지난 2008년은 대규모 해킹·개인정보 유출 등 보안 사고로 얼룩진 한 해였다. 중국발 해킹으로 인해 국내 대표 오픈마켓 회원 1,000만명의 개인정보가 유출됐고, 포털 사이트의 고객 상담정보가 해커에 의해 탈취됐으며, 정유회사 고객정보 1,100여만건이 내부 직원에 의해 유출되는 등 다양한 형태의 보안 사고가 발생했던 한해였다.

지난 십여년에 걸쳐 진행된 정보화 혁명으로 인해, 거의 모든 정보들이 디지털화되고 인터넷을 통한 유통이 일반화되면서 정보보호 이슈는 날이 갈수록 심화되고 있는 실정이다. 인터넷이 우리 사회에 가져온 순기능은 형언할 수 없을 만큼 크지만 개인정보 침해를 비롯한 역기능 또한 심각한 수준에 이르고 있다. 향후 유비쿼터스 시대 도래 등과 더불어 다양한 개인 맞춤형 IT 서비스가 더욱 확산된다면 개인정보 보호와 프라이버시에 대한 이슈는 지금보다 더 첨예하게 대두될 것으로 예상된다. 더 많은 정보사회의 편익을 누리기 위해 개인정보의 적절한 수집과 활용은 계속될 것이기 때문이다. 그런 의미에서 개인정보보호는 고도 정보화 사회를 위한 기본 전제조건이자, 결정적인 신뢰요소다. 그리고 지금은 우리 사회의 개인정보보호 수준재고를 위해 모두의 지혜가 필요한 시점이다.

글 **김인호** | SK텔레콤 IT보안팀 매니저 _ ino1170@sktelecom.com

선한 사마리아인과 정보보호

비즈니스 환경 변화와 정보보안 Risk 증대

여러 형태의 보안 위협은 기업·기관의 경영 활동에 있어 주요한 리스크(Risk) 중 하나가 되고 있다. 기업·기관이 해킹·고객정보 유출 등 보안 사고를 당하게 되면 피해 기업·기관은 수사기관의 조사 및 부정적 언론 보도로 인한 이미지 하락은 물론, 사안의 중요성에 따라 정부의 징계 및 형사처벌, 고객 집단소송 등 막대한 유무형의 피해에 직면하게 되는 것이 일반적인 현상이다. 또한 장기적으로는 고객이탈 및 매출 감소, 기업 브랜드 가치 훼손 등 보안 Risk가 악순환 형태로 지속·반복되며 피해가 확대되는 특징을 보이고 있다.

정보보안 사고 발생 시 기업/기관의 Risk 확대 과정

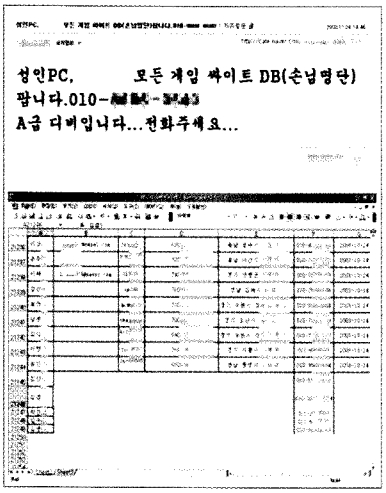
최근 해킹·고객정보 유출 등 정보보안사고 발생 시,
① 수사기관의 조사 → ② 언론노출 → ③ 정부의 징계 및 형사처벌(과태료/과징금) → ④ 고객 집단소송으로 인한 민사상의 책임 직면 → ⑤ 고객이탈 및 매출 감소 → ⑥ 기업 브랜드가치 훼손 등의 보안 Risk가 악순환 형태로 지속, 반복되며 피해가 확대되는 특징을 보이고 있음

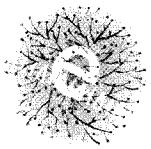
개인정보 유출 사고가 근절되기 힘든 원인으로는 여러 가지가 있겠지만, 몇 년 전부터 개인정보가 화폐와 거의 동일한 가치를 가지며 국내외를 막론하고 공공연히 거래가 되는 환경이 조성돼 악의적인 사람들이 개인정보 유출시도를 멈추지 않는 강력한 동기 요인으로 작용하고 있다.

Rank for Sale	Rank Requested	Goods and Services	Percentage for Sale	Percentage Requested	Range of Prices
1	1	Bank Account Credentials	18%	14%	$10-$1,000
2	2	Credit Cards with CVV2 numbers	16%	13%	$0.50-$12
3	5	Credit cards	13%	8%	$0.10-$25
4	6	Email addresses	6%	7%	$0.30/MB-$40/MB
5	14	Email passwords	6%	2%	$4--$30
6	3	Full identities	5%	9%	$0.90-$25
7	4	Cash-out services	5%	8%	8%-50% of total value
8	12	Proxies	4%	3%	$0.30-$20
9	8	Scams	3%	6%	$2.50-$100/week for hosting: $5-$20 for design
10	7	Mailers	3%	6%	$1-$25

