

The image features a decorative border at the top and bottom, composed of a grid of squares. Some squares are solid brown, while others contain patterns: small white dots, diagonal white lines, and wavy white lines. The central area is a solid brown rectangle.

TREND REVIEW

ICT 2019

Frost & Sullivan 2019 ICT Outlook 세미나

ICT 산업에서 가장 주목받는 ‘그것들’

5G, 커넥티드 기기, IoT 등 ICT 관련 기술들이 성숙화·상용화되는 단계에 접어들었다. 그러나 여전히 해결해야 할 과제가 남았다. 이에 글로벌 시장조사기관 프로스트 앤 설리번(Frost & Sullivan)이 지난 4월 3일 코엑스에서 ‘Investment Opportunities Beyond IoT Concept’을 주제로 브리핑을 개최했다. 현재 ICT 산업에서 가장 부상하는 5G와 IoT, Cyber Security의 미래 전망과 비즈니스 기회를 살펴볼 수 있었다. 프로스트 앤 설리번 ICT 산업 전문가 3인을 통해 바라본 ICT의 미래는 어떨까?

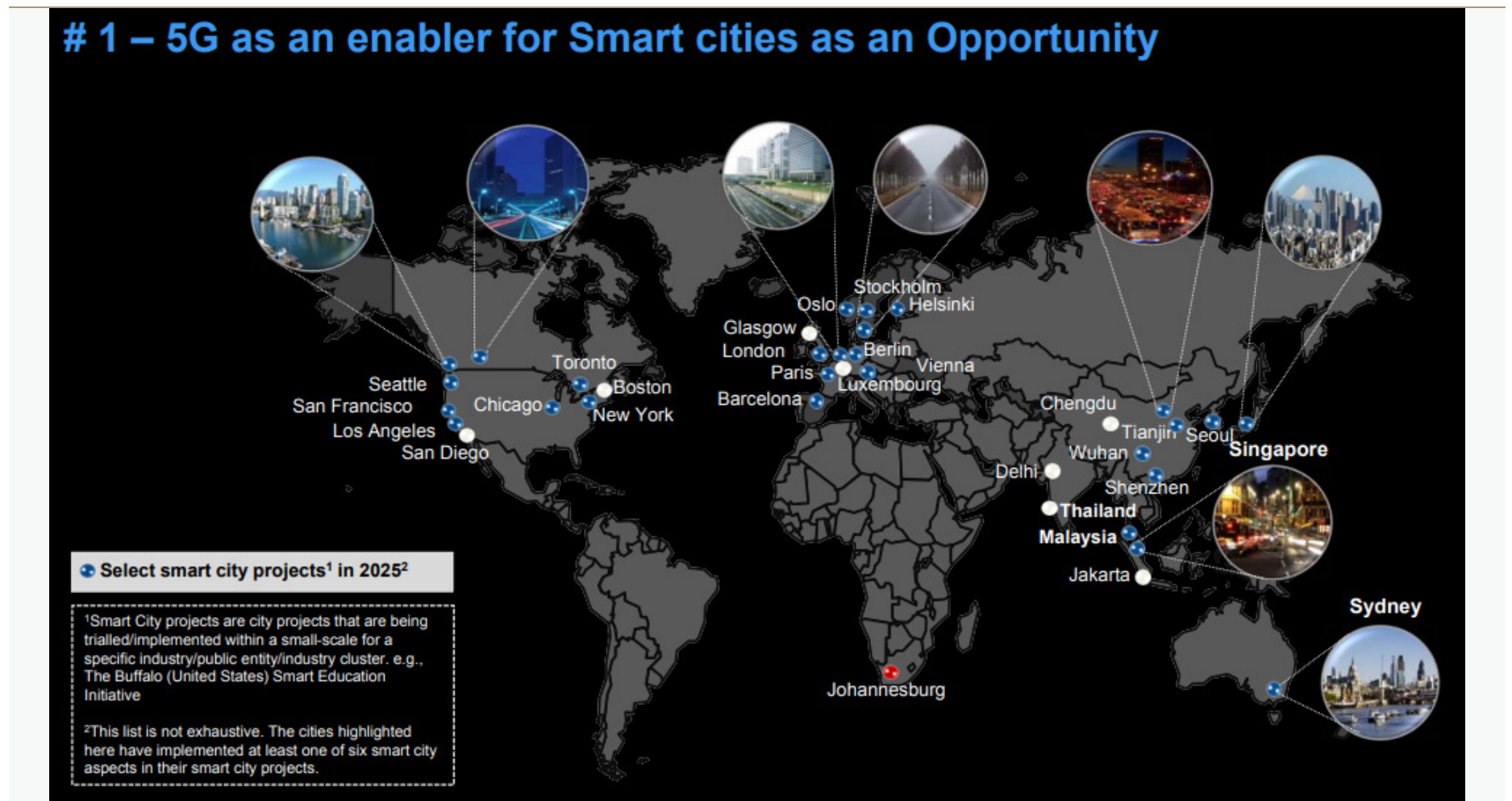
5G, 블랙홀인가? 만병통치약인가?

