소프트웨어세미나 3

정보 보안 인식제고

정보보안 개요

정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법을 의미

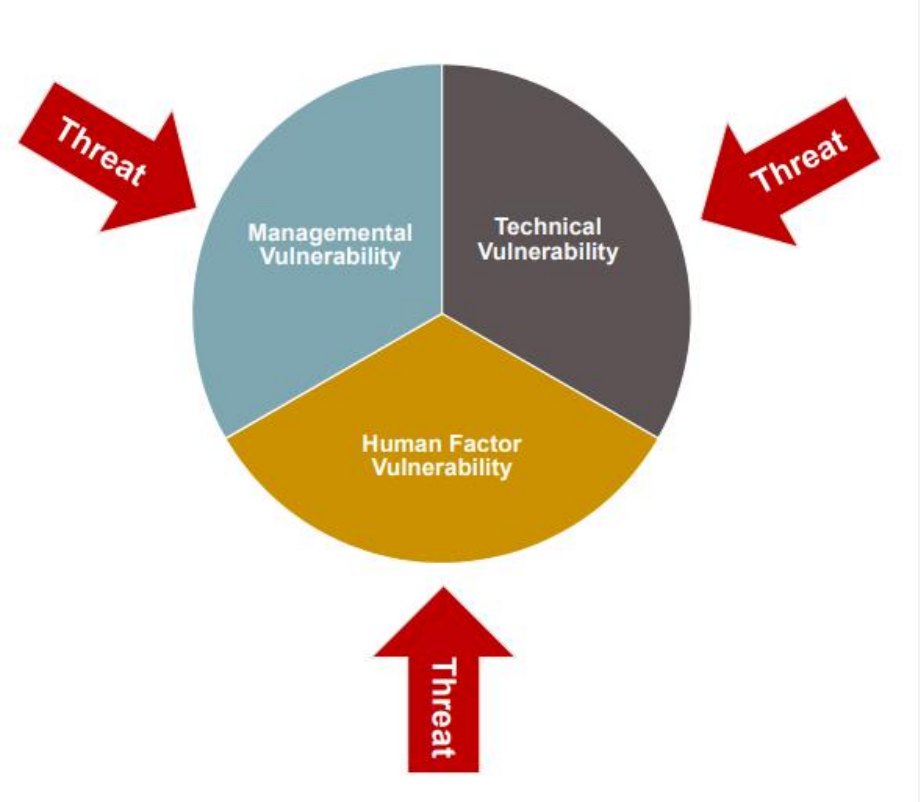
공급자 측면 : 내·외부의 위협요인들로부터 네트워크,시스템 등의 하드웨어, 데이터베이스, 통신 , 전산시설 등 정보자산을 안전하게 보호·운영하기 위한 일련의 행위

사용자 측면 : 개인 정보 유출, 남용을 방지하기 위한 일련의 행위.

다변화 되고 있는 보안위협

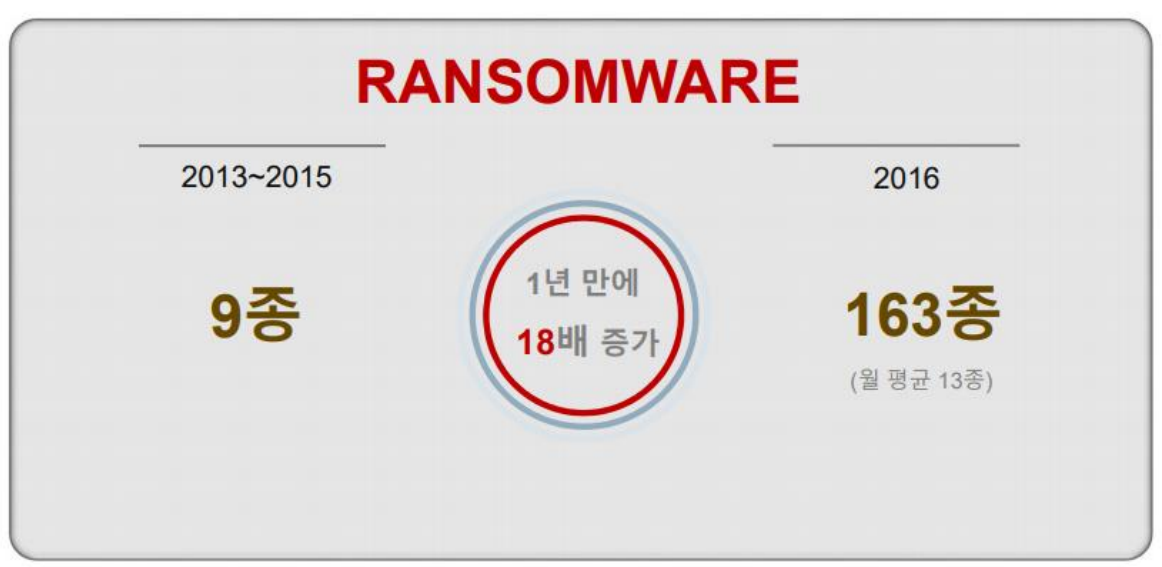
최근 보안 위협의 접촉면

- 취약성 (Vulnerability)
  - Managemental
  - Technical
  - Human Factor Vulnerability



