Deloitte.

커넥티드 배럴 보호하기

업스트림 석유 & 가스를 위한 사이버 보안

July, 2017

사이버 위협 떨쳐내기

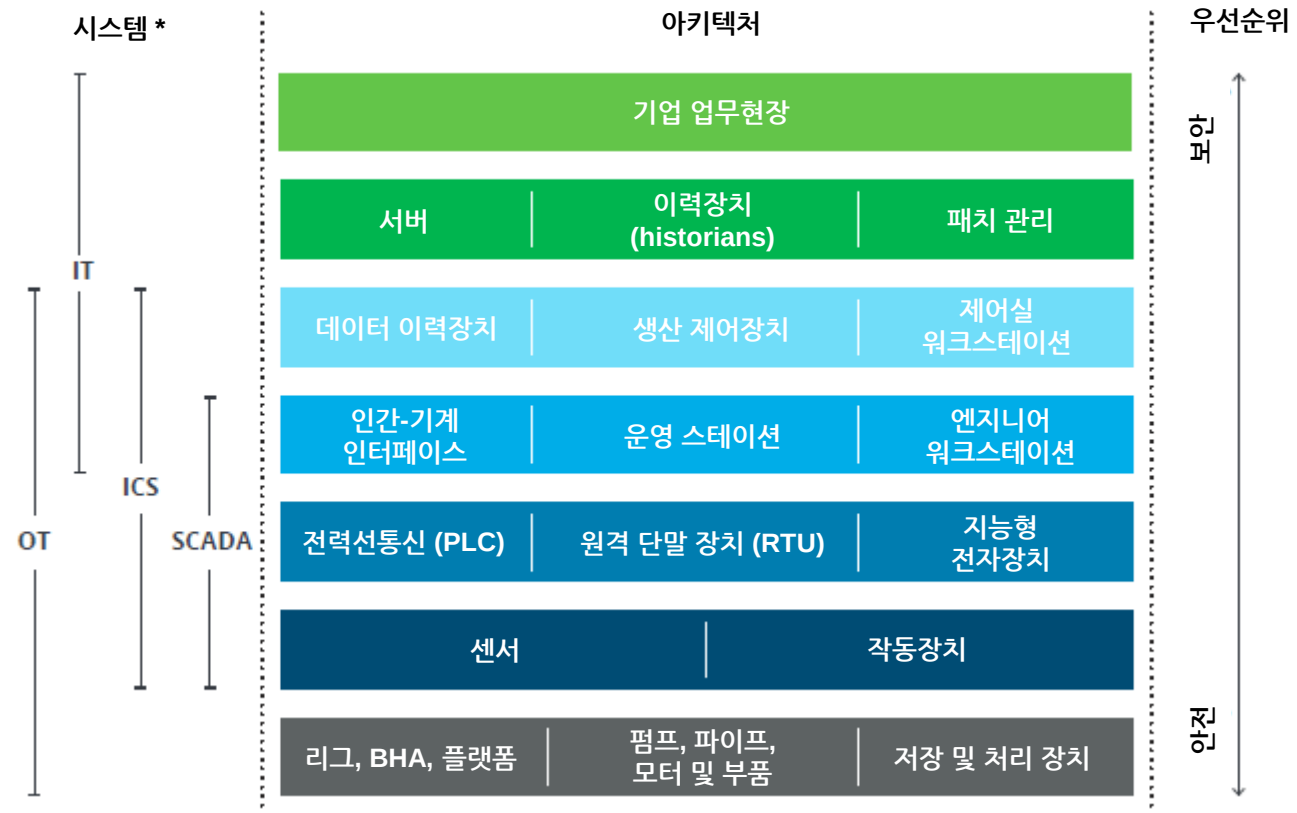
지난 몇 년간 원유 및 천연가스("O&G") 회사를 타깃으로 한 사이버 공격이 발생했으며, O&G 업계에서 연결 기술을 더 많이 사용하게 되면서 공격 빈도, 복잡성 및 여파가 증가하였다. 지금까지 O&G 업계는 사이버 공격의 대상이 될 가능성이 적다고 느끼고 있었지만 해커의 목적이 사이버 테러에서 데이터 탈취로 변화되고 연결 기술이 점점 더 중요해지면서 위험성이 빠르게 증가하고 있다.

