보안 위협 모델링

리스크 평가(Risk Assessment)에 대해 더 읽고 싶다면 여기 링크에서 확인하십시오: HTTPS://SSD.EFF.ORG/

보안 위협 모델링은 당신이 중요시 여기는 것들에 대한 위협을 식별하고 누구로부터 보호해야하는지 알도록 도와줍니다. 보안 위협 모델을 세울 때, 스스로에게 다음과 같은 질문을 해보십시오:

- 내가 무엇을 보호해야 하는가?
- 내가 누구로부터 이것을 보호해야 하는가?
- 내가 보호에 실패하면 어떤 결과가 생기는가?
- 이러한 결과들은 얼마나 가능성이 있는가?
- 가장 가능성이 높은 리스크에 어떻게 대처할 수 있는가?

보안 위협 모델링 용어들:

자산(Assets): 내가 보호해야 하는 것들

공격자(Adversaries): 이 상대로부터 자산들을 보호해야 함

위협(Threats): 보호에 실패하면 생기는 결과의 나쁨 정도

리스크(Risks): 특정 자산에 대한 특정 위협이 실제로 발생할 가능성

공격자 능력(Adversary capability):
공격자가 목적을 달성하기 위해 할 수 있는 것을 의미합니다. 예를 들어 당신의 이웃이 창문에서 당신을 관찰할 수 있는 능력을 가진 반면, 한 국가의 정보 보안 서비스는 당신의 전화 통화를 감청할 수 있는 능력을 갖고 있을지도 모릅니다. 공격자가 능력을 "갖고 있다"는 것은 꼭 그 능력을 사용한다는 의미는 아닙니다. 그러나 당신이 이러한 가능성에 대해 인지하고 준비해야 한다는 것을 의미합니다.

직접 한 번 시도해보십시오! 보석 가게 주인을 위한 보안 위협 모델을 만들어 봅시다.

보석 가게 주인을 위한 보안 위협 모델

당신은 도시에 있는 보석 가게를 물려받았습니다.
보석 가게에는 다음과 같은 것들이 있습니다:

- 1백만 달러 값어치의 다이아몬드들
- 다섯 명의 직원들
- 보안 경보 시스템 한 개
- 금고 한 개
- 현금 계산대 한 개
- 출입문 감시 카메라 한 개
- 출입문 PIN코드 보안 경보 한 개

1 당신은 어떤 자산을 보호해야 합니까?

- 1백만 달러 값어치의 다이아몬드들
- 금고 안의 현금
- 보안 경보 PIN코드
- 그 외에 다른 것들?

2 당신을 향한 공격자는 누구입니까?

- 보석 강도들
- 그 외에 다른 사람들? (다음을 고려해 보십시오: 보석 금고에 누가 접근권한을 갖고 있습니까? 금고 유지보수 직원이나 청소 직원들은 어떤가요?

3 보호에 실패하면 어떤 결과가 생기게 됩니까?

- 보석 도난
- 그 외에 다른 **위협들?** (만약 보안코드나 경보코드가 도난당한다면?)

4 이러한 결과가 생길 가능성은 얼마나 됩니까?

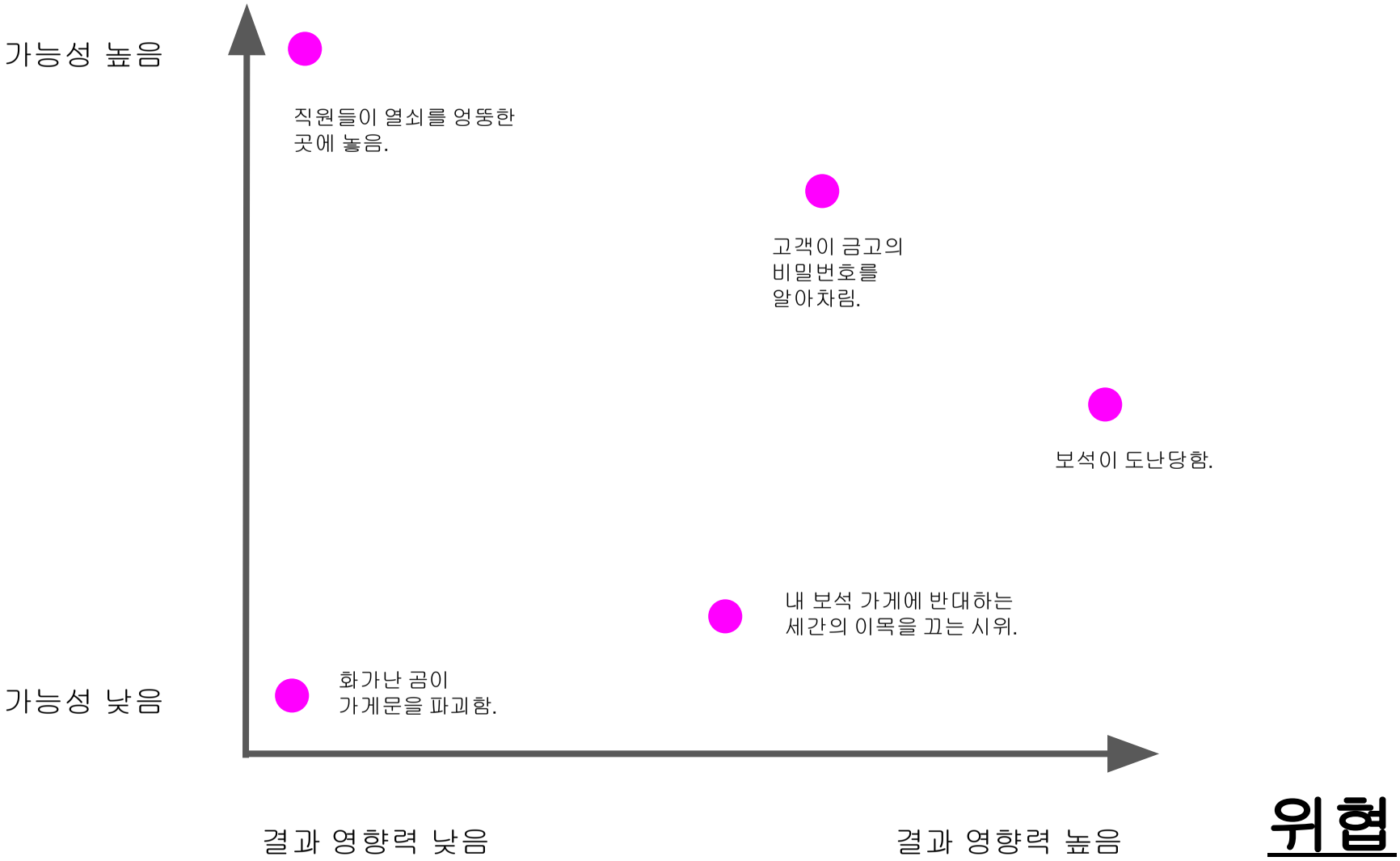
이러한 위협들이 발생할 가능성을 뒷장에 매핑(mapping)해 봅시다.

