Deloitte.

제조업에 미치는 사이버리스크의 대응방향

- Deloitte와 MAPI의 사이버리스크 연구를 바탕으로

딜로이트 안진회계법인
Consumer & Industrial Products(C&IP) Industry
Industrial Products & Services(IP&S) Sector Leader
홍창식 전무

December 2016

제조업에 미치는 사이버리스크의 전망과 대응방향

들어가기

제조업을 영위하는 기업들은 변화하는 글로벌 시장상황에서 경쟁하기 위하여 제품혁신, 제조공정혁신 그리고 산업생태계상의 관계혁신을 치열하게 추진하고 있다.

사업을 운영하기 위한 기술은 복잡한 글로벌 네트워크의 형성, 수많은 백오피스 비즈니스 애플리케이션과 리스크가 높은 제조과정을 통제하는 다양한 산업통제시스템(ICS)과 연관되어 있고 새로운 기술개발을 통하여 끊임없이 진화하고 있다. 게다가, 제조업을 영위하는 기업은 글로벌시장에서 살아남기 위해 끊임없이 제품혁신, 제조공정혁신 그리고 산업생태계(ecosystem)와의 관계혁신을 광범위하게 추진하고 있으며 그 결과 제조업은 다음과 같은 최근 경향을 반영한 기술의 변화속도가 더 빨라지고 있다.

- ✓ 지적재산과 기하급수적으로 발전하는 기술에 대응하기 위한 대규모 투자
- ✓ Industry 4.0과 관련된 디지털 제조기회의 탐구와 산업생태계의 상호연관성 증대
- ✓ Sensor Technology, Smart Products, 사물인터넷(IOT) 등을 적용
- ✓ 고객서비스와 비즈니스효율을 추구하기 위한 애널리틱스의 급격한 도입

상기의 경향을 반영한 비즈니스와 제조기술의 급격한 변화는 제조업을 영위하는 기업들이 향후 10년간 짚고 넘어가야 할 사이버리스크의 범위와 복잡성에 심각한 영향을 미칠 것으로 전망된다. 최근 제조업, 특히 IP&S(Industrial Products & Services) Sector에서는 첨단제조업에 미치는 사이버리스크에 대한 영향에 대한 논의가 대두되었고, 최근 Deloitte와 MAPI(미국의 생산과 혁신을 위한 제조업자 연합;The Manufacturers Alliance for Productivity and Innovation, 이하 MAPI)에 의해 이루어진 엔터프라이즈 사이버리스크 연구는 제조업을 영위하는 기업이 직면하는 사이버리스크에 대하여 많은 시사점을 제공하고 있다.
이러한 사이버리스크에 대한 연구와 국내에서 사이버보안의 주무기관인 한국인터넷진흥원의 조사결과를 토대로 제조업이 직면하고 있는 사이버리스크에 대해 살펴보고자 한다.

사이버리스크의 내용과 기업의 인식

사이버리스크란 사이버상의 사고로 인하여 기업이 부담하게 될 비용이 증가하는 것으로 볼 수 있다. 사이버 공격의 빈도와 강도가 갈수록 높아지고 있다는 데 반박할 사람은 거의 없을 것이다. 많은 조직이나 기업들이 사이버 사고를 경험하고 있는데, 이 기업들은 사이버 사고가 조직에 미치는 영향을 온전히, 완벽하게 파악하고 있을까? 보안전문가인 데이비드 웰던의 조사내용을 인용하면, 일반적으로 데이터 유출과 관련하여 발생하는 직접적인 비용은 '숨겨진 비용'에 비하면 미미한 수준이라고 할 수 있으며, 사실 '숨겨진 비용'은 사이버 공격이 조직 비즈니스에 미치는 전체 영향의 90%에 이르기도 하는데, 대부분의 경우 사건이 발생하고 2년 이상이 지난 후부터 드러나기 시작한다고 한다.

최근 딜로이트 어드바이저리(Deloitte Advisory)가 '사이버 공격이 표면 아래 비즈니스에 미치는 영향을 심층 분석'한 결과, 사이버 공격의 비즈니스 영향은 아래와 같이 14가지로 분류하고 있으며, 이러한 영향은 다시 두가지 범주 인 '표면 위' 즉, 명확히 알려진 사고 비용과 '표면 아래' 즉, 숨겨지거나 잘 보이지 않는 비용으로 분류하고 있다. 또한 현재 시장은 사이버 사고의 비용을 극히 과소평가하고 있으며, 비율로는 훨씬 더 작은 표면 위의 잘 드러나는 영향에만 집중하는 경향이 있다고 보고하고 있다.