▲ 암시장(underground market)에서 거래되는 개인정보의 가치

출처 : Symantec Global Internet Security Threat Report Trends for July~December 07, Volume XII, Published April 2008





◀ 인터넷상의 개인정보 매매 화면

출처 : http://www.kukinews.com/news2/article/view.asp?page=1&gCode=soc&arcid=0921107501&cp=nv

한편 이용자들은 개인정보 노출을 극도로 꺼리며 정보유출 사고 발생 시 집단소송을 제기하는 등 매우 적극적으로 대응하고 있어 보안 사고를 당한 피해 기업·기관은 이중, 삼중의 곤란을 겪게 된다. 2009년 1월 기준으로, 개인정보 유출 사고 관련해서 50여건이 넘는 집단소송이 현재 진행 중이며, 총 20여만명이 참여하여 소송금액만도 2,100억원을 넘어서고 있다.

개인정보보호를 위한 법제도 개선

정부는 개인정보 유출 피해 방지와 이용자 불안감 해소를 위해 정통망법을 개정(2008년 6월 공포, 2008년 12월 시행)하고 개인정보 취급 사업자의 책임을 대폭 강화한 바 있다. 이러한 환경 변화와 법제도 개선으로 사회 전반의 개인정보보호 인식이 한층 개선되었고 사업자는 물론, 이용자들의 자율적인 정보보안 노력도 상당히 증대되고 있다.

많은 기업·기관에서 개인정보 유출 사고를 비롯한 보안 사고는 기업·기관의 존폐를 위협할 수 있는 결코 간과할 수 없는 사안이라는 인식이 확산되면서 이제는 CEO가 관심을 가져야 할 사항(CEO Agenda)으로 대두되고 있다. 개인정보보호가 고객중심경영의 중요요소이며, 조직 비전과 미션 달성과 무관하지 않은 중요한 활동이라는 공감대가 형성되면서 체계적인 개인정보보호 활동 강화가 진행 중이다.

반면, 이용자들의 보안의식과 실천도 한층 개선되고 있다. 정보보호가 중요하다고 느끼는 이용자가 지속적으로 증가하고 있으며, 개인정보 침해에 대한 관심과 우려도 꾸준히 증가하고 있는 것으로 나타났다.[1] 방송 통신 융합시대의 인터넷 최대 현안은 '개인정보보호'[2]라고 여겨질 만큼 개인정보보호는 우리 사회 전반에 걸쳐 이슈화 되면서 안전한 인터넷 이용환경에 대한 이용자의 욕구는 날로 증대되고 있는 실정이다.

이런 현실을 반영하듯, 지난 2008년부터 시행된 정보통망법 개정안에서는 정보유출 사고 발생시 경우에 따라 해당 기업·기관은 과징금 및 형사처벌을 받을 수도 있게 되는 등 처벌내용이 대폭 강화됐다.[3] 이러한 법제도의 강화는 우리 사회의 정보보호 수준 제고를 위해 분명 바람직한 것이다.

다만 보안 사고의 특수성으로 인해, 이러한 조항이 오히려 보안사고를 은폐시키고 위험과 사회적 비용을 증대시키는 부작용으로 이어지지 않을까 우려된다. 끊임없이 신규 취약점이 출현하는 보안의 특성상, 법에서 명시하는 보호조치를 모두 이행했을지라도 보안 사고가 발생할 수 있기 때문에 결국 보호조치를 성실히 이행한 선의의 기업·기관도 미이행 기업·기관과 동일하게 민·형사상의 책임에 직면하게 될 수 있다. 많은 기업·기관이 보안 사고 발생시 집단소송에 직면할 수 있기 때문에 피해 사실 공개를 꺼리고, 이로 인해 사고 발생에 따른 적절한 사후대응도 미흡하게 되는 악순환이 발생할 우려가 존재하는 것이다.[4]

개인정보보호에 대한 책임과 면책 명시 필요하다

이러한 부작용을 방지하기 위해서는 개인정보보호를 위해 선의의 주의 의무를 다한 기업·기관(즉, 기술적·관리적 보호조치를 충실히 이행하고 보안 사고 발생시 자발적 공개·통지를 실시한 기업·기관)에게는 보안 사고 발생시 해당 기업·기관의 책임을 경감 또는 면책하는 내용을 법에 명시할 필요가 있다. 이러한 면책 조항

1 2008 정보보호 실태조사(KISA, 2008.12)

2 '전문가가 진단한 방통융합시대 인터넷 이슈와 전망'(한국정보사회진흥원, 2009.1)

3 기술적 조치 미이행으로 인한 개인정보 침해(제28조)발생시 관련 매출액의 1% 이하 또는 4억원 이하의 과징금제도의 신설, 2년 이하 징역 또는 1천만원 이하 벌금으로 상향 조정(제73조 벌칙)

4 개인정보유출 사실을 자진 공개하고 후속 피해 방지를 위해 노력했던 옥션, GS칼텍스 등은 집단소송에 직면하고 있어 향후 기업은 개인정보 유출 사건 발생시 더욱 은폐를 시도할 가능성이 있어 개인정보보호 측면에서는 나쁜 선례로 작용할 수 있다. 정보 유출 사고가 발생했을 때 은폐하고 피해 방지를 위해 노력하지 않았던 기업에 비해 오히려 더 큰 피해를 보고 있는 셈이다.