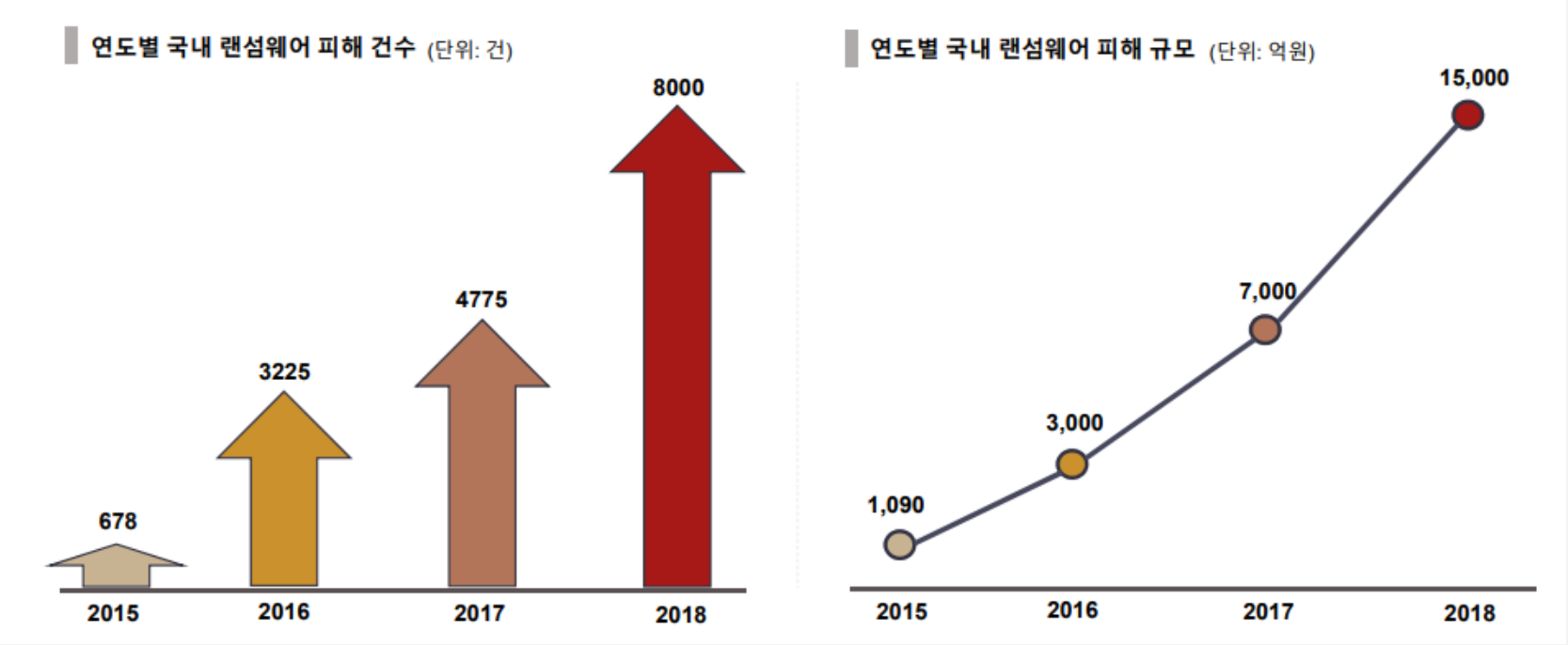
인간 요인 취약성

- 실제 예시
  - 랜섬웨어
    - 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류



인간 요인 취약성

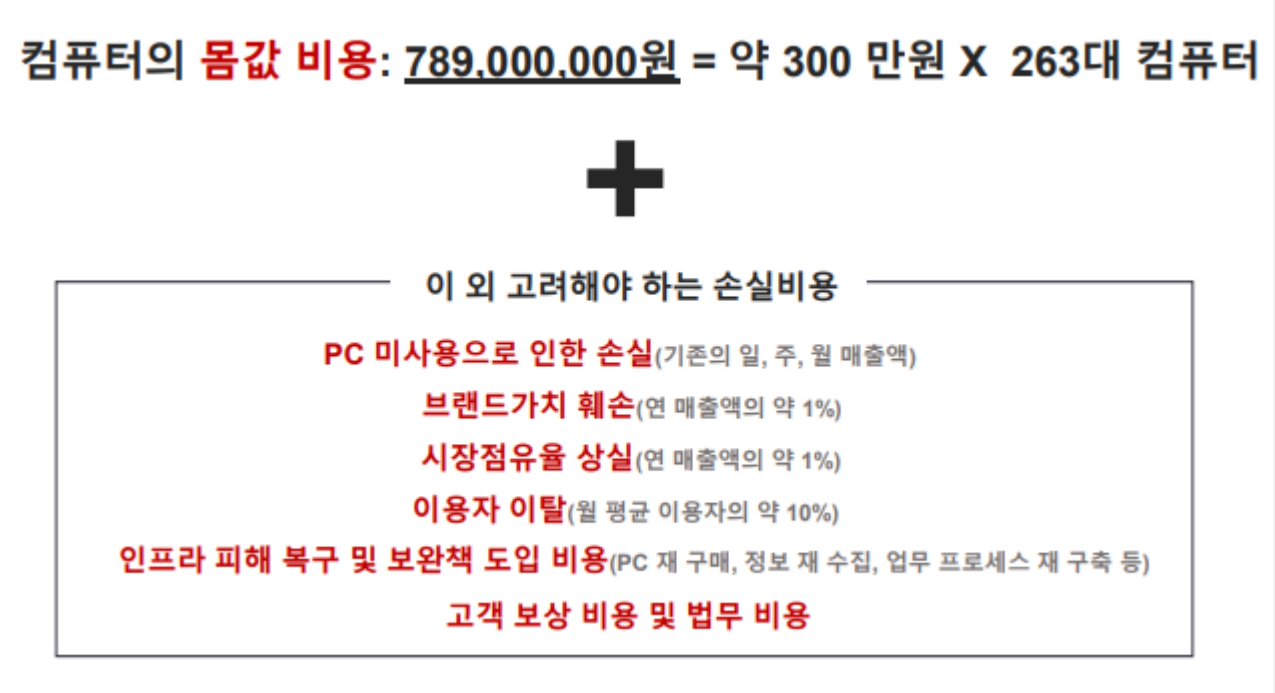
- 실제 예시



출처: 한국랜섬웨어침해대응센터

인간 요인 취약성

- 실제 예시



인간 요인 취약성