5 가장 가능성이 높은 리스크에 어떻게 대처할 수 있습니까?

- 비밀번호를 매달, 그리고 직원이 퇴직한 직후마다 바꾸기
- 그 외 방법은?

리스크

이러한 결과들이 일어날 가능성은 얼마나 될까요? 이 가능성은 당신을 향한 **공격자들의 능력에 따라** 다릅니다.



나의 리스크 평가해보기

1 **자산:** 무엇을 보호하고 싶습니까?

2 **공격자:**
누구로부터 그것을 보호하고 싶습니까?

무엇이 당신의 공격자에게 동기를 부여합니까?

당신을 향한 공격자들의 능력은 무엇입니까?

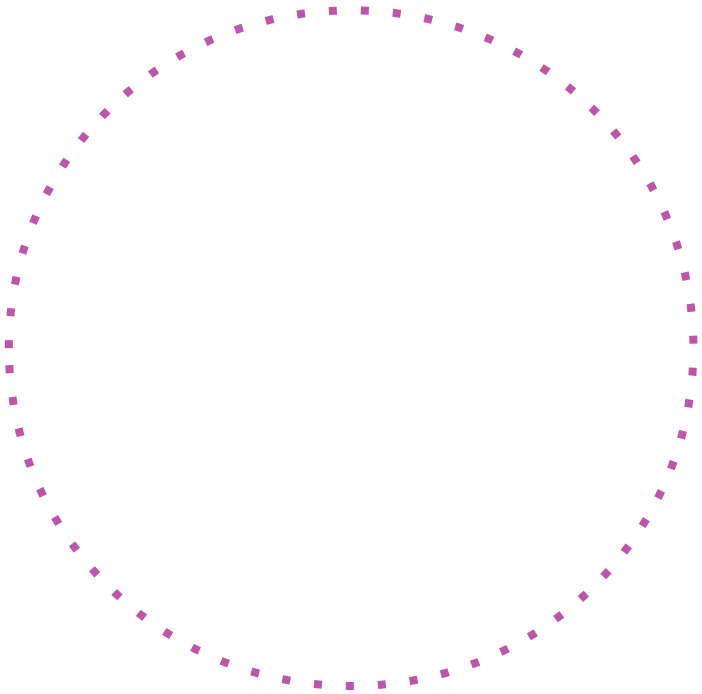
3 **위협:**
공격자가 당신의 자산을 어떻게 위협할 것입니까?

다음 페이지에서 위협의 가능성을 매핑해보십시오.

4

5 공격자에 대한 대응으로 어떤 종류의 보호가 적절합니까?

앞의 4번을 다음 페이지에 완성하였다면 이 항목을 작성하십시오.
리스크에 대한 당신의 선호도에 따라 적절한 조치방법을 결정하십시오.



6 **기술과 함께 위협은 변화합니다.**
당신의 리스크를 재평가하는 계획을 세우십시오.

나의 보안 위협 모델을 재평가하는 날짜: _____

리스크

이러한 위협이 일어날 가능성이 얼마나 됩니까? 이 가능성은 당신을 향한 **공격자들의 능력에 따라** 다릅니다.