ROM: Risk Overall Management

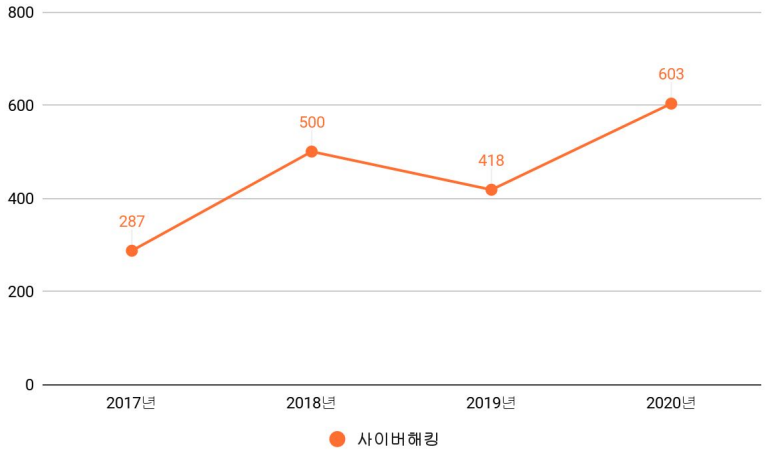
세종대학교 정보보호학과 캡스톤 팀 “CapTeen”

목차

INDEX

1. 개발동기

개발 배경



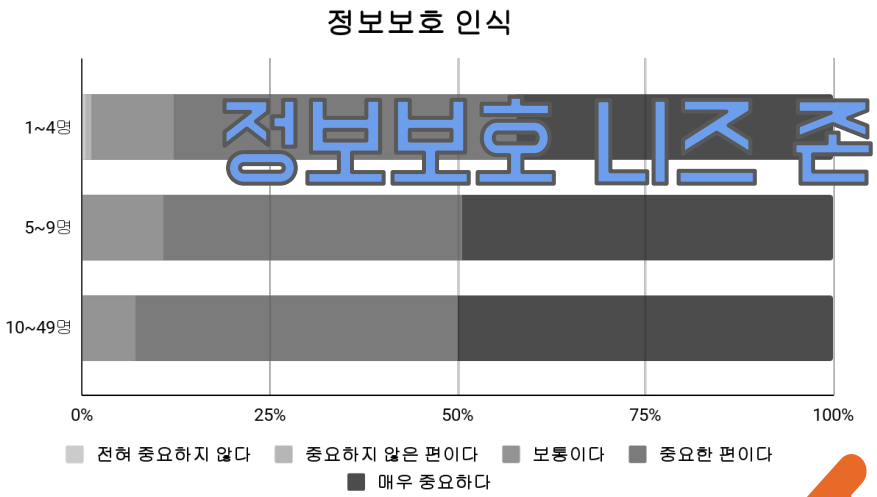
민간기업을 대상으로 한
사이버해킹이
2017년-2020년
3년 새 두 배 이상 증가

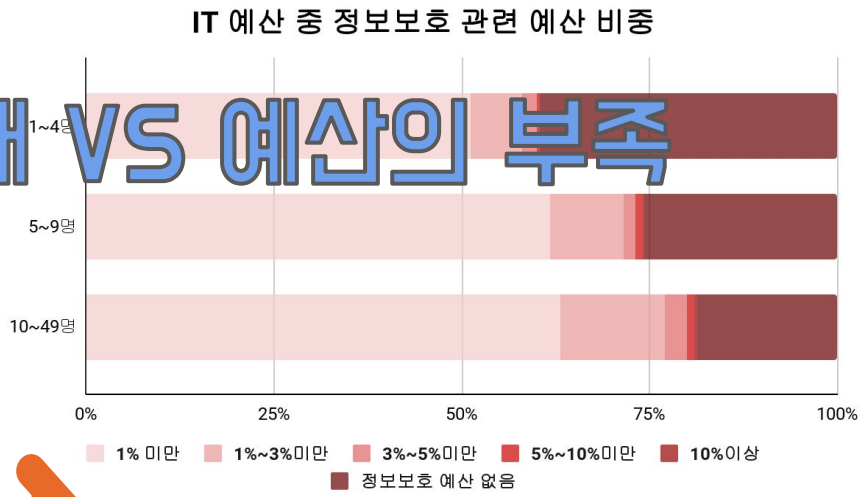
구분	2018	2019	2020	2021.8
대기업	4	10	23	10
중소기업	**467**	**386**	**522**	**390**
비영리	29	22	58	20

출처: 과기정통부 및 한국인터넷진흥원

피해 기업의 **98%**가
중소기업

개발 배경





정보보호 니즈 존재 VS 예산의 부족

50인 미만 사업장 중 85% 이상이
정보보호의 중요성 인식

동일 규모 사업장 중 정보보호 관련 예산이
0~5%: 98% 이상

출처: 2021 개인정보보호 실태조사 보고서

사용대상 및 목적

사용 대상

1. 전기통신사업자*와

2. 인터넷으로 서비스를 하는 사업자 중:
   - 인증 의무* 는 없지만 정보보안의 니즈가 존재하는 기업

사용 목적

1. 사용 대상 기업에게 약식 위험 관리 제공

2. 기업의 보안 상황에 대한 대략적인 해결책 제시

3. 위험 관리 교육 툴의 역할 수행

*「전기통신사업법」 제2조 제8호에 정의
*정보통신망법 제47조 제2항에서 명시된 정보보호 인증 의무

기대 효과

- 쉬운 UI 구성, 한눈에 볼 수 있는 그래픽을 제공함으로써 보안에 대한 심리적, 자원적 장벽을 낮출 수 있음

- 법이 보안 인증의 의무를 부여할 수 없었던 보안 사각지대에 일정 수준의 보안 독려

2. 위험관리

위험관리란?