- 실제 예시
  - 랜섬웨어 주요 감염 경로

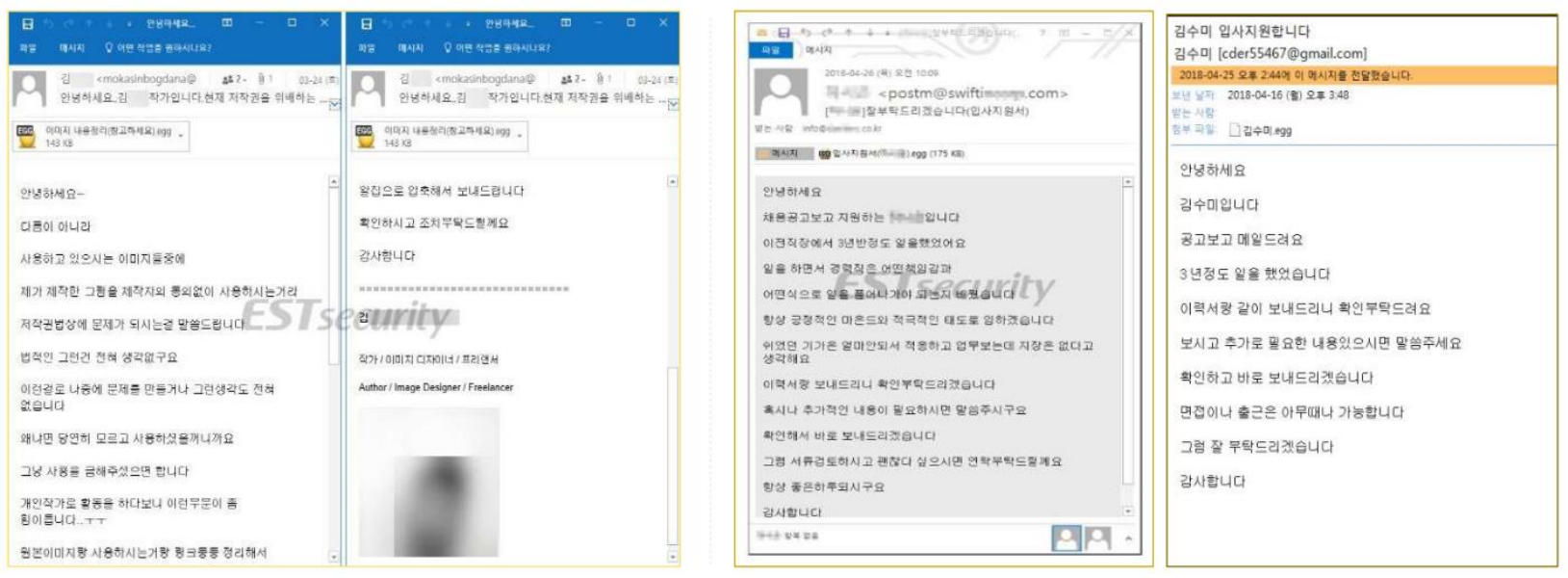
랜섬웨어 주요 감염 경로

랜섬웨어 주요 공격 방식

- 교통 범칙금 안내메일
- 입사 지원 메일
- 저작권 침해 공지 메일
- 소송 관련 메일
- 고객 VOC 메일
- 한진택배 배송관련 안내메일
- 견적서 요청메일
- 청와대 사칭메일
- 피고소환장 사칭 메일
- 세금납부 안내 및 채무 안내 사칭 메일

