Deloitte. Insights

A report from the Deloitte Center for Government Insights

스마트 시티의 사이버보안:

점점 더 연결되어 가는 도시 미래의 뚜렷한 위험을 다루는 법

May 2019

서론

스마트 시티(smart city)는 도시 생활의 미래이다. 스마트 시티는 도시 공공서비스의 효율성과 효과를 늘리기 위해 3D, 즉 디지털 기술(Digital technologies), 데이터(Data), 디자인 사고(Design thinking)를 활용한다. 그러나 디지털 변화의 새로운 파도는 스마트 시티의 존재 자체에 중요한 영향을 끼칠 수 있는 사이버 위험 또한 가져온다. 사이버 위협은 수년간 증가해왔고, 최근 몇 년 동안에는 데이터와 물적 자산을 타깃으로 삼는 사이버 공격이 폭발적으로 증가했다.

연결된 기기(connected devices)가 빠른 속도로 급증하고 있다. IoT(Internet of Things; 사물인터넷) 기기의 수가 현재 84억 개인데, 2020년까지 그 수가 약 2백억으로 증가할 것으로 예상된다. 이에 따라 한 지역이 당한 사이버 공격과 취약성이, 수많은 지역에 파급 효과를 미칠 수 있다. 그 결과는 단순히 데이터 손실, 재정적 영향, 명예 실추 등의 문제 등, 그 자체로도 이미 충분히 심각한 문제들을 넘어선다. 그 결과는 보건, 대중교통, 법률 집행, 전력 및 공익사업, 주거 서비스 등 광대한 영역의 주요 공공서비스와 인프라의 붕괴까지 포함한다. 이러한 붕괴는 인명손실과 사회적 및 경제적 시스템의 붕괴로 이어질 수 있다.

도시의 빠른 초연결(hyperconnectivity)과 디지털화는 사이버 위협의 성장을 가속화하고 있다. 이 문제를 해결하기 위해서는 정부 리더들과 도시 설계자, 기타 이해 당사자들이 사이버 보안 원칙을 뒷전으로 미루지 않고, 이를 스마트 시티 거버넌스, 설계, 운영 등의 필수 요소로 만들어야 한다. 본고에서 우리는 스마트 시티 생태계 내에서 사이버 위험에 영향을 끼치는 주요 요인과, 시 리더들이 이러한 위험을 다루는데 채택할 수 있는 광범위한 접근법을 살펴보고자 한다.

스마트 시티가 독특한 사이버 리스크를 마주한다

스마트 시티는 공공서비스, 공공단체, 민간 기업, 인력, 프로세스, 기기, 도시 인프라가 서로 지속적으로 교류하는 복잡한 생태계이다. 이 생태계의 기저에 있는 기술 인프라는 가장자리(the edge), 중심부(the core), 커뮤니케이션 채널(the communication channel)로 이루어져 있다(그림 1). 가장자리 층은 센서, 작동기, IoT 기기, 스마트폰 등으로 이루어져 있다. 중심부 층은 가장자리 층에서 흘러들어오는 데이터를 처리하고 분석하는 기술 플랫폼이다. 커뮤니케이션 채널 층은 중심부 층과 가장자리 층이 서로 지속적으로 데이터를 교환하도록 하여 이 생태계의 다양한 구성 요소들을 원활하게 통합한다.

엄청난 양의 정보 교환, 서로 전혀 다른 IoT 기기 간의 통합, 역동적으로 변화하는 프로세스로 인해 새로운 사이버 위협이 나타나는데, 이러한 위협은 기술 인프라를 감싸는 생태계의 다른 구성 요소들의 복잡한 특징들에 의해 더 심각해진다. 예를 들어 도시들에게 데이터 거버넌스는 골치 아픈 이슈일 수 있다. 왜냐하면 데이터가 내부적인지 외부적인지, 데이터가 거래성인지 개인용인지, 거래 정보가 IoT 기기를 통해 수집되었는지, 데이터가 어떻게 저장, 보관, 복제 및 삭제되는지 등에 대해 생각해야 하기 때문이다. 게다가 공통된 기준과 정책의 부재로 많은 도시는, 상호운용성 및 통합 문제를 야기하고 사이버 위험을 악화시키는 새로운 공급업체들과 제품들을 가지고 실험하고 있다.

그림 1

스마트 시티 생태계는 가장자리, 중심부, 커뮤니케이션 채널, 이 세 개의 층으로 구성되어있다.

