Deloitte.

금융기관의 사이버보안 현황

“만병통치약” 접근법은 없다

July 2018

원문 Link

CISO들의 사이버보안 업그레이드 노력

딜로이트는 51개 금융기관의 최고 정보보안 책임자(CISO)들을 대상으로 설문조사를 수행해 보안조직이 어떻게 조직되고 관리되는지, CISO의 보고 대상은 누구인지, 보안에 대한 이사회의 관심 수준, 리스크 관리 기능의 외주 수준, 사이버 보안 강화를 위한 투자 우선순위 등을 질문하고, NIST(National Institute of Standards Technology) 프레임워크의 4 단계 성숙도를 기준으로 자사의 사이버보안 수준을 평가하도록 요청했다. 그 결과, 기업 규모, 성숙도 수준, 지배구조에 따라 분명한 차이가 존재함을 발견했다.

그림 1. 사이버보안 성숙도

출처: FS-ISAC/Deloitte 사이버 리스크 CISO 설문조사에 기술된 NIST 프레임워크

사이버보안 특성은 성숙도 수준에 따라 다른 경우가 많다

성숙도 수준에 따라 리스크 관리 접근법과 실무를 차별화하는 요인에는 무엇이 있는가? 여기 몇 가지 소견을 제시한다.

책임은 최상부에서 시작된다. 거의 모든 이사회와 경영위원회 임원들이 기업의 전반적인 사이버보안 전략에 관심이 많았지만, 적응 가능 수준 기업의 이사회는 사이버보안 예산의 상세 사항, 구체적인 운영 역할과 책임, 계획의 전반적 진전도 등에 관심을 기울였다. 그보다 2단계 아래인 견문 보유 수준 기업의 이사회는 현재의 위협, 계획의 진전도, 보안 시험 결과를 검토하는데 관심이 덜했다.

공유된 책임이 차이를 만든다. 대기업 응답자들 중 2/3가 중앙 집중화된 접근법을 사용하고 있었다. 하지만, 적응 가능 수준 기업의 응답자들은 혼성 접근법-중앙 집중화된 부서가 있으나, 각각의 사업부/혹은 지역별로 전략과 실행 역량을 보유하고 다른 사업부들과 협조하는-을 보다 선호했다.

복수의 방어선을 유지. 견문 보유 수준 기업 중 거의 절반 가량의 응답자가 사이버리스크의 방어를 위한 어떤 보험에도 가입하지 않았다고 답했다. 대조적으로, 적응 가능 수준의 기업의 2/3가 거의 모든 예상 가능한 시나리오를 보호해 주는 적절한 사이버보험을 구매했다고 답했다. 나머지 1/3은 예상되는 위험 노출 중 적어도 절반을 보호해주는 보험에 가입했다.

외부의 지원을 추구. 성숙도가 낮은 기업은 사이버보안 기능 또는 인력을 외부에서 더 많이 조달했다. 하지만 가장 빈번하게 아웃소싱의 도움을 받는 영역은 사이버공격의 위협 하에서 기업의 보안, 경계, 회복력을 평가하는 "레드 팀(red team)" 활동이었다.