프로스트 앤 설리번 ICT 산업 통신팀 메이 리 쿠아(Mei Lee Quah) 수석 연구원이 ‘5G, 블랙홀인가? 만병통치약인가? (5G The Investment Blackhole or Panacea for Service Providers)’라는 주제 발표를 통해 “5G가 새로운 서비스 및 비즈니스 모델에 대한 가능성을 열었지만 아직까지도 해결해야 할 과제가 남았다”며 “5G 투자 효과 극대화를 위해 몇 가지 우려 사항들을 짚어보고 해결 방안을 살펴봐야 한다”고 했다.

메이 연구원은 5G가 필요한 이유에 대해 짧은 지연 시간, 큰 규모의 처리량 및 빠른 속도, 다량 연결 지원 등 세 가지를 꼽았다. 디지털 트랜스포메이션이 중요해지며 통신사부터 제조업, 교통, 헬스케어 산업 등 다양한 산업군에서 5G가 필요하게 되었다. 그러나 아직까지 많은 기업이 5G 기술 활용, 또는 관련 계획을 세우는데 어려움을 겪고 있다.

“5G를 활용할 기회를 잡기 위해서는 스마트시티와 같은 새로운 기회를 인지해야 한다”고 메이 연구원은 말했다. 모든 기술이 한데 모여 클러스터를 이루는 스마트시티 구축에 5G가 큰 역할을 할 것이며, 그곳에서 어떤 일을 할

수 있을지 고민해야 한다는 것이다. 그뿐만 아니라 IoT, 분석 툴 등에 5G가 쓰일 수 있기 때문에 이 또한 주목해야 한다고 했다.



[그림 1] 5G를 상용화하는 스마트시티 프로젝트 (*자료 제공: Frost & Sullivan)

여전히 많은 회사가 4G에 비해서 3배 높은 비용, 이동 전화 시스템의 변경, 통합된 5G 시스템에 대한 보안의 필요성, 투자 대비 효과에 대한 확신 부족 등의 이유로 5G 도입을 더디 진행하고 있다. 그러나 모든 서비스를 갑자기 중단하고 5G로 넘어가자는 것이 아니기 때문에 마이그레이션 로드맵을 잘 짚다면 보다 순탄하게 새로운 기술을 활용할 수 있게 될 것이다. 또한 5G를 단순 제공하는 것이 아닌 활용 방향과 오가는 모든 정보에 대한 보호 방안까지 고려해야 한다. 메이 연구원은 “5G를 어떻게 활용할 수 있을지에 대해 충분히 고민한다면 우리에게 새로운 기회를 가져다줄 것”이라고 말했다.

IoT에 대한 궁금증, 팩트 체크

프로스트 앤 설리번 한국 지사 컨설팅 부문 최승환 상무는 ‘IoT에 대한 궁금증, 팩트 체크(IoT in enterprises: separating myths from reality)’ 발표를 진행했다. 최승환 상무는 “싱가포르, 홍콩, 호주 3개국의 CIO들을 대상으로 진행했던 설문 내용을 기반으로 준비했다”며 “IoT가 안고 있는 몇 가지 오해를 풀어보는 시간을 갖고자 한다”고 말문을 열었다.