은 단순하지만, 이로 인한 기대 효과는 다음에서 볼 수 있는 것처럼 매우 클 것으로 예상된다.

첫째, 무분별한 소송과 소송을 부추기는 변호사(Ambulance Chaser)로 인한 불필요한 사회적 비용이 증대되는 것을 어느 정도 방지할 수 있을 것으로 기대된다. 선의의 주의 의무를 다한 기업에 대한 책임을 경감하겠다는 의지를 명백히 함으로써, 무분별한 집단소송으로부터 선의의 기업은 일정 부분 보호하고 악의적인(개인정보를 의도적으로 오남용하고 주의의무를 성실히 수행하지 않는) 기업에 대해서는 책임을 더욱 강화할 수 있을 것이다.

둘째, 기업의 보안 투자를 촉진시킬 수 있을 것으로 기대된다. 선의의 주의 의무를 이행한 사업자에 대한 면책조항이 법에 명시되면 기업·기관으로서는 정보보안 및 개인정보보호를 위한 예산 확보·투자에 있어 명백한 당위성 확보가 가능해져 보안 강화를 위한 노력에 한층 힘이 실릴 수 있을 것이다. 불의에 의한 보안사고 발생시, 정부의 징계 또는 형사처벌의 위험을 줄일 수 있고, 이용자 집단소송을 억제하는 효과를 기대할 수 있기 때문이다.

사실 정통망법 내에는 내용은 다소 다르지만 선의의 주의 의무를 다한 사업자에 대해 책임을 경감 또는 면제하는 유사한 조항이 이미 존재하고 있다. 명예훼손 등 잘못된 정보의 삭제 요청 관련 조항(제44조, 제44조의 2)[5]과 인터넷게시판 이용 시 본인확인제도 관련 조항(제44조의 5)[6] 등이 그것이다. 따라서 개인정보보호를 위해 선의의 주의 의무를 다한 사업자에 대해 책임을 경감하는 것은 법의 정신에도 크게 위배되는 사항이 아닌 것으로 보인다.

선한 사마리아인과 정보보호

이제 우리는 좋든 싫든, 원하든 원하지 않든 보안을 위해 막대한 사회적 비용을 지출해야 하는 시대에 살고 있다. 그것은 정보화 혁명 속에서 우리가 받아들여야 할 숙명과도 같은 것이다. 국가가 군대를 유지·운영하는 것은 전쟁이라는 불의의 사태가 발생했을 때 대비하기 위함이 첫 번째 목적이지만 강건한 군대를 유지하고 있는 것 자체가 국민에게 안심을 주고 불순한 전쟁의 도발을 억제하는 효과를 거둘 수 있다. 마찬가지로, 국가든 기업이든 정보보안의 테두리 없이는 정상적인 정보화 사회의 편익을 영위할 수 없음은 물론, 이용자에게 신뢰와 안심을 제공하지 못하는 시대가 된 것이다.

이용자가 보안을 간절히 원하는 만큼 이를 뒷받침하기 위한 사회적 제도나 장치는 더욱 정교하게 설계되고 개선되어야 할 것이다. 기업·기관의 보안 담당자들이 효율적인 정보보호를 위한 활동에 매진할 수 있도록 해주고, 선한 사마리아인의 책임은 경감하고, 악의적인 사업자나 해커의 처벌은 더욱 강화해 범죄의지를 억제하기 위한 방향으로 법제도가 개선되어야 한다. 이것이 우리가 가야할 바람직한 첫 걸음이 아닐까 생각한다. S

5 명예훼손 등 잘못된 정보의 삭제 요청 관련 조항(제44조, 제44조의 2)
제44조 (정보통신망에서의 권리보호)
② 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 제1항에 따른 정보가 유통되지 아니하도록 노력하여야 한다.
제44조의2 (정보의 삭제요청 등)
② 정보통신서비스 제공자는 제1항에 따른 해당 정보의 삭제 등을 요청받으면 지체 없이 삭제·임시조치 등의 필요한 조치를 하고 즉시 신청인 및 정보게재자에게 알려야 한다.
⑥ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보에 대하여 제2항에 따른 필요한 조치를 하면 이로 인한 배상책임을 줄이거나 면제받을 수 있다.

6 인터넷 게시판 이용시 본인확인제도 관련 조항(제44조의 5)
제44조의5 (게시판 이용자의 본인 확인)
① 다음 각 호의 어느 하나에 해당하는 자가 게시판을 설치·운영하려면 그 게시판 이용자의 본인확인을 위한 방법 및 절차의 마련 등 대통령령으로 정하는 필요한 조치(이하 "본인확인조치"라 한다)를 하여야 한다.
④ 공공기관 등 및 정보통신서비스 제공자가 선량한 관리자의 주의로써 제1항에 따른 본인확인조치를 한 경우에는 이용자의 명의가 제3자에 의하여 부정사용됨에 따라 발생한 손해에 대한 배상책임을 줄이거나 면제받을 수 있다.