사이버보안에 있어 규모가 중요한 경향이 있다

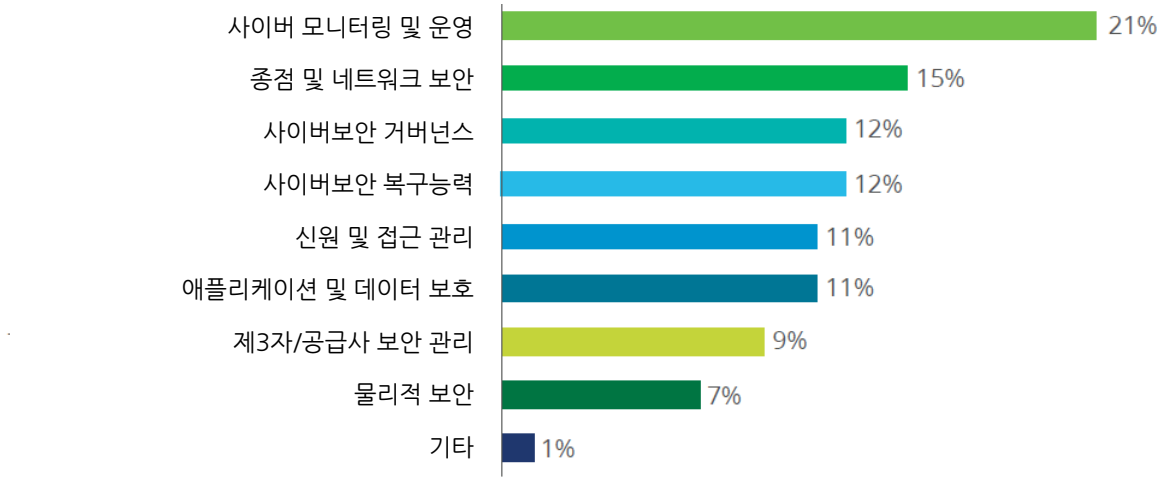
설문조사는 대형 금융기관이 어떻게 사이버보안 운영을 다루는가에 있어 몇 가지 차별점을 보여주었다.

금융기관들이 충분한 자원을 할당하고 있지 않을 수 있다. 사이버보안이 응답자들의 전체 IT 예산에서 차지하는 비율은 5%에서 20% 사이였고, 평균은 12%였다. 대형 금융기관 중 절반의 사이버보안 관리 비용이 연 2천만 달러 가량이었는데, 이것이 의미하는 바는 매출의 1% 이하 정도만을 이 영역에 쓴다는 사실이다. 잠재적인 운영 교란, 평판 손상, 조사 및 고객 관계 비용, 복구 비용 등을 고려할 때, 이는 충분하지 않은 규모일 수 있다.

지배구조의 유형이 차이를 만든다. 상장기업인 금융기관의 경우 개인소유 기업보다 더 많이 지출하는 경향을 보였다. 대형 상장 금융기관 중, 약 1/3이 4백만-2천만 달러의 예산을 보유했고, 1억 달러 이상을 보유하는 기업의 비율은 그보다 좀 더 높았다. 이는 개인 소유 대형 금융기관과 대조적인데, 이들 중 거의 대부분의 기업이 4백만-2천만 달러 사이의 예산 구간에 속했다. 이는 상장기업에서 대형 보안 침해가 발생할 경우, 주주와 애널리스트들을 뒤흔들 뿐 아니라 주가에 악영향을 미치게 되는 잠재적인 승수효과를 반영하는 것 일 수 있다.

부가적인 것보다 필수 업무에 집중. 응답자들은 사이버보안 예산의 2/3 이상을 운영 활동에 썼고, 변환적 추진계획에는 1/3 미만만을 사용했다. 사이버 모니터링과 운영이 예산 및 직원 할당에서 가장 큰 부분을 차지했다. 규모 별로 보면, 대기업은 사이버리스크 관리 예산의 1/3을 변환적 추진활동에 할당했지만, 중소기업은 예산의 ¼만을 그러한 계획에 할당했다. 설문 결과가 시사하는 바는 기업 전반적으로 혁신에 지출하는 수준에 발맞추기 위해 사이버보안 운영 관련 지출도 중심축의 이동이 필요하다는 점이다.

그림 2. 사이버리스크 관리 영역에 대한 예산/직원 할당



출처: FS-ISAC/Deloitte 사이버 리스크 CISO 설문조사, Deloitte Center for Financial Services analysis.

CISO의 보고 체계는 차이가 많음. 우리의 설문조사에 따르면, 기업 규모는 금융기관의 사이버보안 보고 체계에 영향을 미치는 요인이다. 중소기업 응답자 중 절반 이상의 CISO가 CEO에 직접 보고해, 수평적인 조직 구조를 반영했다. 대기업 응답자는 CISO가 CIO, COO 혹은 CRO에 보고하는 경우가 많았다. 중견기업 응답자의 절반은 CISO가 CRO에게 보고한다고 답했다.