중심부 (THE CORE)

중심부 층은 데이터를 처리하고 가장자리 층으로부터 흘러들어오는 데이터를 분석하기 위해 비즈니스 로직을 생성하는 기술 플랫폼(클라우드 플랫폼, IoT 데이터 플랫폼)이다.

커뮤니케이션 층 (THE COMMUNICATION LAYER)

커뮤니케이션 채널(블루투스, NFC, LTE, 와이파이 다이렉트 등)은 중심부와 가장자리 층이 서로 지속적으로 데이터를 교환하도록 하여 생태계의 다양한 구성 요소들을 원활히 통합한다.

가장자리 (THE EDGE)

가장자리 층은 센서, 작동기, 스마트폰과 같은 기기뿐만 아니라 스마트 조명과 스마트 쓰레기 수거 등의 IoT 응용 프로그램으로 이루어져 있다. 이것이 스마트 시티의 프런트엔드(front end)이다.

스마트 시티 생태계에서는 세 가지 요인이 잠재적인 사이버 위험에 영향을 끼친다(그림 2).

1. 사이버 세계와 물리적 세계의 융합
2. 기존 시스템과 새 시스템 간의 상호운용성(inter-operability)
3. 서로 다른 공공서비스의 통합과 이를 가능케 하는 인프라

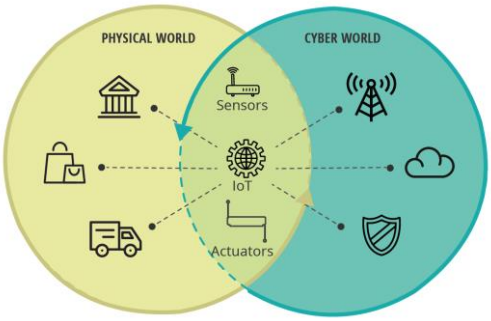
사이버 위험의 상황을 어떻게 해결할지 이해하기 위해서는, 각 요소를 더 깊이 탐구하는 것이 도움 된다.

그림 2

도시 내에 사이버 위험에 영향을 끼치는 세 개의 핵심 요인

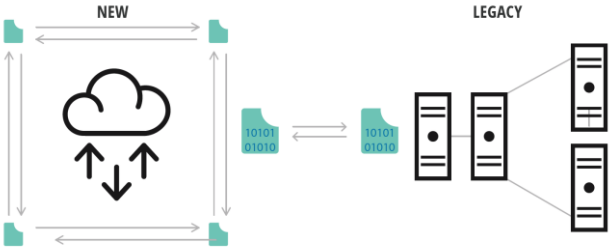
1. 융합

사이버 세계와 물리적 세계의 경계를 허무는 IT와 OT(operational technology) 인프라의 융합



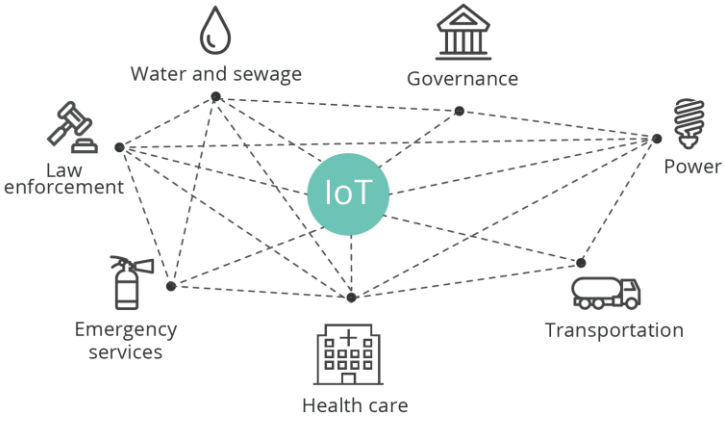
2. 상호운용성

기존(legacy)의 시스템/플랫폼과 새로운 시스템/플랫폼 간의 공존과 빈번한 상호작용



3. 통합

IoT와 디지털 기술을 통한 여러 분야 서비스의 통합과 혼합



사이버 세계와 물리적 세계의 융합

스마트 시티는 사이버 세계와 물리적 세계 간의 경계를 희미하게 만든다. 이런 환경 속에서, 데이터 중심의 컴퓨팅에 사용하는 정보 기술(IT; information technology) 시스템과 사건, 프로세스, 기기를 감시하고 도시 운영을 조정하는 데 사용하는 운영 기술(OT; operational technology)을 통해 사람, 프로세스, 장소가 통합된다. 이 융합으로 도시들은 원격 사이버 운영을 통해 기술 시스템을 컨트롤하고 통제할 수 있다.