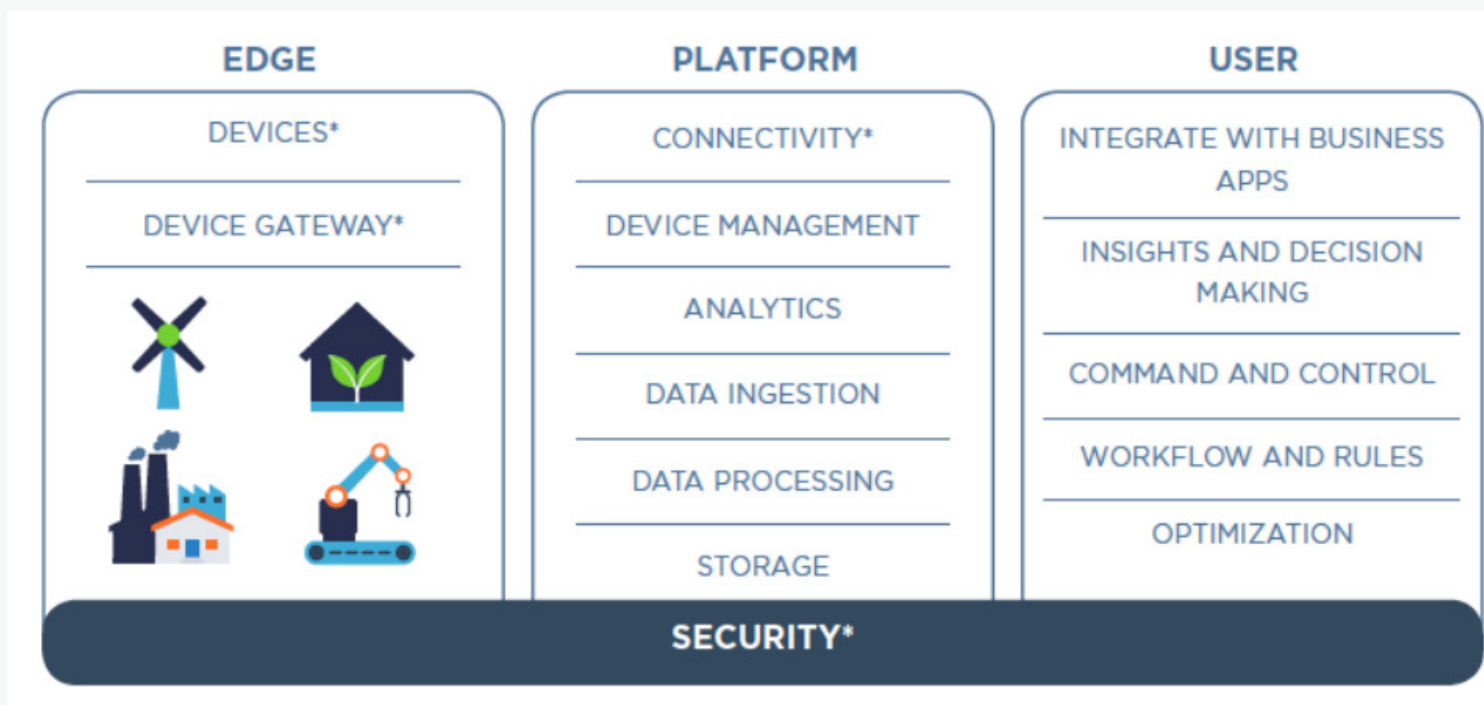
이미 많은 기업들이 개념화 단계를 지나 IoT 구축에 매진하고 있다. 최근에는 헬스케어, 농업부터 스마트시티로까지 활용 범위가 더욱 확장된 듯하다. 하지만 IoT를 정확히 인지하는 기업들이 많지 않아 기대보다 다소 좁은 관점에서 활용되고 있다. 다음은 IoT에 관해 자주 등장하는 5개의 질문과 그에 대한 프로스트 앤 설리번의 설명이다.

Q. 실제 업무에 바로 적용 가능한가?

가능하다. 이미 싱가포르, 홍콩, 호주 기업의 37%가 실무에 적용했다. 특히 홍콩의 경우 물류, 교통의 허브(Hub)로서 IoT를 적극적으로 사용하고 있다.

Q. IoT는 플러그만 꽂으면 다른 추가 작업은 필요 없는가?

그렇지 않다. IoT에 필요한 레이어를 전부 설치하는 것은 정말 중요하면서도 어려운 일이다. 특히 애플리케이션과 보안 솔루션을 연동하는 것은 녹록지 않은 작업이다. 그럼에도 불구하고 ‘보안’이라는 환경 안에서 엣지-플랫폼-사용자가 유동적으로 연결될 수 있도록 구축해야 한다.