에너지 산업은 2016년 두 번째로 사이버 공격에 취약한 산업이었으며, 미국의 O&G 회사 중 거의 4분의 1이 최소 한 번 이상의 사이버 사고를 경험하였음에도 소수의 에너지 기업만이 사이버 위험을 주요한 위험으로 보고 있다. 중대한 사이버 사고로 수억 달러의 비용이 발생할 수 있으며, 사람들의 생명과 인근 환경에 위험을 초래할 수도 있다. 예를 들어, 사이버 공격자가 오프쇼어 개발 유전에서 나오는 시멘트 슬러리 데이터를 조작하여 오프쇼어 시추 화면이 꺼지거나 유체 분출을 멈추는 데 필요한 유전 흐름 데이터를 지연시킬 경우, 그 영향은 대단히 파괴적일 수 있다.

디지털화가 문제를 확장시키다

업스트림(upstream) 업계의 "핵심 인프라" 지위와는 별개로, 전 세계에 퍼져있는 계산, 네트워크 및 물리적 작업 프로세스의 복잡한 생태계는 업스트림 업계를 사이버 공격에 매우 취약하게 만든다. 즉, 이 업계에 공격에 취약한 부분과 공격 벡터(attack vector)가 많다.(그림1 및 '사이버 문제' 참조)

그림 1. O&G 기업의 전형적인 정보기술("IT")/운영기술("OT") 아키텍쳐



(출처: Deloitte analysis)

사이버 문제

- **복잡한 생태계:** 여러 지역에서 공동 작업이 진행되고, 보안 지침이 상이한 여러 공급업체를 고용함.
- **분화된 오너십**: IT 및 OT는 별개의 목적을 가지고 개발되었으므로, 사이버 오너십 및 책임도 조직간에 분화됨.
- **보이지 않는 문제**: 방화벽은 시간이 관건인 ICS 시스템이 운영상 제약에 직면했을 경우 수용 불가한 보이지 않는 문제를 유발할 수 있음.
- **사이버 표준 비일관성**: 독점 기술과 기성 기술의 혼합이 문제를 복잡하게 만듦.
- **비정기적인 패치 적용:** 시스템이 멀고 사람이 없는 지역에 있어서 많은 시스템의 보안 패치가 비정기적이고 공급업체마다 다름.
- **구형 문제**: 많은 시스템이 긴 라이프 사이클(10년 이상)을 지니고 있어 사이버 보안을 고려하여 만들어지지 않았음. 개보수 또는 업그레이드는 비용이 많이 들고 운영에 영향을 미침.

디지털화의 증가와 운영의 상호 연관성으로 인해 사이버 위험이 더욱 높아졌으며, 연결된 업스트림 작업으로 인해 새로운 공격 벡터가 생겨났다. IoT 기술에는 센서 기술과 무선 통신 네트워크 및 여러 분석/자동화 도구가 포함되며, 이들은 복잡한 업스트림 생태계의 보안 사고에 매우 취약하다. 연결 기술의 채택 및 침투가 현재의 사이버 보안 관행을 앞서감에 따라, IoT에서 생성된 정보 및 가치뿐 아니라 미래의 기회비용이 위험에 처해 있다.