그러나 이 융합으로 인해 가장자리 층(the edge)의 많은 기기가 사이버 위협의 매개체가 될 수 있고, 악성 행위자들이 시스템에 들어와서 현장 운영을 방해하고 사이버 위험 전망을 기하급수적으로 확대할 수 있는 위험 가능성이 증가한다. IoT 기기의 급증으로 공격자들은 이제, 도시의 시스템을 위태롭게 하고 그 결과 생겨나는 취약성을 악용할 수 있는 수많은 진입점(entry point)을 가지게 된다.

기존 시스템과 새 시스템 간의 상호운용성

보통 디지털 변화를 추구하는 조직들은 새로운 디지털 기술을 기존 시스템에 통합한다. 이는 일관적이지 않은 보안 정책과 절차, 서로 다른 기술 플랫폼들 등의 중대한 문제와 위험을 불러일으킨다. 이 문제점들은 스마트 시티 생태계 도처에 잠재적인 보안 취약성을 야기한다.

많은 도시가 점차 IoT를 해결책으로 사용하나 이를 개조 모델 내에서 사용함에 따라, 상황은 악화된다. 예를 들어, 도시 내의 대규모 가스 및 수도 시스템은 대대적으로 센서를 배치했다. 이 센서들은 중앙으로 데이터가 집계되고 분석되도록 광범위한 네트워크에 연결되어야 한다. 그러나 이 센서들은 최소한의 보안 프로토콜을 가지고 있다. 장기적으로 봤을 때, 많은 기기가 물리적으로 업그레이드되는 것이 불가능해질 수 있기 때문에, 개조는 실행 가능한 옵션이 아닐 수 있다.

또 다른 문제점은 IoT 기기의 기능을 통제하는 데 일반적으로 받아들여지는 기준이 없다는 점이다. 시의 부서와 기관은 보통, 다른 포맷으로 데이터를 만들어 내고 다른 커뮤니케이션 프로토콜을 사용하는 여러 업체의 센서 기술을 사용한다. 이런 상황에서 상호운용성을 생성하는 것은 어려울 수 있다. 도시들은 상호운용성과 보안성 사이에서 저울질해야 할 수 있다. IoT 생태계에 새로운 기기가 더해질 때마다 공격에 노출되는 부분이 늘어나 악의적 공격의 기회가 늘어난다.

도시 공공서비스들의 통합과 인프라

전통적으로 도시들은 광범위한 분야의 서로 독립적인 공공서비스를 제공해왔다(예를 들어 전력, 수도, 하수도, 대중교통, 공공사업, 법률 집행, 소방, 복지 등). 일반적으로 독자적인 시스템과 프로세스, 자산을 사용하는 기관들이 각 공공서비스를 제공했다. 이제 이 서비스들은 디지털 기술로 상호 연결된 웹을 통해 천천히 연결되며 통합되고 있다.

도시들이 새로운 서비스와 효율성을 위해 기회를 확보하는 동안, 이러한 서비스와 시스템의 통합은 그 자체의 독특한 문제들을 발생시킨다. 늘어나는 통합과 상호연결성, 데이터 교환으로 인해 한 서비스 분야의 문제가 다른 분야로 빠르게 퍼지게 된다. 즉 취약성을 공유하게 되는 것이다. 이는 광범위한 참사로 이어질 수 있다. 게다가 도시들은 규제 요건을 재고하고, 다양한 보안 프로토콜을 합리화하며, 데이터 소유권과 사용 문제를 고심해야 한다.

그뿐만 아니라 다른 여러 시스템에 저장된 데이터는 남용되기 쉬우며, 이는 시민의 프라이버시에 영향을 줄 수 있다. 예를 들어 데이터의 개인 식별자를 마스킹하거나 삭제하는 것은 중요한 일이다. 그러나 악의적인 공격자들이 개인을 재식별하기 위해 다른 데이터 세트를 매치시키는 기법과 방법이 점차 정교해지고 있다. 그래서 다수의 시스템과 데이터 세트를 위태롭게 하는 위반 행위는 도시들에게 심각한 프라이버시 사건이 될 수 있다.