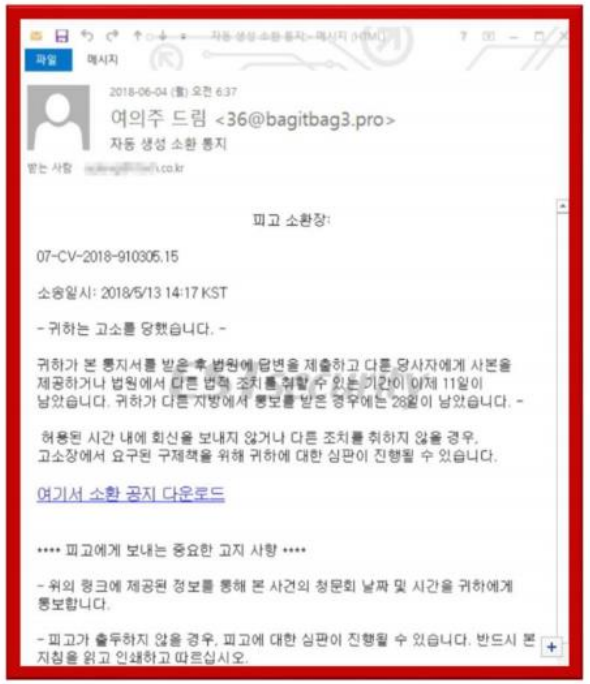
인간 요인 취약성

- 실제 예시
  - 랜섬웨어 주요 감염 경로 예



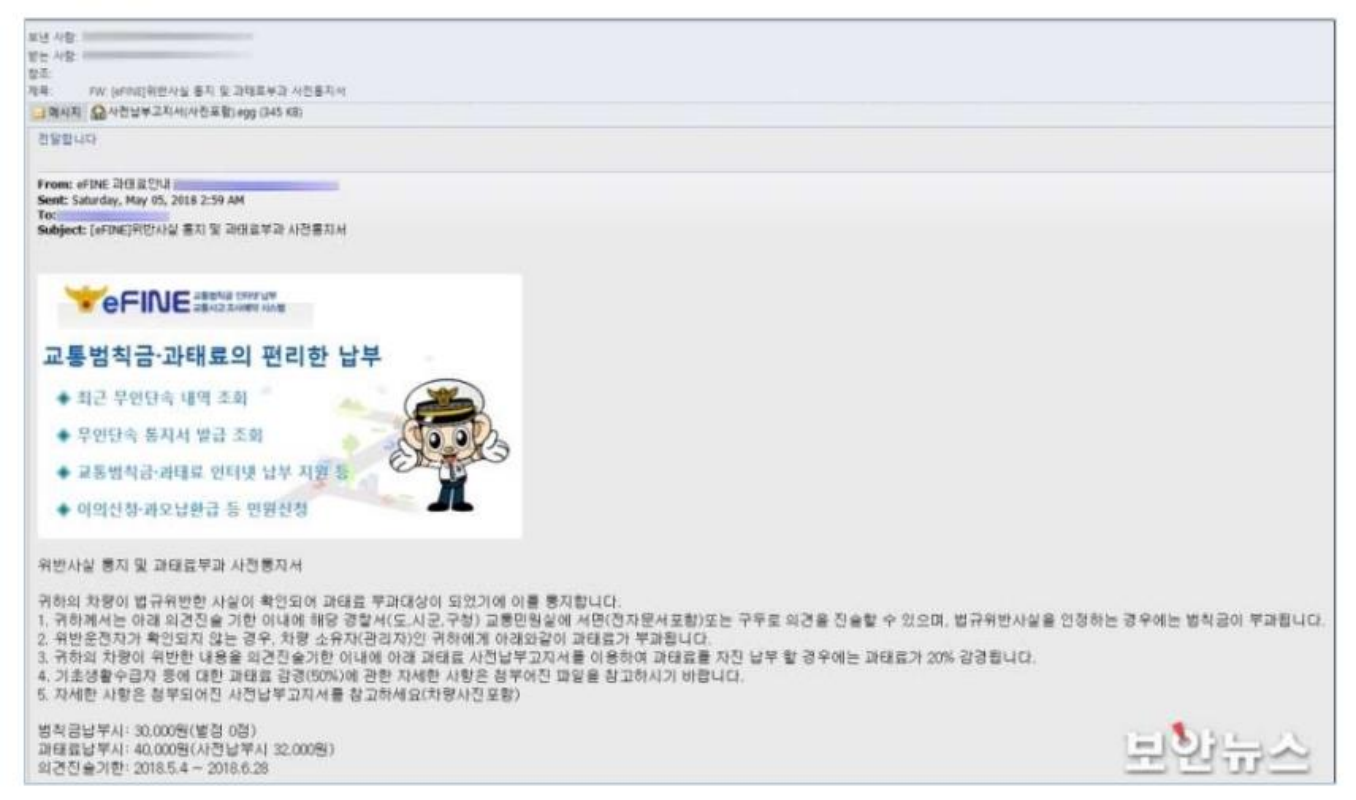
인간 요인 취약성

- 실제 예시
  - 랜섬웨어 주요 감염 경로 예



인간 요인 취약성

- 실제 예시
  - 랜섬웨어 주요 감염 경로 예

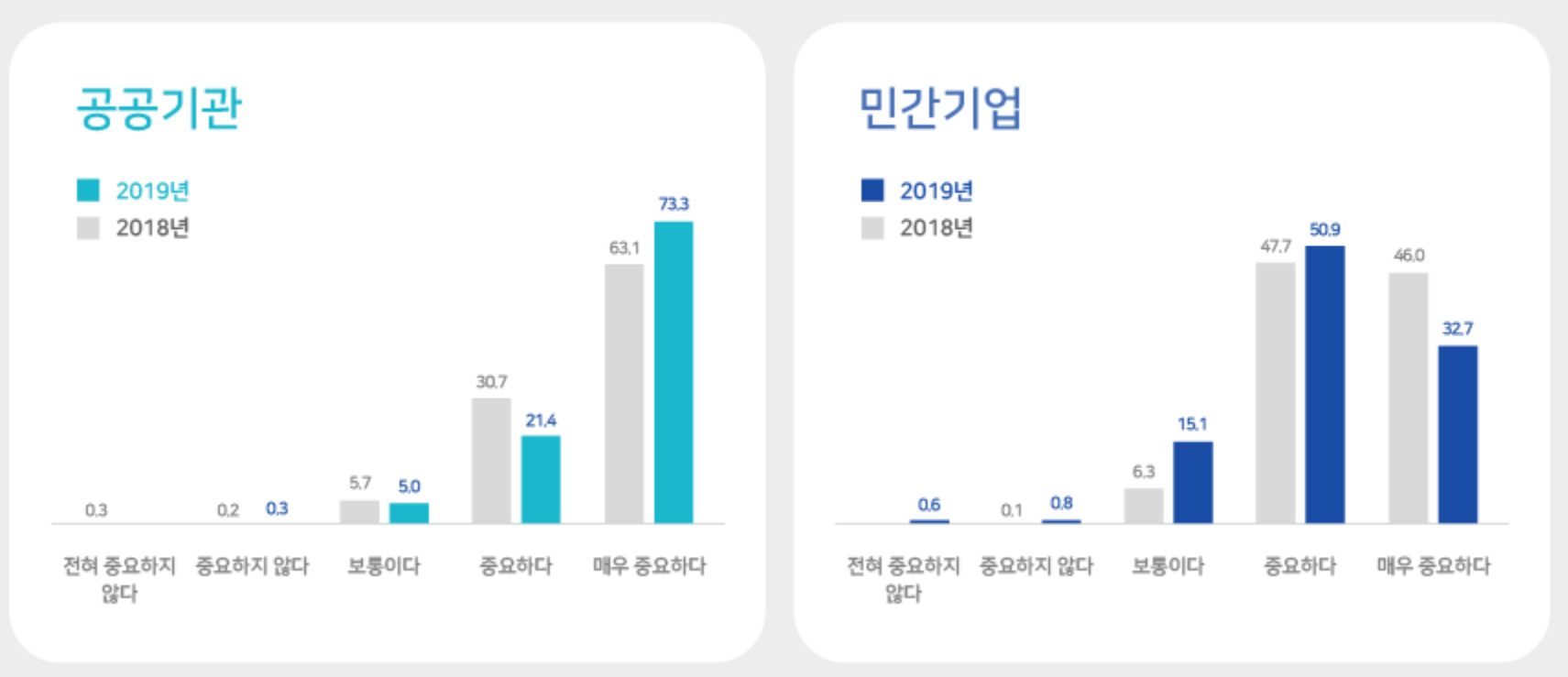


정보보호 인식의 중요성

- 용어
  - 인식(AWareness) : 사물을 분별하고 판단하여 앎
  - 정보보호 인식 (Information Security Awareness) : 정보보호를 분별하고 판단하여 앎
  - 의식(Consciousness) : 사회적.역사적으로 형성되는 사물이나 일에 대한 개인적.집단적 감정이나 견해.사상
  - 정보보호 의식(Information Security Consciousness) : 사회적.역사적으로 형성되는 정보보호에 대한 개인적.집단적 감정이나 사상