사이버 투자 우선순위 설정을 위한 취약성 평가

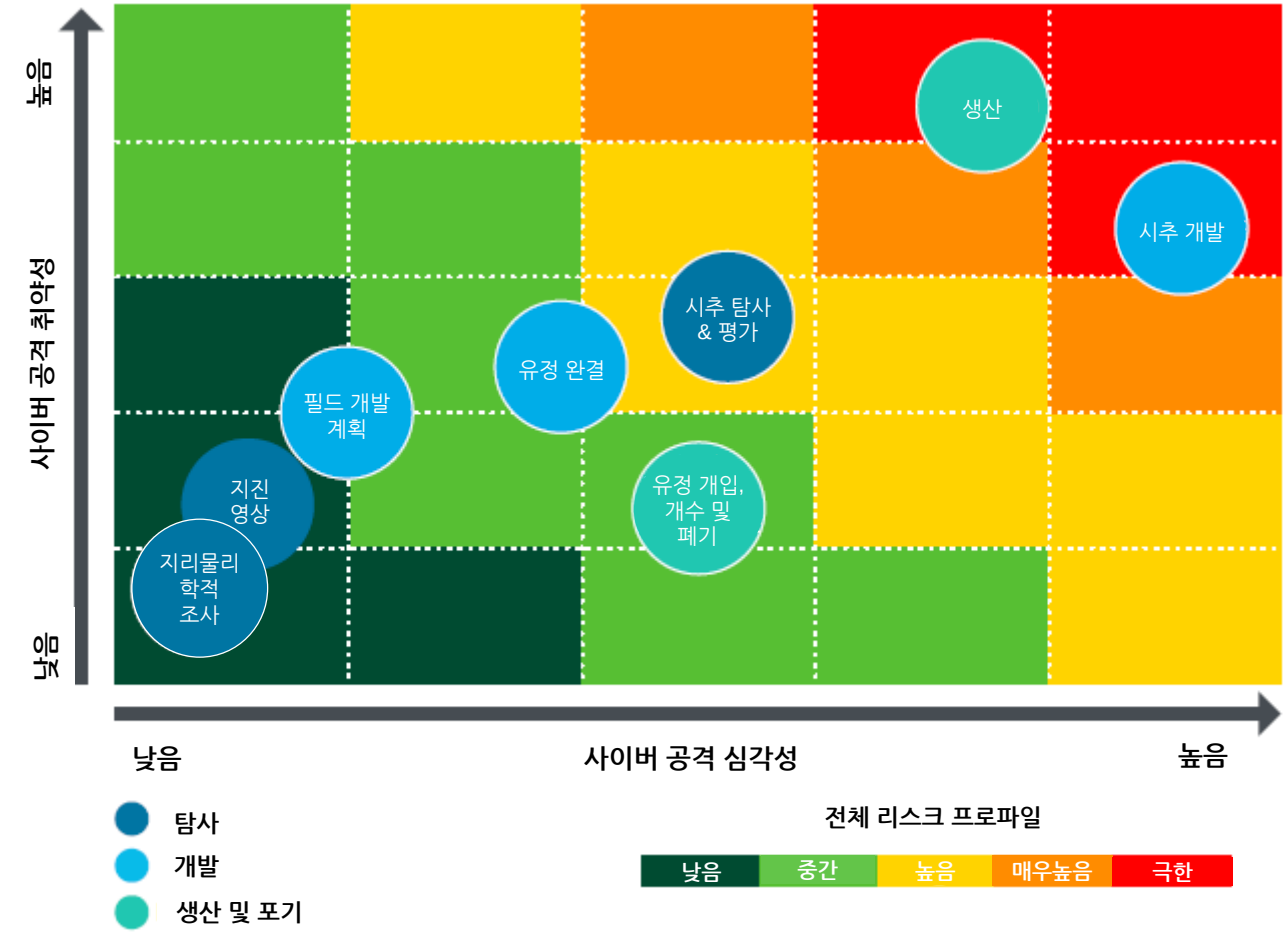
업스트림 작업의 '취약성'은 ①공격 대상(예: 벤더, 사용자 및 인터페이스의 수 또는 산업 제어 시스템의 개수와 유형 등), ②데이터 모드와 흐름(물리적 또는 디지털 & 일방, 쌍방 또는 다방향), 기존 보안 및 제어 상태에 따라 결정된다. 한편, '심각성'은 건강, 환경 및 보안 사고, 사업 중단, 법률 및 규제 이슈, 기업 명성 훼손 및 지적 재산 도용의 형태로 된 직간접 비용을 포함한다.

