CPO들이여, 프라이버시 리더십을 갖자

Brent Carey

Manager, Privacy & Feedback / Executive Service / Department of Justice, Victoria, Australia

국내에서 점차 CPO(Chief Privacy Officer)의 역할과 업무영역에 대한 관심이 증가하고 있는 가운데, 이번 호에서는 호주 빅토리아 주 법무부의 프라이버시 피드백 및 프로젝트 매니저로 활동하고 있는 Brent Carey를 만났다. 지난 3월 KISA가 주최하고 한국CPO포럼이 주관한 'Privacy Global Edge 2009'에서 기조연설을 맡기도 했던 Carey는 프라이버시 보호 분야에서 활발한 활동을 펼치고 있다. 한국 문화에 관심이 많고, 김치와 갈비를 특히 좋아한다는 그를 정보보호뉴스에서 만나봤다.

| 정보보호뉴스 취재팀 |

지난 3월 Privacy Global Edge 2009을 통해 개인정보보호 리더십에 대해 발표해 준 바 있는데, "개인정보보호 리더십"이라는 용어가 한국 정서에서 다소 낯설다는 생각이 든다. 여기에서 의미하는 리더십은 구체적으로 어떤 의미를 가지고 있나?

A 최고 프라이버시 담당자(Chief Privacy Officer)가 된다는 것은 기관 내에서 한 자리를 맡는다는 것 이상의 의미가 있다. 기관의 정보보호 규정 준수 프로그램을 맡고 있는 프라이버시 전문가들은 그들의 기관이 프라이버시에 있어서 모범 사례가 되도록 이끌어갈 필요가 있다. 프라이버시 전문가들은 또한 프라이버시에 대한 올바른 인식의 의미를 만들어내고, 이에 따라 직원들을 교육시키는 것을 주도해야 하며, 일련의 행동들과 관련된 프라이버시 위험들에 대해서도 목소리를 높여야 한다. 직원들의 프라이버시 의식을 견고하게 만드는 일은 쉬운 일은 아니다. 하지만 자신들의 속한 기관 혹은 기업이 사람들의 개인 정보를 다루는 데에 있어서 높은 신망을 받고 있다는 것 자체가 그들에게는 큰 보람이 될 것이다. 그런 만큼, 프라이버시 전문가들은 프라이버시에 있어서 자신들이 가지고 있는 비전을 어디에서든 이야기할 수 있어야 할 것이다. 여기서 중요한 것은 프라이버시 전문가로서 전달하는 주요 메시지를 받아들이고 적극적으로 지지하도록 최선을 다하는 것이다. 리더십은 바로 그런 의미다.

기업이 고객의 정보를 보호하기 위해 개인정보보호 조직을 구성하는 움직임이 늘어나고 있다. 개인정보보호 조직이 구성될 때 가장 중요한 요소는 무엇이라고 생각하는가.

A 개인정보보호 부서는 회사가 통제할 수 있는 개인정보의 카테고리를 이해하고 있어야 한다. 정보를 제공하는 주체들은 기업이 수집한 각 개인의 정보가 어떻게 이용 및 관리되고 보호되는지에 대해 관심을 가지며, 이는 기업에 대한 신뢰도를 완성하는 중요한 요소가 된다. 프라이버시 전문가는 그 개인정보에 어떤 일이 일어나고 있는지에 대해 관리하면서 개인정보를 보호하기 위한 프라이버시 툴들을 사용해야 할 것이다. 이런 '툴'에는 표준 프라이버시 정책들, 웹사이트의 프라이버시 사항 고지, 표준 계약 조건들, 프로젝트에서의 프라이버시 위험을 관리·예방하기 위한 개인정보보호 영향평가(Privacy Impact Assessment) 등이 포함되어야 한다. 수준 높은 프라이버시 교육 프로그램 및 인식 제고 프로그램 또한 개인정보보호 관련 요구사항들을 직원들이 준수할 수 있도록 하는 좋은 도구가 될 것이라고 본다.

국내에서는 비용적인 이유에서, 그리고 인력 관리적인 측면에서 CERT 혹은 IT 보안 부서가 개인정보보호 업무를 함께 맡는 경우가 많다. 이럴 경우 발생할 수 있는 문제점이 있다면.