혁신이 최우선 순위이다. 응답자들은 투자에 있어 가장 중요한 사이버보안 역량을 중심으로 분명한 우선순위가 존재함을 보여주었다. 모바일, 클라우드, 데이터/애널리틱스가 2년 안에 기업에 도입할 최상위 3가지 우선순위로 꼽혔는데, 이들 새로운 추진계획에 사이버 방어 능력을 내재화하는 일이 보안 시사점을 가진 가장 중요한 사업 문제에서 최우선 사안으로 선정됐다.

새로운 투자에 있어서, 설문 응답자들이 꼽은 CISO의 혁신 및 신기술 최우선 관심사로는, 클라우드, 데이터 및 애널리틱스, 소셜 미디어가 대기업들이 관심을 가지는 기술 항목의 최우선 사안으로 꼽혔다.

금융기관들은 여기서 어디로 가는가?

이번 설문 대상 규모가 작긴 하지만, 그럼에도 불구하고 기업들이 사이버보안 역량과 성숙도의 개선을 지속할 때 고려 가능한 방법을 제시해 준다. 많은 사례가, 산업 전반에 걸쳐 사이버리스크 관리 수준이 매우 광범위하다는 사실을 다시 한번 강조해준다. 리스크와 혁신 사이의 균형을 개선하기 위해, 금융기관들은 다음 활동을 고려해야 한다.

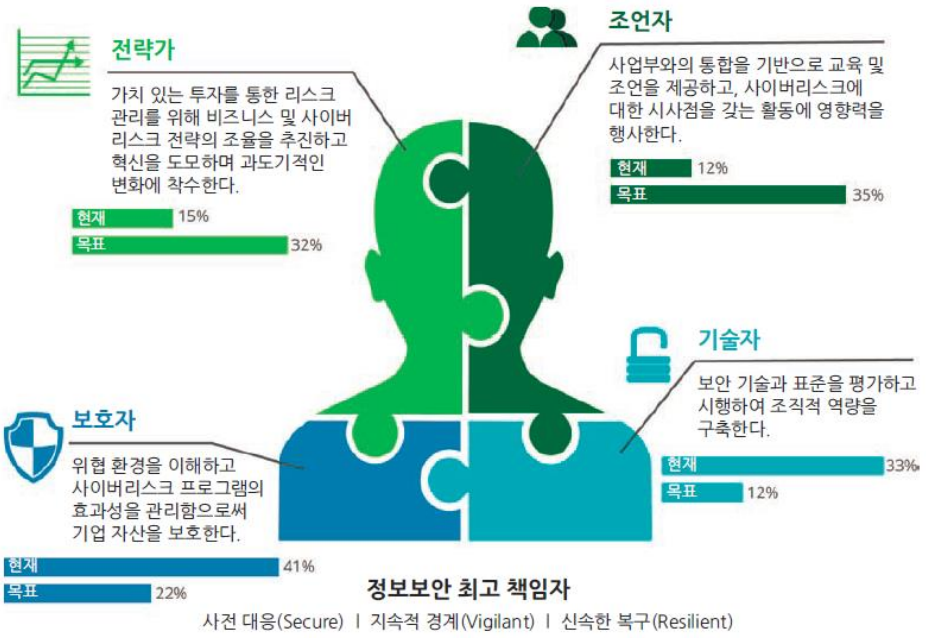
적극적으로 이사회와 관계. 이사회 임원들에게 관리진이 중요한 위험 노출을 어떻게 다루고 있는지에 대한 상세 정보를 제공하라. 그들의 관심이 강화되면 최고 경영진이 접근법을 완벽히 하고 관리 지표를 개선하는데 보다 집중하게 될 뿐만 아니라, 그러한 고위층의 철저한 검토가 조직 전체에 걸쳐 공명을 일으킨다.