[그림 2] IoT를 구성하고 있는 에코시스템 (*자료 제공: Frost & Sullivan)

Q. 실제로 적용할 곳이 많은가?

그렇다. 벌써 다양한 유즈케이스(Use Case)가 확인되고 있다. 특히 물류와 유통 분야에서의 사용 사례가 많은 편이다. 이미 IoT를 도입한 회사의 경우 회사 당 약 4.7건의 사용 사례를 보고했다. 이는 예상했던 평균 3.7건보다 높은 수치다.

Q. 사업 성과가 있는가?

그렇다. 실제로 IoT 사업을 시작한 회사는 효율성, 생산성, 매출 향상 등의 모든 항목에서 예상보다 성과가 높다는 평가를 내렸다. 즉 IoT에 대한 투자 가치가 상승한 것이다. IoT 활용도가 성숙할수록 IoT가 회사에 가져오는 효용 가치가 높다.

Q. 보안에 대해서는 걱정하지 않아도 되는가?

보안은 가장 중요한 과제 중 하나다. 디지털 트랜스포메이션 시대에 IT, OT(Operational Technology, 제조운영 기술), IoT는 연결되어 있으며 보안을 필요로 한다. 세 영역의 보안이 매우 중요해졌다.

최승환 상무는 IoT에 대한 명확한 사업 목표 설정과 성공을 위한 환경 조성이 중요하다고 강조했다. 단일 부서에만 국한되는 내용이 아니기 때문에 여러 부서 간의 협업과 성공 사례 공유가 중요하다. 또한 그는 “실제로 실행을 해 보는 것이 중요하다”며 “IoT를 사업에 적용하는 것이 쉽지 않더라도 실패를 통해 교훈을 얻으려는 자세가 필요하다”고 말했다.