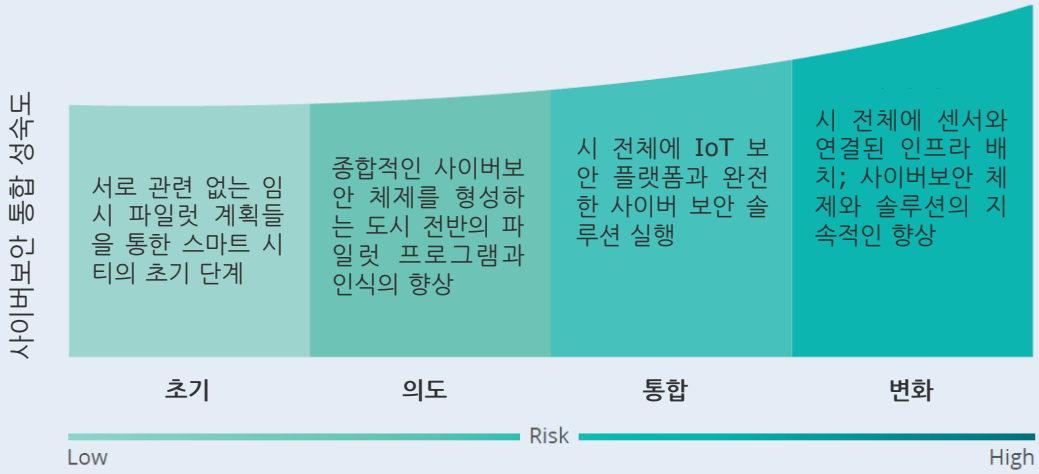
많은 도시가 훨씬 더 많은 데이터, 시스템, 기기를 연결하며 다양한 공공서비스와 인프라의 통합을 계획함에 따라, 사이버 위험은 향후 몇 년간 계속 진화할 것이다.

스마트 시티의 사이버 위험 진화 곡선 이해하기

대부분의 스마트 시티는 기존 기술과 신기술의 다양한 혼합에 따른 4단계의 진화 경로를 따른다. 단계가 올라갈 때마다, 기술 인프라의 규모와 잠재적 공격 매개체가 크게 증가하며, 이에 상응하는 사이버 보안 전략의 발달이 필요하다.

그림 3

사이버보안 전략은 스마트 시티의 디지털 변화와 함께 진화해야 한다.



Source: Deloitte analysis.

초기 단계에는 시가 통제하는 하드웨어에 내장된 적은 수의 센서들을 통해 데이터가 수집된다. 이 단계에서는 위반 행위가 일어날 잠재적 지점(points)이 일반적으로 제한되어있다. 그러나, 다음 단계인 의도 단계에서 도시는 연결된 인프라와 시민들의 스마트폰으로부터 데이터를 모으기 시작한다. 이때 갑자기 몇백만 개의 통제되지 않은 잠재적인 위반 행위 지점이 생겨난다. 대부분 시의 통제를 벗어나 있다. 후기 단계에서는 중심부(the core)에 있는 소프트웨어 봇들이 인공지능을 이용하여 인간의 관여 없이도 결정을 내리고 행동한다. 이때 잠재적인 공격 매개체들은 무한에 가까우며 지속적이다.

도시가 이 진화 곡선을 따라 올라갈 때, 융합의 정도, 기술 인프라와 이에 상응하는 상호운용성의 규모, 공공서비스의 통합이 증가한다는 사실을 주목해야 한다. 예를 들어, 초기나 의도 단계에는 도시에 몇백 개의 연결된 기기밖에 없을 지 몰라도, 통합 단계와 변화 단계에는 그 수가 수천, 혹은 수백만이 될 수 있으며 이 성장을 지원하는 더 나은 인프라가 필요하다. 이 상황은 결국 스마트 시티 생태계의 중심부와 가장자리, 커뮤니케이션 층을 더 복잡하게 만든다. 그러므로, 사이버 위험 역량의 성숙도는 스마트 시티 생태계 구성요소들의 통합 정도와 정비례한다. 그리고 사이버 위험 관리 접근법은 이러한 구성 요소를 모두 고려해야 한다.

사이버보안에 대한 총체적 접근법

디지털 인프라와 물리적 인프라의 융합, 그로 인해 나타나는 상호운용성, 도시 시스템과 데이터 사이의 상호연결성을 위해 많은 도시가 계속해서 노력하고 있다. 기밀 유지, 완전성, 유용성, 보안, 탄력성 등의 스마트 시티의 보안 목표는 데이터를 안전하게 지키기 위해 전통적인 IT에 근거해야 하고, 시스템 및 프로세스의 안전과 탄력성을 보장하기 위해 OT의 목표에 근거해야 한다. 이 통합된 보안 목표들은 도시들이 더 안전하고 탄력성 있는 운영 환경을 유지하도록 돕는다.

