금융 분야의 클라우드 및 망분리 규제 개선 방안에 대한 의견

Opinion

금융IT의 현안을 **관련 분야 전문가의 시각**을 통해 소개합니다.

글. 김성래(멘로시큐리티 코리아 지사장)

| 규제로 발목 잡힌 혁신, 되살아날까?

지난 5월 1일 금융위원회는 '클라우드 및 망분리 규제 개선사항'이 금융현장에 원활히 안착할 수 있도록 '금융 분야 클라우드 가이드라인'을 개정한다고 밝혔다. 이에 따라 새로운 금융 보안 시대가 열릴지 귀추가 주목되고 있다. 금융위원회는 가이드라인 등의 내용을 담은 '전자금융감독규정' 개정안을 변경예고했는데, 클라우드 및 망분리 규제 개선방안은 클라우드의 경우 사후보고 전환 등 이용절차를 간소화하고, 망분리 규제는 개발·테스트 분야부터 단계적으로 완화하는 것이 골자다.

그동안 금융권의 클라우드 사용은 어땠을까? 주로 메일이나 메신저와 같은 내부 업무와 고객 상담, 마케팅과 같은 고객 서비스 등 후선 업무에 주로 활용했다. 최근에는 데이터 분석, 시스템 관리, 인

터넷·모바일 뱅킹 등 핵심 업무에도 클라우드 활용을 높여나가고 있다. 금융권은 고객 맞춤형 상품 개발을 위해 클라우드 기반의 AI 기술로 빅데이터 분석을 수행하고, 리스크 분석이나 파생상품 개발 등 복잡한 계리 업무를 클라우드상의 고성능 서버를 활용해 빠르게 처리하면서 활용 폭을 넓히는 중이다.

현재 금융권은 비중요 업무뿐만 아니라 중요 업무에도 클라우드를 이용할 수 있다. 다만 업무 중요도 평가, 업무 연속성 계획, 안전성 확보 조치 방안 수립, 업무위수탁기준 보완, 클라우드서비스제공자(CSP) 안전성 평가 등을 수행한 후 정보보호위원회의 심의 및 의결을 거쳐 클라우드 이용계약을 체결하고 금융감독원에 사전 보고까지 해야 하는, 까다로운 절차를 거쳐야 한다.

망분리는 외부 침입으로부터 내부 전산 자원을 보호하고 내부망과 외부망을 분리하는 네트워크 보안 기법이다. 국내에서는 내부망과 외부망의 전산시스템, 단말기를 별도로 두는 '물리적 망분리'를 채택해 운영해 왔는데, 기업과 업무의 유형을 고려하지 않고 운영되고 있어 인터넷과 연계가 불가피한 신기술 개발의 효율성과 혁신 기술의 활용도가 떨어지고 기업에 과도한 부담이 된다는 지적이 많았다. 이에 금융위원회가 추진하는 법안으로 업계에 드리워진 안개를 걷어낼 것으로 보인다.

| 현행 금융 보안 규정의 시초

지난 2013년 3월 20일 오후 2시경 농협, 신한은행, KBS, MBC, YTN 등에서 동시 다발적으로 임직원 PC의 디스크가 파괴되고, 리부팅되는 사건이 발생했다. 외부 해커가 원격으로 조직의 중요한 시스템을 파괴하고 중요한 정보를 탈취할 수 있다는 위협이 실제로 일어난 것이다. 그간 외국의 보안 벤더들이 언급하던 APT(Advanced Persistent Threat; 지능형 지속 위협) 공격의 실체를 전 국민이 알게 된 사건이었다.

이 사건 이후로 금융위원회와 금융감독원 등 금융 보안 감독기관은 기업의 중요 시스템 보안을 위해 망분리 시스템 도입을 적극 검토했고 이를 규제화하기로 했다. 10여 년이 지난 지금 국내 거의 모든 금융기관은 망분리 시스템을 운영하고 있으며 망분리는 보안의 핵심이자 기본적인 시스템으로 인식되었다.

