Ken DeJarnette

개인정보보호, 위험관리를 넘어 필수요인으로

개인정보보호에 대한 관심과 사회적 이슈는 국내뿐만이 아니라, 전 세계적인 공동의 관심사로 떠오른 지 오래다. 국제기구가 프라이버시 보호 법안을 제정해 각국 정부에 권고하는 한편, 개인정보보호, 프라이버시 보호와 비즈니스의 연관관계를 분석하는 시도가 늘어나고 있다. 국제적인 컨설팅 그룹 딜로이트에서 보안 프라이버시와 데이터 보호 분야를 맡고 있는 Ken DeJarnette에게 비즈니스와 개인정보 및 프라이버시 보호의 연관성에 대해 다양한 조언을 요청했다.

정보보호뉴스 취재팀

Ken DeJarnette
(Deloitte and Touche LLP)

Q 국내에서 개인정보보호와 프라이버시에 대한 중요성이 강조되고 있다. 기업의 관점에서 더욱 부각되는 개인정보보호, 혹은 프라이버시 보호의 중요성에 대해 말해 달라.

A IT 기술 분야는 그동안 많은 발전을 이뤄왔고, 그 기술 대부분은 기업이 전세계 시장을 대상으로 신속하고 효율적으로 그리고 저비용으로 사업을 수행하게 하는데 일조했다. 그런데 이와 같은 기술의 발전은 개인정보의 사용과 보호와 관련된 새로운 과제들을 요구하기 시작했다. 대표적인 예로 RFID, 전자상거래, 원격 컴퓨터 사용, 데이터 저장 장치, 웹 기술, 그리고 콘텐츠 모니터링 등이 있다. 이들 기술이 보다 활성화되기 위해서는 개인정보와 같은 데이터들이 오용되지 않고, 보호되고 있다는 사실이 입증되어야 한다. 하지만 개인정보보호의 중요성에도 불구하고 기업들은 ERP와 CRM 시스템의 단일화 단계를 통해 정보를 중앙 집중화된 형태로 만들어감에 따라, 막대한 오용이나 개인적 정보(혹은 지적 재산)의 손실과 같은 부정적인 결과가 늘어나고 있는 실정이다. 이런 상황에서 개인정보보호는 기업이 비즈니스를 영위해 나가기 위한 필수적인 조건이 되고 있다.

Q 국내에서 개인정보와 프라이버시가 비슷한 의미로 통용되고 있다. IT 환경에서의 프라이버시 보호는 무엇을 의미한다고 생각하나.

A 실제로 프라이버시는 많은 다른 의미를 가지고 있고, 대부분 그 정의는 우리가 어떤 문화권에 속하느냐에 따라 달라지게 된다. 하지만 일반적으로 프라이버시는 개인정보의 주체자 즉, 데이터를 제공하는 개인-그 개인이 소비자이건, 직원이건, 판매자이건, 사업 파트너이건 간에-의 권리가 어떤 영향과 규제를 받게 되는지와 관련된다. 또한 프라이버시의 정의에는 정보의 사용, 보호, 책임소재에 대한 문제가 포함된다. 때문에 기업은 개인정보를 활용할 때 각 단계별로 적용되는 법률을 준수하면서 마케팅에 활용하는 방법을 이해하는 것이 필요하다. 특히 다국적 기업은 고객이 어떤 국가와 법률의 영역에 속하는지에 따라 다르게 정보활용 전략을 수립해야 한다.

물론 프라이버시 보호에는 정보보호 측면이 포함돼 있다. 예를 들어 신용카드 등을 잃어버리거나 도난당할 경우에 대비해 주요 정보들을 암호화 또는 마스킹 처리하는 것은 매우 중요한 것이다. 일반적으로 프라이버시와 관련된 정보보호 정책은 데이터 기

밀성 및 가용성, 그리고 부인방지, 무결성의 입증, 데이터 접근제어 등을 포함하고 있다.

개인정보보호, 비용절감 측면에서도 유효하다

Q 정보보호에 대한 투자가 이뤄지지 않는 원인으로 투자효과가 불분명하다는 점을 꼽고 있다. 정보보호 분야에서도 투자효과에 대한 수치화 혹은 계량화가 가능하다고 생각하나. 가능하다면 어떤 방식으로 이뤄질 수 있다고 생각하나.