통합된 사이버 위험 프레임워크는 스마트 시티 계획, 설계, 변화 단계에 포함할 관리 원칙을 도시들에게 제시할 수 있다. 이 프레임워크는, 어떻게 사이버 위험이 유저, 정부, 공공서비스, 인프라, 프로세스 등의 모든 생태계 구성원에 영향을 미칠 수 있는지 알아내고 각 시스템과 자산의 상호 영향력을 평가하는 산업 기준과 법적 및 규제 사항으로 이루어져 있다. 이러한 통합적인 접근법은 도시 이해 당사자들이 특정 서비스나 운영상의 영향에 대응하기보다는, 위험과 취약성을 큰 그림으로 바라볼 수 있도록 해준다. 이 접근법은 궁극적으로 아래의 표에 나타난 사이버 보안 프로그램의 핵심 역량을 발달할 수 있도록 해준다.

사이버보안으로의 통합적인 접근법은 다섯 개의 핵심 구성요소에 기반한다.

구성 요소	디테일
디지털 신뢰 플랫폼 (Digital trust platform)	신뢰도 높은 원활한 연결을 실현하고, 연결된 생태계 내의 신원과 관계를 관리하는 플랫폼. 사람, 기기, 시스템 사이의 맥락적인 관계를 관리하는데 도움 될 수 있다. 이 접근 방식은, 위치 기반의 상황 인식을 제공하는 지리 공간 기술에 의해 증강된 적응형, 행동 기반의 보안 메커니즘을 통해, 사람과 기기를 식별, 인증 및 승인할 수 있도록 설계되어야 한다.
프라이버시 보호 설계 (Privacy-by-design)	프라이버시 보호 설계는 기술, 프로세스, 인프라를 설계할 때 먼저 시민의 프라이버시를 포함함으로써 보호하는 것을 목표로 하는 개념이다. 이는 개인 정보 수집을 제한하고, 데이터 암호화 프로세스를 더 엄격하게 하며, 개인 정보를 익명화하고, 데이터 만료 문제를 다룬다.
사이버위험 정보 및 분석 플랫폼 (Cyberthreat Intelligence and analysis platform)	도시들이 내부 데이터를 넘어 넘어 일어나고 있는 사건이나 외부 데이터베이스를 바탕으로 위험을 파악하도록 하는 정찰 역량을 가진, 생태계 전반에 걸친 플랫폼. 이 플랫폼은 행동 분석, 머신 러닝, 인공지능 역량을 사용함으로써, 시나리오 계획과 대응에 더 나은 정보를 제공할 수 있는, 위협 상황의 완전한 그림을 제공할 수 있다.
사이버 대응 및 회복력 (Cyber response and resilience)	사이버 대응과 회복력이란 잠재적인 사이버 공격에 대비하는 것이다. 사이버 전쟁 게이밍과 시뮬레이션은 시 당국이 사이버 위협에 대응하는 준비성과 신속성을 측정하고 잠재적 공격을 다루기 위한 강력한 회복 플랜을 만드는 데 도움이 된다. 이는 또한 위협을 추적하고 다른 도시 시스템에 퍼지지 않도록 방지하는 사이버 포렌식 역량을 개발하는 것도 포함한다.
사이버 역량 및 인식 프로그램 (Cyber competencies and awareness program)	사이버 노동 인력의 부족은 정부에게 지속적인 과제이며, 사이버보안 전략을 추진하는데 장애물이 될 수 있다. 스마트 시티 운영에는 IT 외에도 노동력의 많은 부분에서 사이버 관련 능력을 갖춘 새로운 노동자들이 필요할 것이다. 예를 들어, 전통적인 도시 인프라 개발은 보통 토목 공학 전문 지식을 요했다. 그러나 스마트 시티가 디지털 인프라와 물리적 인프라 사이의 경계를 흐리면서, 전통적인 토목 공학 교육을 넘어서서 데이터 거버넌스와 정보통신기술을 포함하는 여러 디지털 및 물리적 인프라 시스템에 걸친 넓은 이해를 가진 토목 기사가 필요하다.

성장을 위해 도시를 안전하게 보호하기

스마트 시티의 잠재력을 실현하려면 스마트 시티의 가능성과 사이버 위험의 잠재성을 견줘보고 관련된 위험을 효과적으로 다루는 것이 중요하다. 도시들은 이해당사자들과 조직들을 더 넓은 생태계에 참여시킴으로 시작해야 한다. 도시가 고려해야 하는 단계는 다음과 같다.