하지만 망분리가 구축된 지금, 국내 금융기관의 사용자 인터넷 접속 환경은 오리무중을 헤매는 것 같다. 사용자들은 더 이상 회사의 업무 PC로 외부 인터넷에 원활하게 접속할 수 없게 되었고, 외부에서 전달되는 이메일은 내부 업무용 PC에서 바로 확인하기 어려워졌다. 또한 외부와 연결이 필요한 상황에서는 인터넷 전용 PC로만 접속할 수밖에 없었다. 이는 임직원의 업무 생산성을 담보로 보안을 강화하는 결과를 초래한 것 같았다.

좀 더 구체적으로 들여다보면 현재의 망분리 환경에서 금융회사 직원들은 회사 네트워크에서 외부

인터넷으로 자료를 조사하거나 간단한 검색조차 쉽지 않다. 또한 외부에서 전달되는 이메일을 업무용 PC에서 바로 확인하고 첨부파일을 확인할 수 있는 환경이 아니라, 이를 인터넷 전용 PC에서 확인하고 업무에 필요하다고 판단되면 승인 절차를 거쳐 내부 PC에 전달하는 과정을 거쳐야 한다. 시간을 다투는 디지털 세상에서 이러한 상황은 마치 90년대 초반의 업무 환경 수준으로 돌아간 듯하고 직원들의 창의성과 생산성 향상을 심각하게 저해한다고 생각한다.

| 시대의 흐름과 규제 개선의 요구가 만난 개선방안

지난 4월 15일 금융위원회는 '금융 분야 클라우드 및 망분리 규제 개선방안'이라는 보도자료를 공지했다. 그간 과도한 망분리 규제로 신기술 도입의 어려움(업무 생산성 확보의 어려움), 금융 분야의 디지털 전환을 안정적으로 뒷받침하기 위한 개선 방안이라고 설명하고 있다.

오늘날의 기업 활동은 IT 기술을 활용한 생산성 향상, 비용 절감, 매출 추구가 이뤄져야 한다. 이는 금융 업무의 디지털 전환으로 추진되고 있으며 여기에는 클라우드, 빅데이터, 인공지능과 같은 신기술 도입이 전제되어야 한다. 하지만, 현행 망분리 규제는 이러한 새로운 신기술 도입에 있어 네트워크의 분리로 인한 제한 요소가 되고 있기 때문에 시대의 흐름과 규제 개선의 요구사항에 따른 당연한 결과라고 본다.

클라우드 및 망분리 규제 개선방안 기본 방향

1 디지털 신기술이 금융 분야에 확대 적용되도록 클라우드 및 망분리 규제에 대해 전면 재검토
2 금융전산사고의 가능성에 대비해 단계적 제도개선 추진

항목	Before	After
클라우드 규제 개선방안	불명확한 업무 중요도 평가 기준	→ 업무 중요도 평가를 위한 구체적 기준 및 절차 마련
	중복 · 유사한 CSP 평가 항목	→ 중복 · 유사한 평가 항목 정비(141개에서 54개로 축소)
	비중요 업무도 모든 이용규제 준수 필요	→ 중요 · 비중요 업무 간 클라우드 이용 절차 차등화
	금융회사 등이 각각 CSP 평가 수행	→ 금융보안원 대표평가제 도입
	SaaS의 경우 CSP평가에 애로	→ Saas에 적합한 별도 평가 기준 마련
	클라우드 이용시 제출 서류 간 중복	→ '업무위탁 운영기준 보완사항' 등 제출 간소화
	금융당국 사전보고	→ 금융당국 사후보고
망분리 규제 개선방안	획일적 · 일률적 · 물리적 망분리 규제	→ 개발 · 테스트 분야 망분리 예외 → 비전자금융업무 및 SaaS에 대한 망분리 예외 추진 (규제샌드박스) → (중장기) 단계적 망분리 완화 추진