업스트림 작업단계(탐사, 개발, 생산 및 폐기)에는 명확한 사이버 취약성 및 심각성 프로파일이 존재한다. (그림 2 참조) 아래에서는 각 단계의 중요하고 위험한 작업들에 대해 설명하였다.

1. **탐사**: 탐사는 세 가지 주요 단계 중 심각성과 취약성이 가장 낮은 작업이다. 지진 영상과 지질학적/지구물리학적 조사 작업은 폐쇄된 데이터 수집 시스템을 사용하며, 이 작업에 대한 사이버 공격이 비즈니스 중단, 건강, 환경 및 안전 위험을 초래할 확률이 낮기 때문이다. 그러나 탐사 데이터가 시추 계획, 완결정 설계 및 매장량 추정 등 업스트림 작업에 실시간으로 투입되기 시작하면 사이버 공격의 영향은 매출 손실에서부터 비즈니스 중단까지 확대될 수 있다.
2. **개발**: 개발은 O&G 가치사슬에서 사이버 사고 위험에 특히 노출된 단계이다. 개발 시추 작업은 보다 활발한 시추 활동, 확장된 인프라와 서비스 및 엔지니어링 회사의 복잡한 생태계로 인해 훨씬 큰 사이버 공격 벡터를 지니고 있다. 취약성과 마찬가지로, 사이버 공격의 심각성 또한 시추 개발 단계에서 가장 높다. 자산 손실, 비즈니스 중단, 규제로 인한 벌금, 기업 명성 훼손, 지적 재산 도용 또는 건강, 환경 및 안전 사고 등 모든 위험 카테고리에서 이 단계의 미래 기회 비용이 가장 높다.

3. **생산 및 폐기**: 석유 및 가스 생산 작업은 업스트림 작업 중에서 가장 사이버 취약성이 높다. 주로 사이버 보안을 고려하여 구축되지 않은 레거시 자산 기반 및 기존 네트워크에 대한 모니터링 도구의 부족 때문이다. 또한, 산업 제어 시스템이 회사의 전사적 자원 계획 시스템과 점점 더 연결되고 있어 석유 및 가스 생산에 대한 사이버 공격의 심각성이 클 수 있다. 유정 개입, 작업 및 포기 단계에는 기계적 변경, 유정 진단, 대체 및 보수 작업이 포함되므로 취약성이 낮다.

그림 2. 업스트림 작업의 사이버 취약성/심각성 매트릭스



(출처: Deloitte analysis)

전체적인 위험 관리 프로그램 활용으로 사이버 위험 완화하기

다음 그림은 잠재된 보안 전략, 경계 전략 및 복구 전략을 설명 및 강조하기 위하여 예시가 될만한 세 가지 사이버 사고 사례를 기술하고 있다. 기업들이 이미 표준적인 IT 솔루션을 갖추고 있다고 전제하고 전략적 솔루션에 보다 집중하였다.

그림 3. 중요한 업스트림 작업에서 발생하는 사이버 사고의 리스크 완화 전략

(출처: Deloitte analysis)

사이버 투자를 위한 지원 얻기

사이버를 안전성, 신뢰성 및 가치 창출을 가능하게 하는 비즈니스 이슈로 제시

업스트림 석유 및 가스 산업은 자동화, 디지털화 및 IoT 기술과 함께 빠르게 발전하고 있으나, 사이버 성숙도는 이를 따라오지 못하고 있다. 사이버 보안에 대한 경영진의 지원을 받으려면 문제점을 전략적으로 프레이밍하고 사이버 보안이 회사의 세가지 중요한 운영상 과제(자산, 인력 및 환경의 안전성, 자산의 연속적인 가용성 및 신뢰성, 새로운 가치 창출)를 어떻게 실현시킬 수 있는지 설명해야 한다. 이제는 사이버 공격으로부터 작업을 보호할 때이다. 사이버는 자동화 및 디지털 유전처럼 필수 투자 항목으로 빠르게 발전할 수 있을 것이다.

Deloitte.