전체 조직을 사이버보안에 참여시킴. 매우 적은 수의 전임 직원들만이 사이버보안에 전념하는 상황에서, 조직의 모든 이들은 침입을 감지하고, 위험 신호를 보고하며, 사고 발생 자체를 막고 만약 사고가 발생할 경우 피해를 제한시키는데 도움을 주는 좋은 보안 습관을 유지하는 데 있어 자신들의 중요한 역할과 책임을 이해하고 받아들여야 한다.

복수의 방어선을 제공. 기업은 사이버보안 실무 및 담당자를 사업부 및 지역 사무소에 내재화시켜 중앙의 사이버리스크 관리 팀을 지원함을 목표로 해야 한다. 사이버리스크의 관리가 모두의 일이 되어야 하기 때문에, 인식과 책임이 조직에 스며들도록 확실히 하고, 책임을 공유하라.

CISO의 책임 배합을 변경하라. 업무를 효과적으로 수행하기 위해, CISO는 CIO를 넘어 보고하고 정기적으로 IT 부서 외부와 교류해야 한다. 대부분의 CISO는 이미 많은 책임을 지지만, 불행히도 많은 이들이 기술자(technologist)와 보호자(guardian)와 같은 전통적인 역할에만 집중한다. 하지만 역할이 보다 복잡해짐에 따라, CISO들은 경영진과 이사회를 더 잘 지원할 수 있도록 업무 시간의 2/3를 전략가(strategist)와 조언자(advisor) 역할에 쓰려 노력해야 한다.

그림 3. CISO의 네 가지 역할



출처: "새로운 CISO: 전략적 보안조직을 이끌기", 딜로이트 리뷰 19호, 2016년 7월

사이버보안 한 단계 끌어올리기

사이버보안이 계속해서 금융기관의 핵심 기능이 될 것으로 예상됨에 따라, 위협이 범위, 기법, 정교함에 있어 계속 진화하는 상황에서 역량의 개선은 지속적인 도전과제가 될 가능성이 크다. 앞으로의 설문조사에서는 성숙도와 기업 규모에 따른 사이버보안 예산 및 인원수에 대한 벤치마크 자료를 만들기 위해 다음과 같은 보다 많은 정보를 탐색할 것이다.

- NIST 영역별 성숙도 점수
- IT 예산에서 사이버보안이 차지하는 비율, 또한 FTE(Full Time Equivalent*) 당 사이버보안 예산
- 전체 IT 인력 및 정보 보안 인력에서 사이버보안 FTE가 차지하는 비율

하지만, 벤치마크가 사이버리스크를 다루기 위한 준비 수준의 평가에 있어 금융기관을 도울 수 있긴 하지만, 사전 대응하고, 지속적으로 경계하며, 신속히 복구하는 능력을 유지하려면 자신의 경험 이상을 살펴봐야 하고 동일한 위협에 직면한 더 넓은 공동체와 함께 계속 협업해야 한다.

사이버보안에 대한 협업은 금융산업 전반에 걸쳐 그리고 개별 하부산업 영역 내에서도 중요하다. 최소한, 금융기관은 동료들의 경험에서 배우기 위해 사이버 전쟁에 대한 이야기를 면밀히 추적해야 한다. 이는 금융기관이 최신의 사이버 위협으로부터 인력과 시스템을 보호하기 위해 쓸데없이 시간을 낭비(reinvent the wheel)해야 하는 상황을 피하도록 도울 수 있다.

* FTE는 임의의 업무에 투입된 노동력을 전일종사 노동자 수로 측정하는 방법이다. FTE가 1이면 A라는 임무에 투입된 전일종사 노동자가 1명임을 의미한다. 만약 반일종사 노동자 2인이 A 임무에 투입되었다면 A 임무에 투입된 FTE는 2가 아니라 1이 된다.

Deloitte.