자료 : 금융위원회

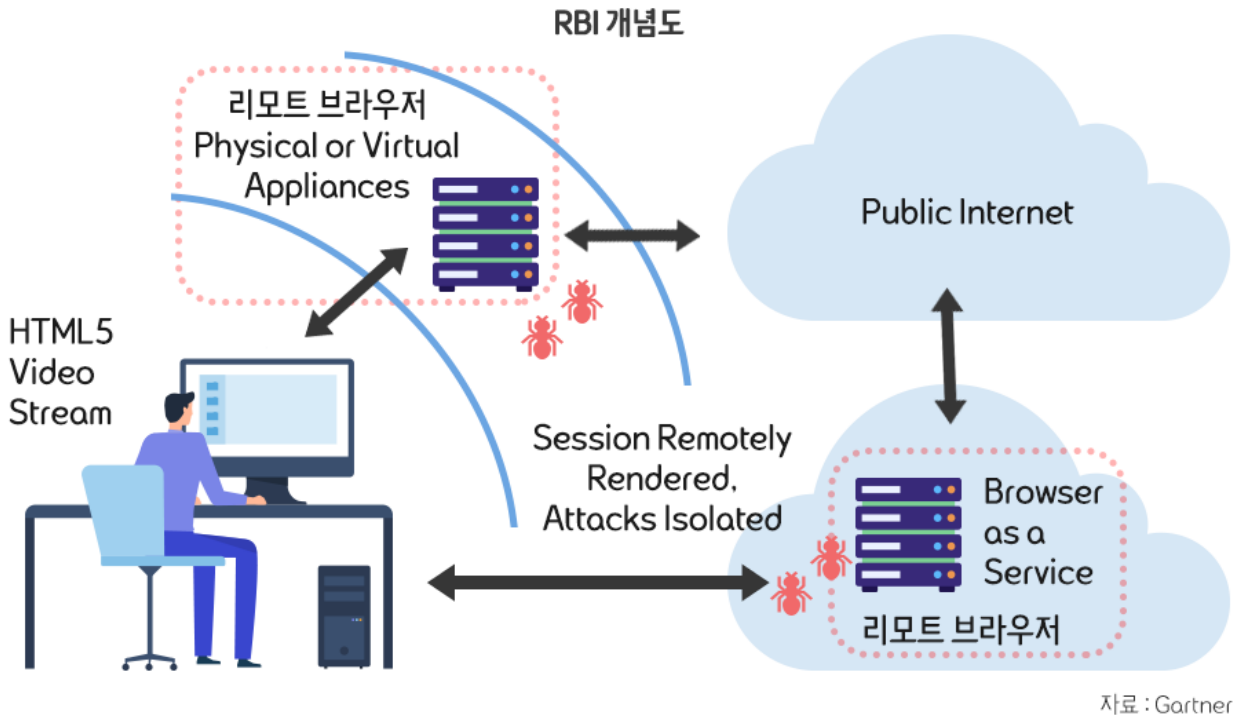
| 제로트러스트 중심의 보안 환경이 중요

금융위원회에서 추진하는 클라우드 및 망분리 규제 개선 방안에 있어서 클라우드 부분에 대해 먼저 언급하면 다음과 같다. 보안 측면에서 클라우드 규제 개선 방안은 망분리 규제 개선 방안과 관련해 개발·테스트 업무 및 비중요 업무의 망분리 예외가 추진된다면 그 동안 망분리 환경에서 담보)되어 왔던 보안성을 망분리에 준하는 보안 수준으로 추가해야 하는 상황이라고 전망한다.