- **스마트 시티와 사이버 전략을 매치시키기.** 도시들은 스마트 시티 전략과 일맥상통하는 상세한 사이버보안 전략을 규정해야 한다. 이 전략은 도시 시스템과 프로세스의 지속되는 융합, 상호운용성, 상호연결성에서부터 오는 문제점을 완화할 수 있어야 한다. 도시들은 기술 프로세스, 정책, 솔루션과 관련된 위험을 파악, 평가 및 완화하기 위해 데이터, 시스템, 사이버 자산의 광범위한 영향력 평가 수행을 고려해야 한다. 주요 자산의 상호의존성에 대한 리스크와 지식에 대한 통합된 관점은 도시들이 포괄적인 사이버보안 전략을 개발하도록 돕는다. 예를 들어, 싱가포르는 2013년도에 국가 사이버 보안 마스터 플랜에 착수했고, 뒤이어 2016년에 새로운 사이버 보안 법안을 내놓았다.

- **사이버 및 데이터 거버넌스를 형식화하기.** 도시들은 데이터, 자산, 인프라, 및 기타 기술 요소에 대한 거버넌스 접근 방식의 형식을 갖춰야 한다. 포괄적인 거버넌스 모델은 스마트 시티 생태계의 각 주요 구성 요소의 역할과 책임을 상세히 설명해야 한다. 사이버 이슈를 해결하는 생태계 접근 방식을 시행하기 위해 다양한 조직들은 확고한 거버넌스 모델을 기반으로 협력해야 한다. 도시들은 다른 도시, 국가 기관, 학계, 기업과 네트워크를 형성하여 사이버 방어를 강화하도록 위험 정보, 역량, 계약 등을 공유할 수 있다. 게다가 견고한 데이터 쉐어링 및 프라이버시 정책, 데이터 분석 기술, 그리고 "도시 데이터" 사용과 소싱을 용이하게 하는 통화 모델을 포함하는 데이터 관리는 이 거버넌스의 중요한 부분을 구성한다. 정책, 입법, 그리고 기술은 보호, 프라이버시, 투명성, 유용성 사이의 올바른 균형을 유지하기 위해 지속적으로 일치해야 한다. 거버넌스, 정책 그리고 프로세스는 도시의 전반적인 사이버 전략과 함께 발달해야 한다. 예를 들어, 헤이그라는 도시는 "헤이그 보안 델타 (Hague Security Delta)"의 본고장이다. 이는 국가 보안, 사이버 및 도시 보안, 주요 인프라 그리고 포렌식스에 종사하는 200개 이상의 단체로 이루어진 생태계이다.

- **사이버 역량을 키우기 위해 전략적 파트너십을 맺기.** 사이버 기술 차이는 금방 사라지지 않을 것이다. 그래서 도시들은 사이버 기술 차이를 메우는 데 있어서 혁신적이고 주도적이어야 한다. 시 당국은 사이버 인재를 활용하기 위해 비전통적인 방식을 탐구해야 할 수 있다. 크라우드소싱, 프라이즈 및 사이버 관련 문제를 해결하기 위한 도전 등과 같은 방식 말이다. 스마트 시티는 다양한 생태계 층에 걸친 새로운 기량과 역량을 요구한다. 도시들은 전략적인 파트너십과 서비스 공급 업체와의 계약을 통해 역량을 증가시킬 수 있다.

도시의 리더들은 사이버 위험으로부터 도시를 보호하는 것이 일시적인 일이 아니라는 것을 알아야 한다. 사이버 위험이 진화하면서 사이버 전략도 진화한다. 사이버 공격이 일어날 때 회복할 수 있는 것 또한 중요하다. 또한 이 싸움은 도시들이 혼자 싸울 수 있거나 싸워야 하는 것도 아니다. 시 당국, 학계, 민간 부문, 스타트업들로 이뤄진 생태계와 함께 해야 한다. 기술은 사이버보안 솔루션의 한 부분이 될 수 있지만, 솔루션은 데이터와 자산에 대한 포괄적인 거버넌스 모델이 필요하다. 스마트 시티 개발 프로세스의 모든 단계에 반영된 사이버보안 원칙으로 사이버 위험을 관리하는 데에, 도시들은 통합적인 접근 방식이 필요하다.

Deloitte.