정보보호 인식의 중요성

- 정보보호 인식 현황

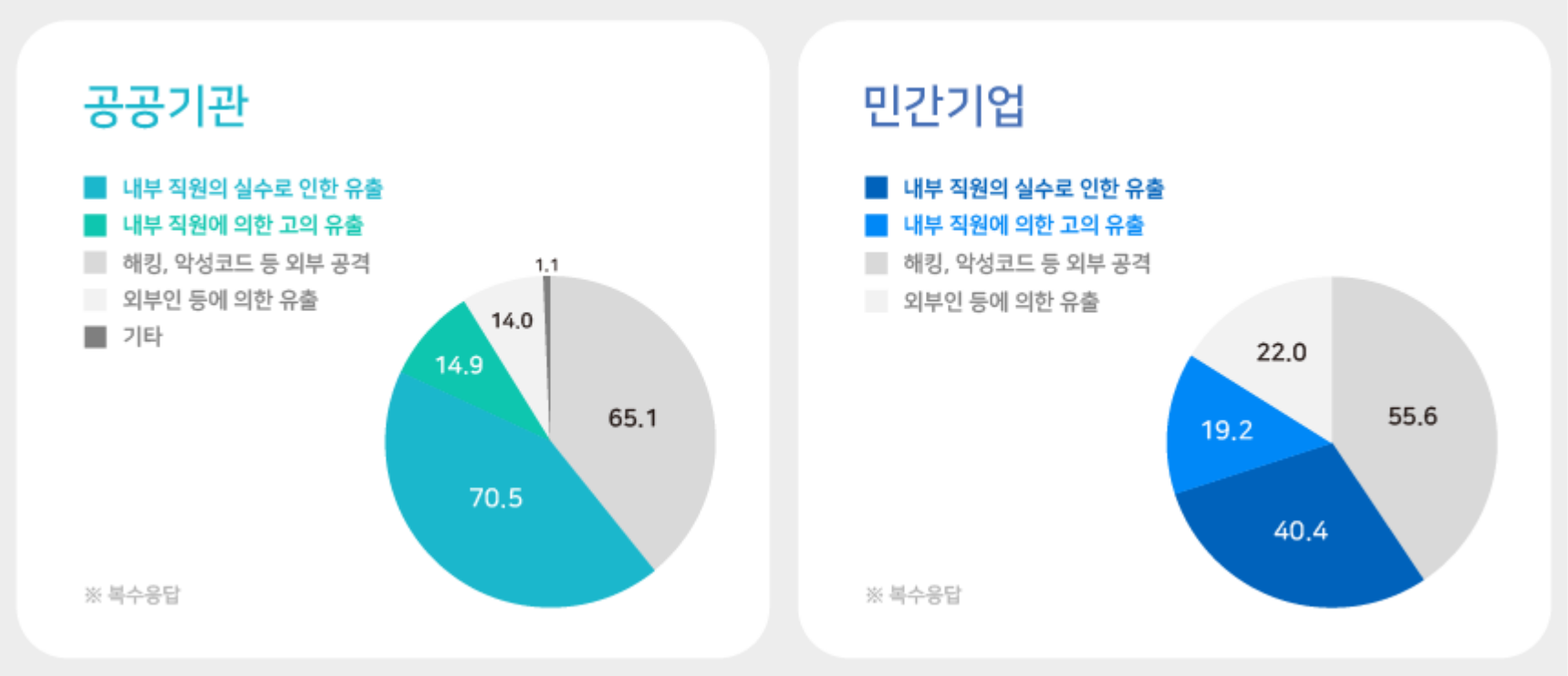


기업의 개인정보 보호에 대한 중요성은 공공기관이 94.7%, 민간기업이 83.6%로 모두 전년대비 높아졌음

최근 개인정보 보호 업규에 대한 규제와 처벌이 강화되고 있어 중요성에 대한 인식은 앞으로도 높아질 것으로 보임

정보보호 인식의 중요성

- 정보보호 인식 현황



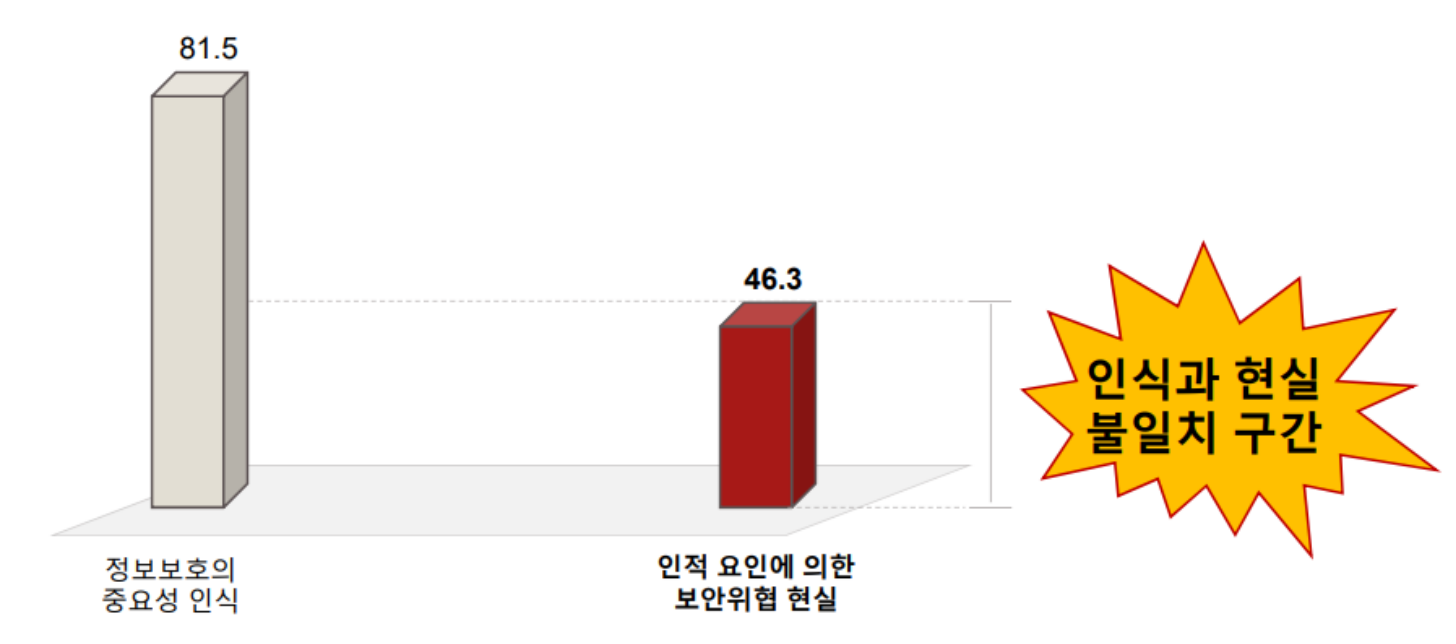
전체적으로 해킹.악성코드와 같은 외부 공격보다 사람에 의해 발생하는 인적 사고. 특히 실수나 악의적 행위 등 내부직원에 의한 개인정보 유출사고의 비중이 가장 높음