A — 이에 대해서는 시스코 최고 보안담당자를 맡고 있는 John Stewart가 한 말을 인용하고 싶다. 그는 보안팀에서 회사의 보안에 대해 전적인 책임을 지고 있고 회사의 나머지 99%는 보안 문제에 책임이 없다는 일반적인 생각에 대해 잘못됐다고 지적했다. 나는 개인정보보호 문제에 있어서 IT 보안부서만이 홀로 책임을 지도록 하는 것에 대해서도 그의 말을 동일하게 적용할 수 있다고 생각한다. 물론 기업 환경 상 어쩔 수 없는 부분도 분명 있을 것이다. 다만 보다 바람직한 방향을 제시하자면, 기업은 최고 프라이버시 담당관을 임명하고, 전문가들(법, 커뮤니케이션, 기술 분야 등)로 이뤄진 프라이버시 팀을 구성해 전 직원들이 개인정보보호 컴플라이언스에 대한 책임이 있다는 것을 지속적으로 일깨워주는 것이 필요하다. 올바른 개인정보보호 컴플라이언스는 프라이버시 전문가들과 IT 보안 실무진 및 책임자들 간의 협력관계를 바탕으로 만들어지는 것이라고 믿는다. 각자의 입장에서 개인정보보호 수준을 높일 수 있는 방안과 위험성에 대해 투명하게 이야기를 나눠야 한다. 여기서 한가지 조언을 하자면, 각 분야의 전문가들은 전문용어의 사용으로 의미가 명확하게 전달되지 못하게 하는 일은 지양되어야 한다는 것이다.

IT 보안전문가와 개인정보보호 전문가, 구별되어야

개인정보를 수집하는 기업의 입장에서 고객의 정보를 보호하기 위해 사내 직원들의 프라이버시를 침해하는 사례도 발생할 수 있다(예를 들어, 사내 직원들의 내부정보 유출을 예방하기 위해 이메일 모니터링을 하는 경우 등). 이런 복잡한 이슈를 풀 수 있는 가장 좋은 방법은 무엇이 되겠는가?

A — 사내 프라이버시는 심각한 이슈 중 하나이다. 직원에 대한 모든 모니터링 활동은 합법적인 것이어야 하며, 모든 직원들에게 이에 대해 투명하게 알려야 한다. 직원들에게 고객의 개인정보를 책임감 있게 다룰 것을 요구한다면, 직원들에 대해서도 그에 상응하는 조치가 있어야 한다는 점은 분명하다. 직원들의 프라이버시 보호 기준과 고객 프라이버시 보호 기준이 따로 존재한다면, 직원들은 고객 데이터를 보호해야 한다는 책임의식을 덜 느끼게 될 것이다. 이런 의미에서 기업에서 모니터링 솔루션을 사용하고자 한다면 공개된, 투명한 방법으로 해야 할 것이다. 이는 곧 어떠한 경우에 그들의 행동들이 모니터링의 대상이 되는지, 그리고 그 목적은 무엇인지에 대해 분명하게 전달해야 하는 것을 의미한다. 인터넷 사용 정책, 이메일 정책, 활용되는 문서 형식 등에 모니터링에 대한 고지를 포함시키는 것도 좋은 방법이다.

CISA, CISSP와 같은 정보보호 자격증은 전 세계적으로 공인되는 분위기다. 그러나 개인정보보호의 경우에는 국가마다 다른 법률 체계와 사회적 정서의 차이가 있는데, 정보보호처럼 세계적으로 공인되는 자격증이 생겨날 수 있다고 생각하는가?

A — 매년 점점 더 많은 국가들에서 프라이버시 법이 법제화되고 있다. 오늘날의 글로벌 비즈니스 환경에서 세계적인 프라이버시 요구사항들에 대한 이해와 관리에 대한 관심은 점점 늘어나고 있다. 프라이버시 관련 법은 각각의 나라에서 비슷한 양상을 보이고 있는 반면, 개인정보보호 분야에 있어서는 많은 차이가 있다. 예를 들어, 어떤 나라에서는 개인정보의 특정한(예를 들어 마케팅 목적의) 사용을 허락하는 반면, 다른 나라에서는 엄격히 금지될 수 있다. 이에 대한 결정 및 판단은 각 국가의 프라이버시 법이나 문화가 범세계적인 기초를 형성할 만큼 서로 공통점을 갖추고 있는지에 따라 좌우될 것이다. 개인정보보호 분야에 있어서 세계적인 자격증이 등장한다면, 거기에는 반드시 '개인적인 정보', '동의', '수집', '사용', '공개' 그리고 '데이터 보안' 등의 개념이 포함되어야 한다고 생각한다.

IT 사회가 발전하면서 '개인정보'와 '프라이버시'라는 말이 혼용되어 사용되고 있다. 이 두 용어를 어떻게 구분할 수 있겠는가?

A — 내가 받아들이기에, '개인정보'가 '프라이버시'보다 더 좁은 개념이다. 개인정보보호는 신원을 파악할 수 있는, 혹은 읽어낼 수 있는 구별된 개인에 대한 정보의 기록을 보호하는 것으로, '개인정보'는 기록이 따로 지정된 보관인에 의해 보호된다는 것을 나타낸다. 개인정보를 보호하기 위해서는 그 정보의 보관인이 적절한 정보를, 적절한 이유에 의해, 적절한 때에, 적절한 방법으로 수집해야 한다. 이에 반해 '프라이버시'는 단순한 정보에서 벗어나 더욱 넓은 개념이 된다고 본다. 유전적 검사, 약물 검사, 그리고 나체 검사 등의 공격적인 절차들에 대항해 사람들이 신체적인 자신을 보호하는 것과 관련된 신체적 프라이버시, 또는 개인의 자유와 연관된 개념들 모두가 프라이버시 영역에 포함될 수 있다.