A 가능하리라고 본다. 정보보호와 프라이버시의 투자효과는 많은 방법으로 보여질 수 있다. 경우에 따라 계량화하기 어려울 수도 있겠기만 데이터 침해는 최근 몇 년간 전세계 많은 신문에서 헤드라인을 장식해왔고, 이런 사건으로 인해 지출된 비용은 막대하다. Deloitte & Touche LLP와 The Ponemon Institute LLC가 지난 2007년 "Enterprise@Risk : 2007 Privacy & Data Protection Survey"라는 제목의 설문을 시행한 바 있는데, 설문 응답자 중 63% 이상은 고객들에게 알려야 할 심각한 침해를 경험했다고 언급한 바 있다. 이 같은 사실은 데이터 침해와 그에 따른 금전적 손실 그리고 기업 명성의 실추 등에서 손실이 막대함을 의미한다.

Q 발생할 수 있는 손실을 막는다는 주장보다는 '개인정보보호를 하면 비용을 절감할 수 있다'는 식의 주장이 더욱 설득력을 얻을 것 같은데.

A 투자효과는 비용방지와 비용절감의 측면으로 나눠볼 수 있다. 효과적인 프라이버시 및 정보보호 프로그램이 존재한다면 기업은 규제 위반에 대한 잠재적 벌금을 포함해 지속적으로 변화하는 개인정보보호와 관련된 규제들을 회피하게 만들어 준다. 반면, 비용절감 차원에서도 분명한 효과가 있다. 효과적인 프라이버시 및 보호 프로그램의 핵심은 정보의 라이프사이클(어디서, 어떻게, 누구에게 공유되고 파괴되는지의 일련의 과정)을 이해하는 데 있기 때문에 과잉된 데이터 프로세스로부터 비용 절감을 밝혀내는 효과를 가져다 줄 것이다. 수많은 데이터 속에서 유용한 데이터만 추출하는 것은 IT 환경에서 매우 중요한 문제가 되기 때문이다.

Q 컨설팅 업무를 진행하다 보면 기업 경영진에게 프라이버시 보호의 필요성을 제기할 것이다. 경험 상 경영진의 개인정보나 프라이버시 보호 의지는 어느 수준에 와 있다고 생각하나.

A 그 대답은 어떻게 회사가 이슈를 구상하는지에 따라 다르다고 판단된다. 만약 기업 안에서 회사의 주요 자산을 어떤 방향으로 활용해야겠다는 식의 토론이 있었다면 그 임원진은 분명 매우 열성적일 것이다. 기업 경영진의 입장에서 보면 브랜드, 명성, 사용, 경쟁관계, 그리고 손실방지에 많은 신경을 쓰게 마련이다. 데이터가 기업에 있어 매우 가치 있는 자산이고, 데이터를 사용하는 것은 프라이버시와 개인정보보호 이슈로 이어지게 되는데 이런 연관관계는 관리단계에서부터 데이터 보호에 대한 관심으로 도출되기 마련이다.

데이터 흐름과 인프라 구조 파악이 최우선

Q 개인정보나 프라이버시 침해는 외부적 요인보다는 내부적 요인 가령, 기업의 내 구성원들의 실수에서 비롯되는 경우가 많다. 이와 같은 문제를 줄일 수 있는 효과적인 방안이 있다면.

A 최근 인가되지 않은 접근의 비율이 오르고 있는 상황에서 그 초점은 기업의 외부로부터 오는 위협 대응에 맞춰지게 마련이다. 그러나 외부로부터의 위협 못지 않게 다양한 내부적 위협, 가령, 직원들의 의도된 혹은 의도되지 않은 실수, 허술하게 설비된 시스템과 제어장치, 혹은 유효기간이 지난 비즈니스 프로세스가 기업에게 위험을 안겨주게 된다. 이를 예방

하기 위해서는 기업이 가진 데이터의 위치와 종류를 확인하고, 데이터를 보호하기 위한 적절한 제어장치의 효과를 평가하는 것, 그리고 비즈니스 프로세스 또는 지역적 범위가 확대될 경우 통제 장치를 재점검하는 것이 필요하다.