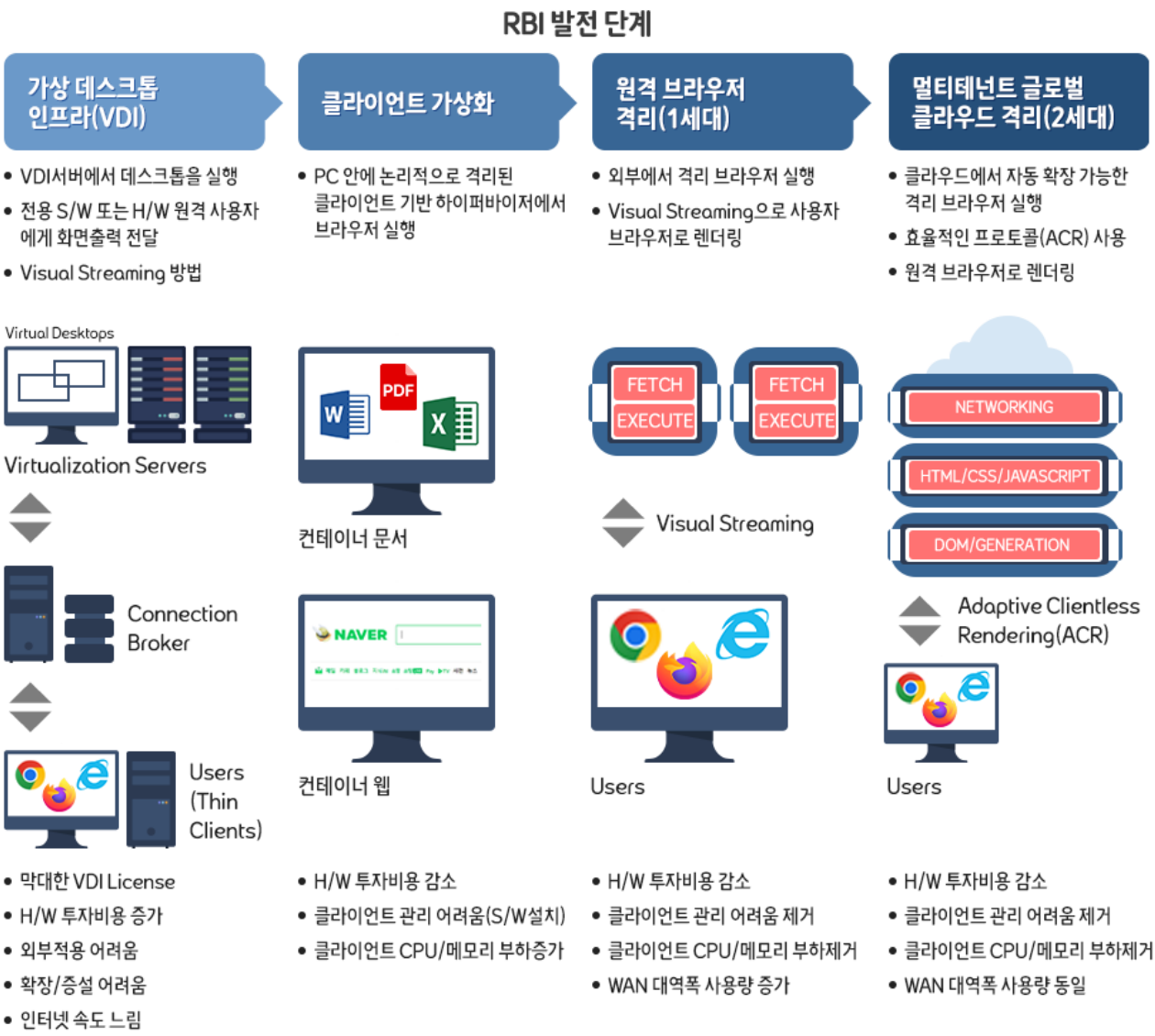
이런 측면에서 지난 '2022 RSA 컨퍼런스'에서 논의된 제로트러스트(Zero Trust) 개념의 보안이 망분리 규제 개선에 따른 개선 방안으로 적용되어야 한다. 제로트러스트는 어떠한 것도 믿지 않고 지속적으로 보안 수준을 체크해야 한다는 의미로 ZTI(Zero Trust Internet: 제로트러스트 인터넷), ZTNA(Zero Trust Network Access: 제로트러스트 네트워크 액세스)등으로 보안 솔루션이 다양하게 출시되고 있으며 글로벌 리딩 보안 기업에서는 제로트러스트 개념이 모든 보안 솔루션의 중심 개념이 되고 있다.

그럼 ZTI와 ZTNA는 무엇일까? 먼저 ZTI는 인터넷 사용시 외부에서 서비스되는 웹 콘텐츠를 어떤 것도 믿을 수 없기 때문에 RBI(Remote Browser Isolation: 리모트 웹 브라우저 격리) 기술을 통해

언제나 안전한 인터넷 환경을 구현하는 것이 핵심이다. 그동안 인터넷 망분리가 내부의 중요한 시스템과 데이터를 보호하기 위해 제로트러스트 개념을 구현한 기술이었다면 RBI는 내부의 사용자 디바이스(PC)를 보호하기 위한 제로트러스트 솔루션이라고 할 수 있다. 개발 및 테스트 시스템과 이메일 시스템이 망분리가 필수 적용될 시스템이 아니라면 이를 사용하는 유저의 해킹 위협을 제거하기 위해 ZTI 개념을 구현한 RBI 기술을 활용해 볼 만하다. RBI는 가트너(Gartner)가 최초로 언급한 개념으로 기본적인 개념은 아래와 같다.