호주나 뉴질랜드에서 개인정보보호의 인식을 높이기 위해 법무부 혹은 다른 기관에서 계획하고 있는 행사가 있다면 무엇이고, 어떤 방식으로 진행되고 있나.

A — 최고 프라이버시 담당자들은 다른 이들의 경험으로부터 많은 것을 배운다. 한국CPO포럼과 같이 프라이버시 전문 기관들에 의해 진행되는 세미나 및 행사들은 중요한 네트워킹 기회이자 전체적인 인식 수준 및 교육에 관련된 정보를 얻을 수 있는 완벽한 장소가 된다. 내가 일하는 기관을 비롯해 다양한 기관들이 프라이버시 보호와 관련된 행사를 개최하고 있는데, 가령, 봄맞이 대청소처럼 프라이버시 컴플라이언스에 대한 집중 점검 기간을 시행한다든지,

프라이버시 만화를 배포하든지, 호주의 프라이버시 관련 뉴스와 빅토리아 법무부의 프라이버시팀의 활동을 뉴스로 생중계하는 등의 방법이 동원되고 있다.

프라이버시 보호, 법적 규제와 기업의 책임감 조화되어야 한다

RFID, CCTV 등 새로운 IT 기술 발전에 따른 신규 프라이버시 침해요인들이 늘어나고, 또 이로 인해 발생할 수 있는 문제를 예방하기 위해 법률과 규제를 제정해 예방하려고 한다. 그런데 새로운 기술이 등장하면 그때마다 개인정보보호와 프라이버시 보호를 위해 동일한 일을 반복해야 한다고 생각하나. IT 기술발전에 따라 보다 유연하고 포괄적으로 접근할 수 있는 방법은 없다고 생각하나.

A — 인류는 원래 발명, 그리고 그러한 발명과 혁신이 우리에게 무엇을 가져다 줄지에 대해 매력을 느껴온 존재이지 않은가. 그런 의미에서 본다면 우리는 새로운 기술이 가져올 다양한 혜택과 그에 따른 부작용, 즉 기술발전이 가진 긍정과 부정적인 면에 대해 끝없는 토론을 하게 될 것이다. 개인적인 시각으로 기술발전에 대한 가장 유연한 접근은 법적 규제와 기업의 책임감이 조화되어야 한다는 것이다. 여기에서 강조하고 싶은 것으로 법은 가장 빠른 대응도, 좋은 대응도, 유일한 대응도 아니라는 점이다. 법의 힘보다 프라이버시를 발전시키는 기술적인 접근, 혹은 기술을 만들고 팔고, 사용하는 사람들의 행동에 영향을 미치는 교육적인 접근이 먼저 이뤄져야 한다. 또 기술을 개발하는 사람들은 고안 단계에서부터 그들이 그 안에 프라이버시 개념을 어떻게 정립할 것인가에 대해 생각해 봐야 한다. 프라이버시에 대한 사회적인 인식은 캠페인과 같은 사회적 운동으로부터 등장한다고 믿고 있다.

마지막으로, CPO의 역할에 대한 당신의 의견을 듣고 싶다. 기관이나 기업에서 CPO는 어떤 사람이어야 하겠는가?

A — CPO는 최근에 만들어진 직책이다. 그러나 프라이버시와 관련된 관리직은 점점 널리 퍼지고 있다. CPO는 어떻게 보면 영업 사원이고, 어떻게 보면 선교사이며, 또 어떻게 보면 대외 관계 전문가이어야 한다. 영업 사원적인 측면은 프라이버시가 기업의 총수에게 법적인 부담감일 뿐 아니라 팔리는 물건이 되어야 하기 때문이다. 선교사적인 측면은 CPO가 사업적인 문맥에 프라이버시 이슈들을 끌어들여야 하고, 이 이슈들에 대해 평가하며, 회사의 발전에 기여할 수 있는 가장 좋은 방법을 결정하기 위해 '신대륙'으로 항해를 떠날 준비가 되어야 하기 때문이다. 또한 CPO는 대외 관계 전문가여야 하는데, 이는 데이터 보안에 대한 우려의 목소리가 들릴 때마다 프라이버시 문제들을 해결하기 위해 그가 하고 있는 일에 대한 원활한 의사소통이 이루어지지 않으면 결론적으로 프라이버시 보호에 실패하게 되기 때문이다. S