한 변화이지만, 상기와 같은 고려사항들은 단계적으로 적용되어야 하며, 변화관리 차원에서 접근해야 실효성 있는 정보보호 혁신을 이룰 수 있을 것이다.

참 고 문 헌

[1] 미래창조과학부, “2015년도 과학기술· ICT 분야 연구개발사업 종합시행계획,” 2014.

[2] Gartner, http://www.gartner.com/newsroom/id/2828722

[3] CSO Online, http://www.csoonline.com/article/2941097/security-awareness/is-the-information-security-industry-having-a-midlife-crisis.html

[4] Gartner, "Prevention is Futile in 2020: Protect Information via Pervasive Monitoring and Collective Intelligence," May 2013.

[5] Schumpeter J. A., "The Theory of Economic Development," Harvard University Press, 1934.

[6] Rothwell R., Zegveld W. “Reindustrialization and Technology,” Longman, 1985.

[7] Kelly P., Kranzberg M.,"Technological Innovation: A critical Review of Current Knowledge," San Francisco Press, 1978.

[8] Arcot Desai Narasimhalu, “Innovation Cube: Triggers, Drivers and Enablers for Successful Innovations,” ISPIM Innovation Conference, Jun 2005.

[9] O’Reilly Radar Team, "Planning for Big Data," O’Reilly Media, Inc., Mar. 2012.

〈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 : 정보보호 거버넌스, 정보보호 관리, 디지털 비즈니스

김 보 경 (Bokyung Kim)

2014년 2월 : 경희대학교 생물학과 졸업
2015년 3월~현재 : 중앙대학교 산업융합보안학과 석사과정
관심분야 : 정보보호 거버넌스, 정보보호 관리, 헬스케어 산업 보안

박 수 형 (Su Hyung Park)

2012년 8월 : Royal Holloway University of London, BSc in Management
2015년 3월~현재 : 중앙대학교 산업융합보안학과 석사과정
관심분야 : 정보보호 거버넌스, 정보보호 관리, 정보보호 컨설팅

김 건 우 (Kunwoo Kim)
정회원

2008년 8월 : 중앙대학교 정보시스템학과 졸업
2010년 2월 : 중앙대학교 정보시스템학과 석사
2015년 3월~현재 : 중앙대학교 융합보안학과 박사과정
관심분야 : 정보보호 거버넌스, 정보보호 관리, 디지털 포렌식