즉, 사용자가 인터넷을 통해 외부 시스템에 접근할 때 사용자 디바이스의 브라우저가 아닌 별도의 격리된 공간에 리모트(Remote) 브라우저에서 사용자 디바이스 대신 외부 웹 콘텐츠를 가져와 실행하고 사용자 브라우저에서는 실행 가능한 어떠한 콘텐츠도 들어오지 않도록 하는 개념이다. 이 기술은 어제 오늘의 기술이 아니며 아래와 같이 발전되어 왔다.



RBI 기술 적용을 통해 망분리 예외가 가능한 개발 및 테스트 업무 시스템과 이메일, 메신저 등의 비중요 업무 시스템 사용자들이 외부의 인터넷에 연결될 때 해커에 의한 지능형 타겟 위협과 서비스의 취약점으로 인한 제로데이 위협 등으로부터 사용자의 디바이스 감염을 안전하게 지켜낼 수 있다.

이 기술은 미국 국방부(DoD)에서 이미 적용하고 있으며 2022년부터는 미국의 모든 정부기관에서 추진하고 있는 제로트러스트 보안 정책의 가장 핵심이 되는 기술이다. 미 국방부는 이 기술을 적용해, 허용/차단 기반의 비효율적 보안탐지체계를 보완하고 사이버 보안 위협의 90% 이상을 차지하는 웹 브라우저를 통한 보안 위협을 원천적으로 제거하는 성과를 거뒀다고 발표했다.

또한, 기존의 다층 구조의 보안 솔루션 장비를 운영하면서 드는 비용의 절감과 불필요한 Alert(위협 경고)를 획기적으로 줄여 보안 관제의 효율성을 증가시켰다고 평가하고 있다. 현재도 이 기술의 도입 확장은 진행 중이며 2022년 미 정부기관의 보안의 화두가 제로트러스트인 만큼 향후 도입이 활성화될 것으로 기대하고 있다.

| SaaS 기반으로 설계된 ZTNA

그 다음은 ZTNA이다. 제로트러스트 네트워크 액세스의 개념은 기존의 VPN이 수행하던 외부에서 내부 시스템과 애플리케이션으로의 접근을 보다 강화된 제로트러스트 개념을 적용한 것으로 사용자와 업무 시스템 간의 접근을 보다 세부적으로 통제하고 외부의 사용자 계정이 유출될 것을 감안하여 원격접속 보안 모델을 적용하는 것이다.

이미 글로벌 보안 벤더뿐만 아니라 국내 보안 벤더에서도 다양한 ZTNA 개념의 원격접속 보안 솔루션을 출시하고 있으며, 전통적인 VPN 솔루션의 단점을 보완해 나가고 있다.

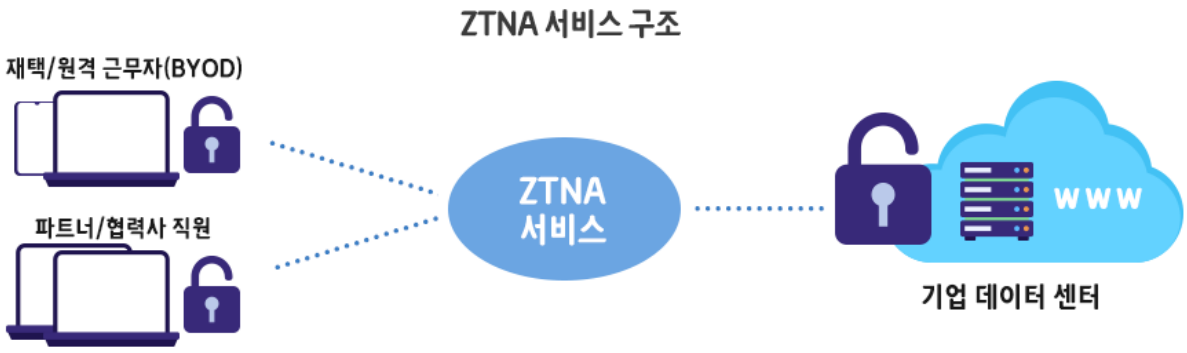
전통적인 VPN 솔루션의 단점은 VPN 서버가 DMZ 구간에서 서비스되고 있고, VPN 솔루션의 개발이 대부분 오픈소스를 기반으로 개발된 솔루션인 만큼 취약점 또한 꾸준히 발견되고 있으며 해커들은 이를 활용하여 VPN 서버 자체를 해킹하는 방법으로 손쉽게 해킹의 통로가 되어 왔다. 국내에서도 원자력연구원, KAI 등에서 VPN을 통한 해킹으로 중요정보 탈취 피해를 입었다고 보도된 바 있다.

