관리적 보안은 주로 인적 자산에 대한 보안을 지칭하고 각종 관리 절차 및 규명을 의미한다. 조직 내부의 기술 보호를 위한 체계를 세워 보안 조직 및 인원을 구성하고 운영하며 내부의 정보 시스템 이용 시 기술 정보가 빠져나가는 것을 방지하기 위해 정보 이용 절차를 수립하고, 보안 사고에 대비하여 계획을 수립하거나 대책을 마련한다. 특강에서는 과거에 우리나라의 임원급 인력들이 2~3배 이상의 높은 임금을 받고 중국으로 이직하여 기술을 유출하는 문제가 발생하여 이를 방지하기 위해 퇴사 시 몇 년 간은 동일 업종에 종사 불가능한 법 규정이 생겼다는 사례를 이야기 해주셨고, 이런 사례가 바로 기술정보를 보유하고 있는 인적 자산에 대한 보호 방안인 것 같다.

물리적 보안은 설비나 시설 자산에 대한 보안이다. 실제 기술을 다루는 사업장이나 기술 정보 및자료들을 저장하고 있는 서버실, 데이터실과 같은 주요 자산 정보 시스에 가해질 수 있는 피해를 최소하기 위해 물리적 대책을 마련해야 한다. 특강에서도 이에 대비하기 위해 일부 기업에서는 출퇴근 직원들의 소지품 수색이 진행되는 예시도 설명하였고, 발판 부분에 감지 시스템이 없어 문제가 되었던 사례도 소개해주시면서 물리적 보안의 중요성과 대책에 대해 강조하셨던 것이 기억에 남는다.

마지막으로 기술적 보안은 정보자산에 대한 보안이다. 즉, 기술에 사용되는 시스템, 네트워크, 어플리케이션, 데이터베이스, PC 등에 대한 보호가 필요하기 때문에 이에 특화하여 기술적으로 마련할 수 있는 정보 보호 대책이 필요하다. 데이터 암호화 기술, 해킹/피싱 탐지 기능, 물리적 보안을 수행할 수 있도록 기반이 되는 지문인식 시스템 등이 있다.