정보보호 인식의 중요성

- 정보보호 인식 현황
  - 가장 약한 연결고리 : 사람
    - 환경 , 위협 , 업무 , 이슈등 변화시 순식간에 가장 약한 고리로 변화

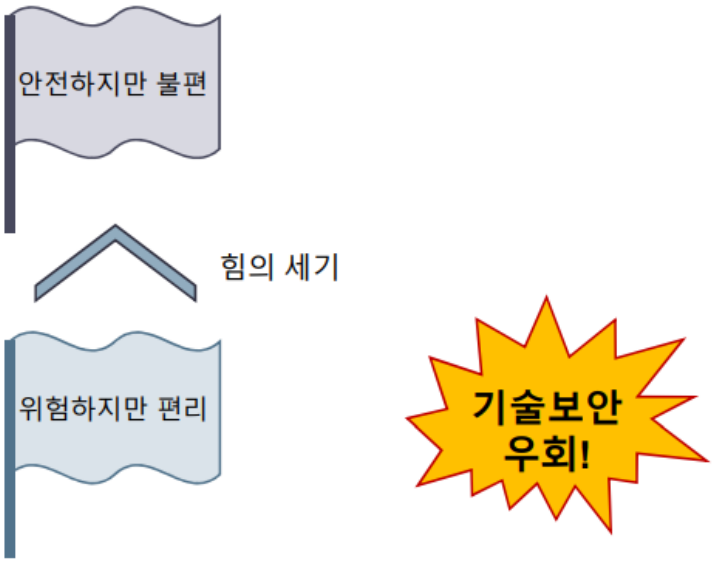
정보보호 인식의 중요성

- 정보보호 인식 현황
  - 아이러니한 현상
    - 인식과 현실의 차이 발생



정보보호 인식의 중요성

- 정보보호 인식 현황
  - 아이러니한 현상
    - 인식의 "쏠림"과 "우회" 현상 발생



정보보호 인식의 중요성

- 정보보호 인식 현황
  - 아이러니한 현상
    - "저항의 대상"이 되는 정보보안

(출처: 네이버 이미지)

'정보보안' 때문에 안 된답니다...

'일'을 하라는 거야? 말라는 거야?

정보보호 인식의 중요성

- 정보보호 인식제고 방안
  - 조직문화 이해
    - 동종업계 보안사고 인지 여부
    - 보안 대책 수립/적용 여부
  - 속도 조절
    - 팀플레이 – 정보보안은 담장자만의 의무가 아니라 모든 구성원들이 함께 지켜야 하는 ' 공동의 가치'
    - 소통 – 정보보안은 '분산화 된 책임'(새로운 보안 통제 전에는 반드시 소통)
    - 기다림의 미학 – 위험 상황이 아닌 한, 통제보다는 가이드 – 새로운 보안통제 적용 전 충분한 '수용의 시간'