그리고, 전통적인 VPN 솔루션은 장비 기반의 온프레미스(On-Premise) 솔루션이며 이를 운영, 유지하기 위한 SW 업그레이드, 패치(Patch) 등의 지속적인 서버 관리와 사용자 디바이스에 설치되어야 하는 에이전트 관리가 필수적이다. 이번 코로나19 팬데믹으로 재택근무가 증가해 VPN 서버의 증설 또한 요구되어 왔고 이는 업무의 생산성과 직결되는 문제로 보안팀과 네트워크팀의 큰 과제가 되었다.

이와 같은 문제점을 해결하기 위해 나온 ZTNA 솔루션은 전통적인 장비 기반의 솔루션이 아니라 SaaS 기반의 솔루션으로 설계되었고 특정한 애플리케이션을 특정한 유저에게만 접속을 허용하도록 하는 특성을 가지고 있다.

기존의 VPN이 가상사설망을 통해 한번 접속한 사용자는 내부 네트워크에 모든 접근 가능한 시스템들에 접근할 수 있었던 반면, ZTNA는 네트워크가 아닌 애플리케이션 단의 접속만을 허용함으로써 Lateral Movement(래트럴 무브먼트)*를 통한 내부 피해 확산의 가능성을 획기적으로 줄일 수 있다. 여기서 래트럴 무브먼트란 감염 확산 공격, 즉 주요 시스템에 도착하기 위해 주변 시스템을 공격해 감염을 확대하는 것을 말하며, 이렇게 주요 시스템을 장악한 다음 공격자는 시기에 맞춰 사이버 공격을 감행한다.

또한, 별도의 에이전트를 사용자 디바이스에 설치, 관리할 필요가 없고 클라우드 기반의 SaaS의 장점인 가용성과 확장성이 담보되기 때문에 버스트(Burst) 트래픽이 발생하더라도 장비를 늘리거나 SW 업그레이드 작업 없이 바로 서비스를 이용할 수 있다.



또한, 전통적인 VPN 서비스의 성능 부족으로 인해 내부 업무 시스템을 DMG망에 오픈해서 발생하는 보안의 취약점을 해결할 수 있다. ZTNA를 도입하면 기업 내부의 애플리케이션을 DMG망에서 내부망으로 이동시키고 허용된 사용자들만 허용된 애플리케이션에 접속하도록 함으로써 획기적인 원격 보안접속 환경을 구축할 수 있다.

| 꾸준한 노력으로 보안 위협 환경에 대응해 나가야

사이버 보안 환경에서는 어제보단 오늘이 오늘보단 내일이 보안사고가 일어날 확률이 높아진다. 과거와 비교해 보면 랜섬웨어 공격, 피싱사이트, 맬웨어 종류와 변형 등이 지속적으로 증가하고 있으며 보안 사고의 유형과 빈도가 꾸준히 증가하고 있는 추세이다. 이는 사이버 해킹 기술이 발달이 엄청나게 빠르게 진행되고 있고 보안 기술의 발달과 적용은 이를 따라잡지 못하고 있다는 것이다. 사이버 위협의 빈도와 수준은 증가하고 있고 보안사고의 가능성은 항상 증가하고 있는 것이다.

국내에서도 시대적 요구와 맞물려 망분리 규제가 완화되고 보안 사고의 책임은 규제 당국보다는 이제 기업에게 점점 더 비중이 가중되고 있다. 이제 금융기관은 보안의 책임을 규제 당국에 의존만 할 것이 아니라, 새로운 혁신적인 보안기술을 연구하고 적용하여 점점 더 증가하고 있는 사이버 보안 위협 환경에 대응해 나가야 할 것이다.