Q 기업 내 구성원들에 대한 교육이 최근 증가하고 있는 실정이다. 어떤 방향으로 교육이 이뤄져야 한다고 생각하나.

A 물론 프라이버시와 개인정보보호에 대한 교육은 어떤 프라이버시 보호 체계에서도 필수적인 요소이다. 직원들은 프라이버시의 중요성에 대해, 그리고 기업이 보유한 데이터의 활용에 있어 해야 할 것과 하지 말아야 할 것들에 대한 충분한 훈련을 받아야 한다. 사실은 직원이 데이터를 취급하기 이전에 훈련을 하는 것이 현명하지만, 이런 과정을 거치는 경우는 많지 않다. 직원들은 프라이버시 의무사항들을 주기적으로 되새길 수 있는 교육을 받아 프라이버시에 대한 인식이 최우선이 되도록 해야 하며, 회사의 프라이버시 정책이나 기준, 시행령 등 데이터 취급 활동에 영향을 줄 수 있는 변화에 민감하게 반응할 준비가 되어있어야 한다.

Q 미국의 경우, 법률을 통해 세부적인 규제사항을 제정하기 보다는 기업의 자율적인 규제강화에 중점을 두고 있는 것으로 알고 있다. 미국 내에서 논의되고 있는 프라이버시 보호 정책의 방향에 대해 간략하게 언급해 달라.

A 미국은 가장 먼저, 프라이버시에 대한 분야별 접근을 시도했는데 이것은 반대로 말하면 미국 내에는 국가 차원의 단일한 프라이버시 관련 법이 존재하지 않는다는 것을 의미한다. 프라이버시 보호 요건들은 금융 서비스, 보건의료, 청소년 보호와 신원도용방지, 강매 방지 등과 같은 일부의 사업들을 위해 발전돼 왔다. 향후에도 프라이버시와 관련된 규제는 이런 분야들로 집중될 가능성이 높다고 생각되며, 국가에서는 규제의 대부분을 법률화하는 역할을 하게 될 것이다.

Q 미국 내에서 기업에 의한 개인정보 유출 혹은 프라이버시 침해로 인해 큰 손실이 발생한 사례가 있다면 간략하게 소개해 달라.

A 불행하게도 오늘날의 뉴스 헤드라인은 악의를 가진 내부자의 활동으로 인해 개인정보 침해를 당한 기업들의 소식으로 가득 차 있다. 이런 많은 사건들의 결과는 결국 수백만 달러의 손해로 이어지게 된다. 이런 상황에서 중요한 것은 어떤 손실이 발생했는가보다 이와 같은 상황에 어떻게 대처했는지가 더 중요하다고 본다. 고비를 넘긴 기업들은 분명 뛰어난 사고대응계획을 가지고 있었으며, 수립된 대응계획은 데이터 침해에 대처하는데 중요한 참고사례가 됐다. 이 사고대응계획에는 기업이 해당 고객들은 물론, 다른 주요 이해관계자들과 어떻게 의사소통을 할지도 포함된다. 한 가지 덧붙이자면 데이터의 영향을 받는 시스템과 네트워크를 매핑하는 것은 매우 중요한데, 이것은 침해로 연결된 실패 시점을 차후에 보완하고 데이터가 무엇과 충돌하고 충돌하지 않는지 여부에 대해 결정을 내리는 데에 도움을 준다.

Q 글로벌 기업들은 다른 지역 혹은 국가들로의 진출을 시도할 때마다 각기 다른 정보보호정책에 부딪히게 되는데, 서로 다른 정책들에 대해 효율적이면서도 빠르게 대처할 수 있는 방안은 무엇이라고 생각하나.

A 우선 정책을 세우는 것에 급급해하지 않아야 한다. 또 다양한 요건들을 이성적인 시각으로 바라보는 능력을 키워야 한다. 그리고 정책을 세우기 전, 위험관점에서 데이터의 라이프사이클과 그것을 지원하는 인프라 구조를 이해할 필요가 있다. 물론 일반적인 정책이 적용되지 않는 지역도 있을 것이다. 하지만 신용과 브랜드 관점에서 기업의 환경을 반영하는 일련의 일반적인 요건들에 기초한 정책을 수립하게 된다면 각각의 정책변화나 위험으로부터 효율적으로 대처할 확률이 높아질 것이다. S