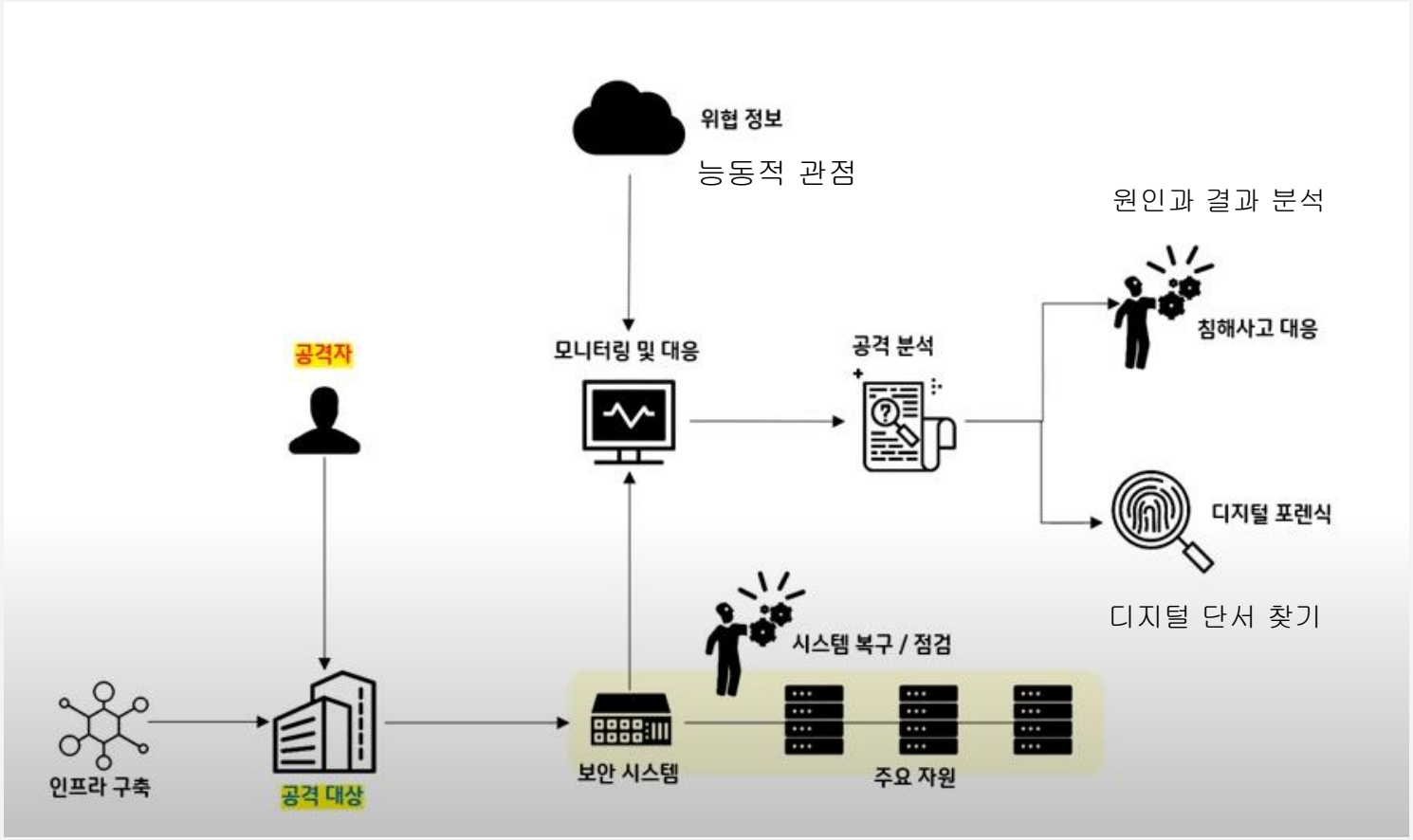
정보보호 인식의 중요성

- 정보보호 인식제고 방안
  - 현상이 아닌 원인에 집중
    - 나뭇가지가 아닌 바람 – 공격자는 우리를 연구합니다. 당신은 공격자를 연구하고 있습니까
    - 원인별로 다른 보안대책 – 안전함과 편리함 (관점이 다르면 결과도 정반대)
  - 정보보호 부서 고유의 업무
    - 사업적 수익을 방해하는 정보보안? – 조직의 안전을 주업무로 하는 유일한 부서
    - '정보보안'때문에 안 돼요? – 보안 법률 준수는 기업 생존의 필수 조건

정보보호 인식의 중요성

- 보안 문화 정착방안
  - 훈련/점검 결과는 보안인식의 새로운 기준
  - 가장 큰 저항을 하는 직원을 설득하면 가장 큰 조력자가 된다.
  - 보안이슈를 문의하는 직원은 이미 조력자
  - 측정할 수 있으면 관리할 수 있고 관리할 수 있으면 개선할 수 있다.
  - 보안문화 형성의 필수 자원은 객관적인 보안지표이다.

정보보안 기술 흐름



대부분의 정보보안 직무는 대부분 방어적,수동적인 관점의 업무가 대부분

정보보안 직무

- 보안개발 : 조직 내의 IT 자산을 효율적으로 지키기 위한 최소한의 방어 수단 구비
- 네트워크 관제 : 관문을 오가는 네트워크 통신에서 비정상적인 흐름을 빠르게 탐지 및 대응
- 악성코드 분석 : 내부에 유입된 악성코드의 유입경로와 수행 기능을 파악 후 대응 방안 마련
- 침해사고 분석 : 외부 공격으로 인해 내부 조직의 피해를 분석하고 대응하기 위한 조직
- 디지털 포렌식 : 악성코드 또는 보안 사고의 책임과 증거 수집을 위한 분석
- 위협 정보 수집 및 분석 : 정보를 능동적으로 수집, 분석 (Bigdata + Information + Security)

보안관련 오픈소스 SW

- GitHub에 800여 가지가 넘는 오픈소스 보안 프로젝트
- 종류
  - 침투 테스트 툴
  - 다단계 방어 툴
  - 네트워크 보안 모니터링
  - 사고 대응 및 포렌식 툴
  - 리서치 툴 및 취약점 스캐너

보안관련 오픈소스 SW

[표 1] 오픈소스 바이너리 분석 플랫폼

도구 명칭	사용언어	개발 국가	연 도
Ghidra	Java	미국	2019
B2R2	F#	대한민국	2019
Angr	Python	미국	2016
BAP	OCaml	미국	2011
BINSEC	OCaml	프랑스	2011
Insight	C++	프랑스	2012

〈자료〉 국제학술대회 및 논문지 저자 조사 및 편집

[표 2] 오픈소스 침투 테스트 도구

도구 명칭	주요 특징
칼리 리눅스 (Kali Linux)	공격에 최적화되어 있는 도구로 기본 운영체제로 사용하거나, 윈도 또는 OS X 상에서 가상시스템으로 사용
N맵 (Nmap)	20년 이상 운영된 대표적 포트스캐너로 자체 보안점검, 호스트 검색과 운영체제 탐지 등 다양한 기능을 제공
메타스플로잇 (Metasploit)	다양한 수작업을 자동화한 가장 널리 사용되는 침투 테스트 프레임워크
와이어샤크 (Wireshark)	네트워크 프로토콜 분석, 일반적인 TCP/IP 연결 조사, 프로토콜 분석 등을 지원
존더리퍼 (John the Ripper)	비밀번호 크래킹 도구, 오프라인 비밀번호 크래킹에 주로 사용
히드라 (Hydra)	SSH, IMAP 등과 같이 온라인 비밀번호 해독
제드어택프록시 (Zed Attack Proxy: ZAP)	OWASP에서 제공하며, 웹 사이트와 브라우저 사이에서 트래픽을 검사하고 수정하는 등의 기본 기능을 갖춘 도구
SQL맵 (SQLMap)	SQL 인젝션 결함 탐지 및 이를 이용한 데이터베이스 서버 연계 프로세스 자동화
에어크랙-ng (Aircrack-ng)	와이파이 안전도 검사 등 보안검사를 위한 도구

〈자료〉 국제학술대회 및 논문지 저자 조사 및 편집


Thank you