- 위험으로부터 조직의 자산(Asset)을 지키는 프로세스
- 기업의 지속적인 생산성을 유지하는 것이 주 목표
- 위험에 체계적인 방법으로 접근하여 최선의 방식으로 대처하는 일련의 행위
  - 위험 발발 전/후를 막론한 일관된 프로세스

- 3개 단계로 구성

  1)위험 분석

  2)위험 평가

  3)위험 처리

위험 관리 과정

위험 분석

- 자산 평가
- 취약성 평가
- 위협 평가
- 보호대책 평가

위험 평가

- 위험도 산출
- DoA 확인
- DoA와 위험도 비교

DoA: Degree of Agreement;
감수할 수 있는 위험의 최대 등급

위험 처리

- 정보보호 전략 수립
  : 위험 처리 전략, 보호 대책, 개선책
- 마스터 플랜 수립

구현한 위험 관리 과정

위험 분석

- 자산 평가
- 위협 평가
- 취약성 평가
- 보호대책 평가

위험 평가

- DoA 확인
- 위험도 산출
- DoA와 위험도 비교

DoA: Degree of Agreement;

위험 처리

- 정보보호 전략 수립
  : 위험 처리 전략, 보호 대책, 개선책
- 마스터 플랜 수립

차트, 그래프 등으로 시각화해 제공

3. ROM

Risk Overall Management

구현한 위험 관리 과정

위험 분석

- 자산 평가
- 위협 평가
- 취약성 평가
- 보호대책 평가

위험 평가

- DoA 확인
- 위험도 산출
- DoA와 위험도 비교

DoA: Degree of Agreement;
감수할 수 있는 위험의 최대 등급

위험 처리

- 정보보호 전략 수립
  : 위험 처리 전략, 보호 대책, 개선책
- 마스터 플랜 수립

위험 관리 과정

위험 분석

- 자산 평가
- 위협 평가
- 취약성 평가
- 보호대책 평가

자산평가 — 기밀성, 무결성, 가용성, 업무의존도 기준으로 자산 등급 산정

위협평가 — 빈도, 피해도 기준으로 위협 등급 산정

취약성평가 — 심각성, 노출성 기준으로 취약성 등급 산정

위험 관리 과정

위험 평가

위험도 매트릭스

등급 설정 매트릭스를
이용해 위험도 결정

- DoA 확인
- 위험도 산출
- DoA와 위험도 비교

DoA: Degree of Agreement;
감수할 수 있는 위험의 최대 등급

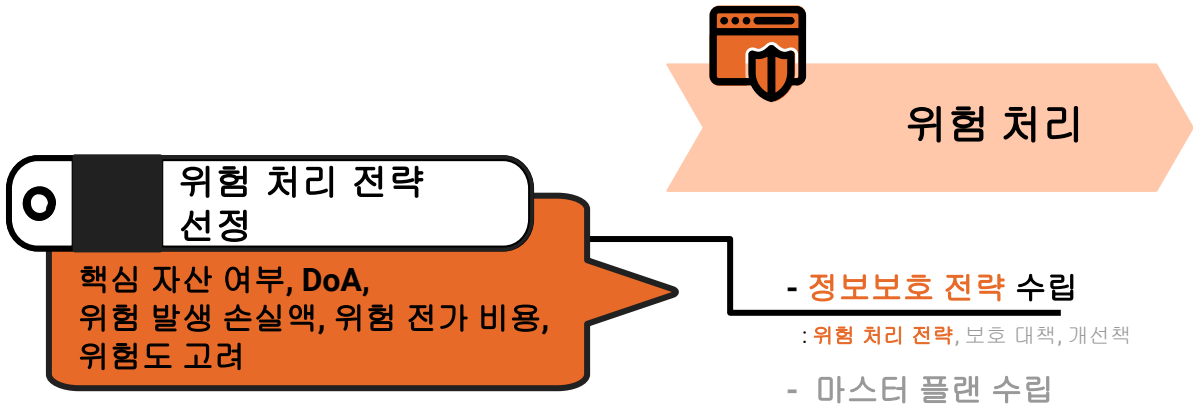
DoA 입력

사용자의 조직이 결정한
위험 수용 가능 최대 등급

"DoA<위험도" 인가?

위험 처리 단계의 일부로 편입,
위험 처리 전략 선정에 이용

구현한 위험 관리 과정



유저가 너무 낮게 입력한 DoA 보정

4. 시연 영상

5. Future Works

Future Works

- 최종 화면: 더 좋은 시각화 고려
  - 예: **Spider Diagram, Risk Hitmap** 등의 그래프 보여주기
- 제시된 해결책 적용 여부를 체크, 회사의 위험 관리 수준을 그래프로 제공하는 기능 추가
- 더불어, 다른 회사들의 평균적인 **Score**와 비교해 주는 기능 추가
- 사용자의 비즈니스 종류를 저장함으로써 비즈니스별로 어떤 종류의 자산을 가지고, 각 자산 별로 어떻게 등급을 부여하는지 분석해 맞춤형 서비스 제공

Q&A