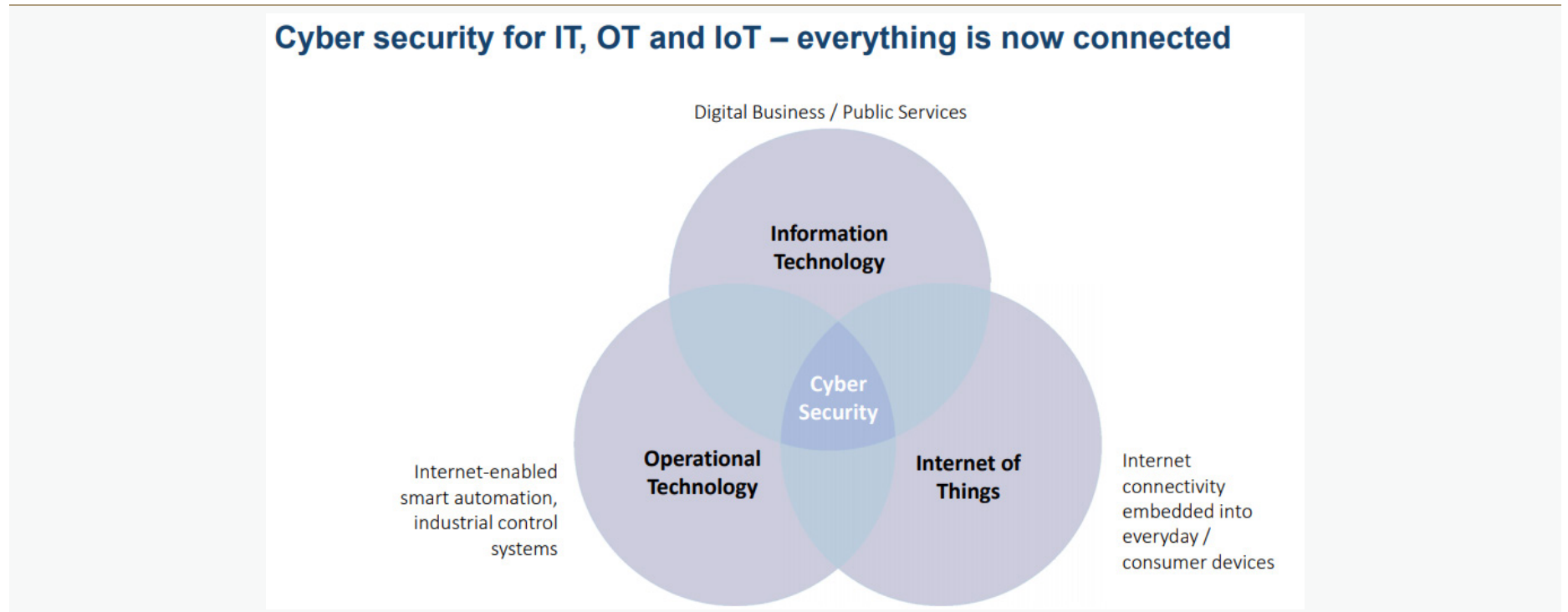
당신에게 필요한 보안의 3가지 관점

5G, IoT에 이어 마지막 세션은 ‘보안’에 대한 이야기로 진행되었다. 프로스트 앤 설리번 ICT 산업 사이버 보안 팀 케니 여(Kenny Yeo) 수석 연구원이 “당신에게 필요한 보안의 3가지 관점(The changing cyber security needs in your enterprise)”이라는 주제 발표를 통해 디지털 사회에서 기업이 고객 정보를 어떻게 보호할 수 있는지에 대해 소개했다.

케니 연구원은 “보안은 누구에게나 일어날 수 있는 일”이라며 호텔, 병원, 항공사 등에서 정보가 유출되었던 경험을 공유했다. 개인뿐만 아니라 사업 군을 막론하고 모든 기업도 위협에 노출되어 있다고 했다. 특히 디지털화를 통해 클라우드와 IoT, 데이터 분석과 같은 IT 기술들이 비즈니스에 통합되며 보안이 더욱 중요해졌다. 케니 연구원은 보안 방안을 고객-직원-기업 3가지 관점에서 제안했다.

‘고객’의 관점에서 보안은 중요한 화제다. 고객에게 있어 보안 수준은 구매 의사 결정에 큰 영향을 미친다. 보안 관리자와 기업 내부에서는 95% 이상이 보안이 제대로 이루어지고 있다고 판단한 반면 고객은 70%만이 이에 동의했다. 또한 86%의 고객은 불편함을 감수하고서라도 보안이 중요하다고 생각했으며 48%의 고객은 정보 유출 사건이 일어났던 기업의 서비스를 더 이상 이용하지 않았다. 케니 연구원이 “기업이 고객의 정보를 보호하고 고객과의 신뢰를 쌓는 방법을 고민해야 한다”고 말한 이유다.

‘직원’은 정보를 지키는 존재이기도 하지만 내부 위협이 되기도 한다. 직원이라는 내부 위협은 해커, 범죄 조직 다음으로 가장 위험한 존재로 손꼽혔다. 해커는 사회공학기법을 활용한 피싱 메일을 통해 내부에 침입한다. 때문에 내부 직원을 교육하고 의심하도록 계속 인지시켜야 한다. 또한 제대로 된 사이버 보안 문화가 정착되어야 한다. 기업 내부의 위협이 무엇인지 파악하고 이를 보완하는 것이 중요하다.



[그림 3] IT, OT, IoT 모두에게 중요한 사이버 보안

마지막으로 ‘기업’ 관점에서의 보안은 IT-OT-IoT가 클라우드를 통해 연결되며 더욱 중요해졌다. 그러나 클라우드를 사용하고 있는 기업이 착각하는 것이 있다. 바로 클라우드 서비스 업체가 충분한 보안을 제공하고 있다는 생각이다. 실제로 5%의 기업만이 클라우드 보안에 준비되어 있고 그 외에는 클라우드 보안을 잘못 사용하고 있다. 클라우드 보안은 클라우드 서비스 업체에서 제공하는 것 외에도 기업에서 준비하고 갖출 필요가 있다.

이제 ICT 기술에 대한 이해를 넘어서 어떻게 사업에 적용할 수 있을지, 또 어떻게 확장할 수 있을지 고민해야 하는 시기다. 또한 산업 분야를 막론하고 사이버 보안에 대한 준비가 중요해졌다. 거센 ICT의 바람에 적응하기 위해서는 반드시 오가는 데이터와 중요한 자산을 지켜줄 보안 시스템을 마련해 놓아야 할 것이다.