프로세스가 모든 것을 말한다

: 한국씨티은행 전산기획부 정보보호팀

지난 2008년말 방통위와 KISA가 주관한 정보보호대상에는 국내에서 정보보호를 잘 한다는 기업들이 대거 참가해 그 어느 해보다 심사에 어려움이 있었던 것으로 알려져 있다. 기업들의 치열한 각축전 속에 치러진 금융부문 정보보호대상은 결국 씨티은행에게 돌아갔고, 이로 인해 씨티은행의 정보보호 체계와 활동에 대해 많은 정보보호 관계자들이 다시금 관심을 갖게 됐다. 그들은 무엇을 어떻게 하고 있을까.

| 정보보호뉴스 취재팀 |

지난 2004년 한미은행을 합병하며, 국내에서 본격적인 금융 업무를 시작한 한국씨티은행(이하 씨티은행)의 정보보호 활동은 많은 사람들의 관심의 대상이다. 글로벌 기업들 중에서도 기업 정보보호 수준에서 매번 모범사례로 손꼽히기 때문이다. 이들의 보안 프로세스, 내부인력 교육, 아웃소싱 관리 등 씨티은행 정보보호팀의 보안활동은 취재팀의 호기심을 유발하기에 충분했다.

: 합병, 그 치열했던 과정

씨티은행 정보보호팀의 공식 명칭은 한국씨티은행 전산기획부 정보보호팀. 그런데 이들 정보보호팀은 내부적으로 보다 세분화된 체계를 갖추고 있다. "씨티은행 정보보호팀은 정보보안을 총괄하는 BISO(Business Information Security Office)와 기술적인 정보보안을 담당하는 TISO(Technology Information Security Office), 그리고 전산운영보안을 담당하는 TI-BISO(Technology Infrastructure-BISO)로 구분돼 관리적, 기술적 영역이 세분화돼 있어요. 또 모든 부서 및 지점에 정보보안을 담당하는 직원이 지정되어 있어 정보보안 정책이 전체 조직에 직접 적용될 수 있도록 조직화되어 있다는 점이 특징이죠." 씨티은행 전산기획부 정보보호팀 박영길 부장은 이 같은 조직체계는 글로벌 기업으로서 씨티은행의 모든 직원이 항상 동일한 정보보안 정책으로 정보보호 활동에 동참하도록 만드는 중요한 열쇠라고 설명한다. 이처럼 씨티은행 정보보호팀이 전문화되어 있기 때문일까, 한미은행과 씨티은행의 합병과정은 상당한 기간이 소요되기도 했다.

"2004년 합병 선언 이후 2007년 마무리된 시점까지 약 3년이라는 시간이 소요됐어요. 결코 짧은 시간은 아니지만, 정보보호 측면에서 많은 요소들이 고려하고 계획했던 것인 만큼 그 시간이 정말 정신없이 지나갔죠." 씨티은행 전산기획부 정보보호팀 이창영 부부장은 두 은행간 합병과정은 철저한 계획수립과 관리를 기반으로 이뤄졌다고 회상한다. 정보보호 관점에서 양사의 전산 인프라와 애플리케이션에 대한 리스크 측정, 양 금융기관의 시큐리티 갭 분석에서는 많은 공을 들이기도 했다. 그중에서도 이들에게 많은 고민을 안겨줬던 것은 바로 보안 프로세스의 정착. "한미은행과 씨티은행의 보안체계가 많이 달랐어요. 보안 프로세스는 업무 프로세스에 접목되어야 하기 때문에 기존의 기업 문화를 극복하고, 보안과 현업이 공존할 수 있도록 교육과 시스템 지원에 많은 시간을 할애했죠." 이 부부장은 보안 프로세스야말로 기업 정보보호 수준을 좌우하는 핵심이라고 강조한다.

▲ 한국씨티은행 전산기획부 정보보호팀 박영길 부장

"정보보호 수준이 강화되기 위해 보안 활동의 중심에는 각 비즈니스 부서가 있도록 하고, 보안부서는 이를 지원하고 검증하는 관계가 이뤄져야 한다고 봐요." 씨티은행 전산기획부 정보보호팀 박영길 부장은 정보보호 실천은 정보보호 부서의 역할만이 아닌 현업 부서의 몫이라고 설명한다.

: 수립, 준수, 검증의 사이클

"기업 정보보호는 보안규정 수립, 준수, 검증이라는 일련의 과정이 가장 중요하다고 생각해요. 물론 여기에 유무형의 보안교육이 뒤따라야 하죠." 이 부부장은 씨티은행의 보안은 수많은 프로세스를 준수하는 것에서 시작되고 그것을 확인하는 것으로 끝난다고 강조한다. 일례로 내부 직원들의 입에서 '일을 잘 하지 못해도 정년은 보장받지만, 보안규정을 준수하지 않으면 바로 퇴사조치'라는 말이 자연스럽게 나올 정도다. 그만큼 보안에 대한 씨티은행 직원들의 보안의식은 남다르다. "저희 직원은 회사 내 PC를 통해 씨티은행이 제공하는 인터넷 뱅킹조차 사용하지 못해요. Active X를 통한 프로그램 설치를 차단해 놓았기 때문이죠. 이런 불편함에 대해 내부 직원들도 이제는 익숙해져 당연하다고 생각하고 있어요." 그런 의미에서 이 부부장은 씨티은행의 정보보호팀은 다른 기업 보안팀과 달리 손쉽게 보안업무를 수행할 수 있다고 말한다.