표면 위, 명확히 알려진 사이버사고 비용	표면 아래, 잘 보이지 않는 사이버사고 비용
침해 사실 고객 통보	보험료 상승
침해 후 고객 정보	차입을 위한 비용 증가
규제 기관 명령 이행 (벌금)	운영 중단
언론 대처, 위기 커뮤니케이션	고객 관계 가치 손실
법률 비용 및 소송	손실된 계약 수익 가치
사이버 보안 개선	상표명의 평가 절하
기술 조사	지적 재산(IP) 손실

딜로이트 앤드 투쉬 LLP(Deloitte & Touche LLP)의 파트너이자 딜로이트 어드바이저리 사이버 위험 서비스 부문 책임자인 에밀리 모스버그는 "경영진이 잠재적인 영향을 제대로 파악하지 못하는 이유는 비즈니스를 원상복구하는데 어떤 어려움을 겪는지에 대해 일반적으로 서로 공유하지 않기 때문"이라며 "그동안 사이버 공격의 영향에 관한 정확한 그림이 없었고 따라서 기업들은 필요한 위험 태세(risk posture)를 제대로 갖추지 못하고 있고 논의는 대부분 어떤 취약점이 존재하며 기술적인 영향은 무엇인가에 집중하고 있다. 그리고 침해 사실 통보, 침해 후 보호 메커니즘이라는 극히 좁은 범위에 집중되어 있을 뿐 폭넓은 영향은 무시되고 있는 것으로 보인다"고 덧붙였다.

위의 모든 영향 영역 중에서 가장 큰 부분은 운영 중단이다. EMT컨설팅(EMT Consulting)의 사장 겸 수석 컨설턴트이며 SIM 사이버보안 그룹 회원인 에릭 토마스는 "각 조직마다 받는 영향은 다르지만 업종별로 공통적인 핵심 영역이 있다. 예를 들어 소매에서는 신용카드 데이터가, 의료보건에서는 PIN(개인 식별 정보)이 가장 중요하고, 제조업체는 지적 재산 손실에 따른 영향이 가장 크다. 그러나 어느 조직에서든 가장 과소평가되는 영향이 바로 비즈니스 중단이다" 라고 지적하고 있으며 "시기와 기간에 따라 다르지만 비즈니스 중단은 금전적 피해, 수익 감소, 차입 비용, 고객 서비스, 브랜드 인식, 미래 기회 등에 광범위하게 영향을 미칠 수 있다"고 설명하고 있다.

발표한 '2016 아시아 태평양 국가보안 전망보고서'에 따르면 한국은 IT기반 구축 수준에 비해 보안 측면의 대응능력과 관련된 인프라 수준이 상대적으로 하위권으로서 사이버공격이라는 새로운 형태의 위기에 직면해 있음을 보여준다.

과연 기업들은 광범위한 영향을 미쳐 큰 비용을 부담하게 하는 사이버리스크가 미치는 영향을 얼마나 심각하게 인식하고 있을까? 관련 연구를 토대로 미국과 우리나라의 상황을 살펴보고자 한다.

최근 2016년 11월에 발간된 'Cyber risk in advanced manufacturing'에서 Deloitte와 MAPI는 미국 제조업을 영위하는 35개 기업의 경영진 및 산업조직과의 인터뷰를 수행하였고, 포브스 인사이트(Forbes Insights)와의 협업으로 제조업에서 확인되어야 할 사이버리스크에 대한 온라인 서베이(225곳 응답)를 실시하였다.
그 결과 미국 제조업에서 사이버리스크에 영향을 미치는 주요 사항으로는 경영진과 이사회수준의 인식(Executive and board level engagement), 사이버 보안관련 인력문제(Talent and Human capital), 지적재산(Intellectual property), 커넥티드 제품(Connected products), 산업통제시스템(ICS, Industrial control system)과 산업생태계(Industrial ecosystem)로 요약이 될 수 있는데, 아래 표에서와 같이 조사대상 기업 임원진의 거의 50%는 사이버보안에 대한 확신을 하지 못하고 있고, 특히 48%는 사이버보안관련 기업의 예산투자가 부족하다고 답변을 하고 있어 전반적으로 미국에서 제조업을 영위하는 기업의 사이버리스크에 대한 준비상황이나 인식이 부족함을 보여주고 있다.

Cyber risk programs: a framework for leading practice board reporting

<출처 : Cyber risk in advanced manufacturing, Deloitte>

국내의 현황을 살펴보면, 2016년 딜로이트 컨설팅이 발표한 '2016 아시아 태평양 국가보안 전망보고서'에 따르면 한국의 사이버리스크 점수는 1,000점 만점 중 884점을 기록하였으며 이는 아태지역 18개국 중 압도적 1위에 해당하는 수치이다. 또한 2위 호주(582점)보다 300점 이상 높으며, 아태지역 평균(201점)보다 4배 이상 높다. 이는 한국이 IT기반 구축 수준에 비해 보안 측면의 대응능력과 관련된 인프라 수준이 상대적으로 하위권으로서 사이버공격이라는 새로운 형태의 위기에 직면해 있음을 설명하고 있다.

국내의 사이버보안의 현실과 전망

한국인터넷진흥원은 분기별로 '사이버위협동향보고서'를 발간해 국내와 글로벌의 주요 사이버위협을 관찰하고 있다. 2016년 11월 4일에 발간한 2016년 3분기 사이버위협동향을 보면 개인정보유출사고, IOT를 사용한 DDOS공격, 포켓몬고의 인기에 편승한 사이버위협, EMV(Europay-Mastercard-Visa, 유로페이, 마스타카드, 비자카드가 공동으로 제정한 IC카드 관련 국제기술표준)방식의 신용카드 도입에 따른 POS침해사고, 랜섬웨어가 가장 사이버보안에 위협을 주고 있는 분야이다.