이와 같은 높은 의식 수준을 보유하고 있음에도 불구하고, 다른 기업처럼 씨티은행에서도 보안사고나 규정 위반 사례가 드물게 발견되기도 한다. 하지만 다른 기업과 가장 큰 차이는 보안사고에 대한 직원들의 자발적인 신고의식이다.

"씨티은행의 강점은 정보보안 사고발생시 국내 사고대응팀 뿐만 아니라 씨티그룹 차원의 사고대응 담당자들과 시스템을 통해 정보가 공유되고, 전세계 전문가들과 함께 문제를 해결함으로써 최적의 해결방안을 모색하고 재발방지 대책을 수행할 수 있다는 점입니다. 수립된 대책은 다른 모든 씨티은행 시스템이 그렇듯, 위험 소멸시점까지 철저히 트래킹되고 보고 관리하게 됩니다." 보안팀 그리고 책임자의 역할은 사고 발생의 원인을 문책하는 것이 아니라, 동일한 일이 일어나지 않도록 보완하고 점검하는 것이라고 박 부장은 덧붙인다.

: 정보보호 실천, 각 부서의 몫으로

씨티은행이 가진 보안 프로세스는 씨티은행 내부로 그치지 않는다. 씨티은행과 협력을 맺고 있는 기업들도 그에 따른 보안수준을 갖춰야 한다. "카드 DM 발송업체나, VAN사에 대한 보안감사가 대표적이죠. 씨티은행과 함께 일하기 위해서는 그에 따른 보안수준을 지켜야 해요. 씨티그룹의 보안표준을 제시하고, 부족한 요소들에 대해서는 교정조치를 요구하고 감사를 통해 확인하는 일련의 과정이 유지되고 있죠." 내부직원은 물론, 아웃소싱 기업에게도 보안 프로세스 적용은 필수적이라고 이 부부장은 설명한다.

한국씨티은행 전산기획부 정보보호팀 이창영 부부장 ▲

"사고의 유무보다 사고발생 시 얼마나 빨리 대처하고, 동일한 사고가 발생되지 않도록 해야 합니다. 이를 위해서는 보안규정에 대한 철저한 이해를 바탕으로, 규정수립, 준수, 검증 과정을 철저히 이행하는 것이 중요하죠." 씨티은행 전산기획부 정보보호팀 이창영 부부장은 보안 프로세스를 거듭 강조한다.

"씨티그룹 전체가 처음부터 정보보호를 잘했다고 생각하지는 않아요. 하지만 다양한 경험과 해결방안을 통해 축적된 정보보호에 대한 노하우가 현재의 수준을 만들었죠. 끊임없는 관리를 통해 문제를 찾아 해결하고, 이를 업무 프로세스에 접목시키는 과정이 반복됐다고 생각하시면 됩니다." 박 부장은 이를 위해 정보보호 부서가 중심이 되는 정보보호보다는 기업 내 모든 부서가 정보보호를 주도하도록 유도해야 한다고 강조한다. 특히 씨티은행에서는 정보보호팀이 아닌 현업부서가 전사적으로 구축된 정보위험관리 시스템에 대한 총괄적인 책임을 지도록 하고 있어 자연스럽게 정보보호 체계가 굳건해 질 수 있다고 한다.

보안투자, 경제불황 속에서도 지속된다

최근 정보보호 관계자들은 전 세계적인 경제불황의 여파로 기업이 정보보호에 대한 투자감소와 그에 따른 보안수준 하락을 우려하고 있다. 이에 대한 씨티은행 정보보호팀의 생각은 어떠할까. "경제불황이 불닥치면 정보보호 부서 이외에도 씨티은행의 모든 부서 예산이 줄어드는 것은 사실입니다. 하지만 경제 상황이 씨티은행의 보안수준에 변화를 주는 일은 없습니다"라고 박 부장은 단언한다. 지금까지 인식제고와 프로세스에 의해 보안강화가 이뤄졌고, 향후에도 이와 같은 이들만의 문화는 지속될 것이기 때문이다.

씨티은행 정보보호팀과의 인터뷰는 약 2시간이 넘게 지속됐지만, 정보보호대상 수상기업인 씨티은행의 정보보호 활동체계와 방안을 꼼꼼히 들여다보기에는 이 2시간도 부족한 시간임에는 틀림없다. 그러나 정보보호를 화두로 나눴던 2시간동안의 이야기를 지면 관계상 모두 소개하지 못한 점은 더욱 아쉬움으로 남는다. 하지만 이들의 보안 이야기는 다시 한번 소개할 기회가 올 것이라고 믿는다. 씨티은행의 즐거운 보안활동이 계속되는 만큼. S