이중 개인정보유출사고의 예를 들면, 국내 I사의 경우, 해당직원 및 가족의 신상정보와 사진을 이용하고, 말투까지 흉내 낸 이메일을 통해 악성코드가 포함된 첨부파일 실행을 유도하는 정교한 APT공격으로 직원의 PC를 감염시켰으며, 그 후 빠른 시간 내에 일사천리로 모든 탈취작업을 마친 것으로 알려졌다. 미래창조과학부와 방송통신위원회의 조사결과 허술한 논리적 망분리가 지목됐으며, 공격자들은 개인정보가 담겨진 DB서버에 접속할 때만 데이터베이스관리자가 해당서버를 가상화하는 논리적 망분리를 적용하는 것을 노려 정보를 빼낸 것이 밝혀졌다. 이 사례에서 보듯이 사이버공격자들의 공격행태는 훨씬 더 광범위하고 정교하게 진행되고 있는 것을 알 수 있다.

한국인터넷진흥원은 사이버위협동향 등을 토대로 국내 주요 6개 보안업체(안랩, 빛스캔, 이스트소프트, 하우리, 잉카인터넷, NSHC)와 '사이버위협 인텔리전스 네트워크'를 운영하고 있으며, 국외 주요 6개 보안업체 (파이어아이, 포티넷, 인텔시큐리티, 마이크로소프트, 팔로알토 네트워크, 시만텍)와 '글로벌 사이버 위협 인텔리전스 네트워크'를 운영함으로써 공조체계 강화의 일환으로 인텔리전스 구성 회원社가 공동으로 보안위협을 선정하여 발표하고 있는데, 2016년 12월 5일에 2016년 한 해 동안 발생한 보안위협을 분석하고 내년 사이버공격 위협을 전망하는 '2017년 7대 사이버 공격 전망'을 발표했다.

우리는 사이버리스크를 최소화하기 위해 사이버사고를 경계하고 사이버사고에 탄력적으로 대처하여 회복할 수 있도록 준비태세를 갖춰야 할 것이다.

이들이 꼽은 2017년 7대 사이버 공격 전망으로는 △산업전반으로 번지는 한국 맞춤형 공격 △자산관리 등 공용 소프트웨어를 통한 표적 공격 △한국어 지원 등 다양한 형태의 랜섬웨어 대량 유포 △사회기반시설 대상 사이버 테러 발생 △멀버타이징 공격 등 대규모 악성코드 감염기법의 지능화 △악성앱 등 모바일 금융 서비스에 대한 위협 증가 △좀비화 된 사물인터넷(IoT) 기기의 무기화 등이다.
이중에서 주목할 만한 사항으로는 사이버공격이 특정산업분야에 국한되지 않고 산업전반적으로 번질 것으로 전망하고 있는 점이다. 특히, Deloitt와 MAPI의 조사결과에서는 제조업을 영위하는 기업이 금융업이나 유통업을 영위하는 다른 산업의 기업들보다 사이버공격에 둔감하고 처리능력이 전반적으로 떨어진다는 것을 지적하고 있다.

결언

2017년 사이버 공격전망에서 보면 산업전반으로 번지는 맞춤형공격이 예상되고 있으며 특히 제조업의 경우는 사이버공격 리스크가 점점 더 커지고 있다. 제조업은 제품혁신, 제조공정혁신을 위하여 IOT나 센서테크놀러지 등을 적용하는 전략을 토대로 커넥티드 제품에 대한 기술의 발전이 기하급수적으로 이루어지고 있는데, 이러한 신규기술 등을 토대로 비즈니스상 부가가치를 창출하고 사이버리스크가 극심하게 활동하는 환경에 대처해서 사이버침해로 인한 비용을 최소화 해야 한다.

Deloitte와 MAPI는 기업들에게 사이버리스크를 최소화하기 위한 조언을 3가지로 요약하고 있다.
첫째, 사전대응(Be secure)이며 이는 어떤 것이 안전한지 확인하기 위하여 산업 내 사이버리스크 표준과 규제를 준수하면서 기존에 알려진 위협과 신규위협으로부터 기업을 보호할 수 있는 신중하면서도 위험중심의 접근방법을 시행하는 것이다. 둘째, 지속적인 경계(Be vigilant)이며 침해사고와 이상 징후를 효율적으로 감지하기 위한 시스템, 애플리케이션과 관련자 및 외부환경의 움직임을 지속적으로 모니터하는 것이다. 셋째, 신속한 복구(Be resilient)이며 사이버 침해로 피해가 커지는 것을 방지하기 위해 조직적인 대비태세를 제고시켜 사이버사고가 비즈니스에 미치는 영향을 최소화할 준비를 하는 것이다.
우리는 위의 조언을 통해 사이버사고를 경계하고 사이버사고에 탄력적으로 대처하여 회복할 수 있도록 준비태세를 갖춰야 할 것이다.

Deloitte.