시급히 해결하여야 할

금융 정보보호

2016. 04. 05

전자금융사고

주요 해킹 및 전산망 사고 일지

2008년 1월	옥션 1,081만명 개인정보 유출
2009년 7월	청와대 등 정부기관 사이트 디도스 공격
2010년 6월	KB국민은행 전산망 마비. 인터넷뱅킹 등 일시정지
2011년 4월	농협중앙회 2일간 현금인출기, 인터넷뱅킹 중단
8월	네이트 · 싸이월드 개인정보 3,500만건 유출
11월	넥슨 메이플스토리 개인정보 1,320만건 유출
2012년 7월	KT 개인정보 870만건 유출
2013년 3월20일	방송사 및 금융권 전산망 마비

※ 출처: 금융감독원 IT.금융정보보호단

정보보호 사고 사례 분석

대 상	사고 개요	사고 원인
코웨이	내부직원 198만명 개인정보 유출(경쟁업체 유입)	내부직원 유출
국민연금	기금운영 대외비자료 유출(자산운용 회사 유입)	내부직원 유출
카페베네	홈페이지 해킹, 변조	외부 해킹
삼성카드 SK 하나카드	회사내 마케팅 직원에 의해 고객정보 유출	내부직원 유출
KT	개인정보 유출로 KT 주식 5% 급락 및 과징금 7억 5,300만원 부과	대리점.협력업체
조선일보	전산망 해킹(실패), 이메일 해킹 공격	기술적 공격
한국전력기술	퇴직자 2명에 의해 한국형 신형 경수로 설계 일부 유출	내부직원 유출
한화손해보험	자동차보험 현장출동지원 시스템 해킹, 15만여건 고객정보 유출, 16개월간 미신고·은폐	외부 해킹
메리츠화재	내부직원에 의한 16만여 보험가입 개인정보 유출	내부직원 유출
주요 정부, 언론 기관	청와대 홈페이지 및 주요 정부기관 사이버 공격	외부 해킹

IT 트랜드 전망

『 새로운 금융상품/여신거래에 대한 **컴플라이언스 준수 및 신속한 新기술 도입** 』

■ 기존 금융회사, **ICT업체 제휴**와 첨단기술 접목으로 **디지털 혁신의** 합류

■ 개인정보의 종류(바이오정보,위치정보 등) 및 양의 급격한 증가, 수집 채널의 다변화

※ 사물인터넷(IoT) : 사람,사물,공간,데이터 등 생활 속 사물들을 유무선 네트워크로 연결해 정보를 공유하는 환경

※ 바이오정보 : 지문·얼굴·홍채·정맥·음성·서명 등 개인을 식별 할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말하며, 가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함

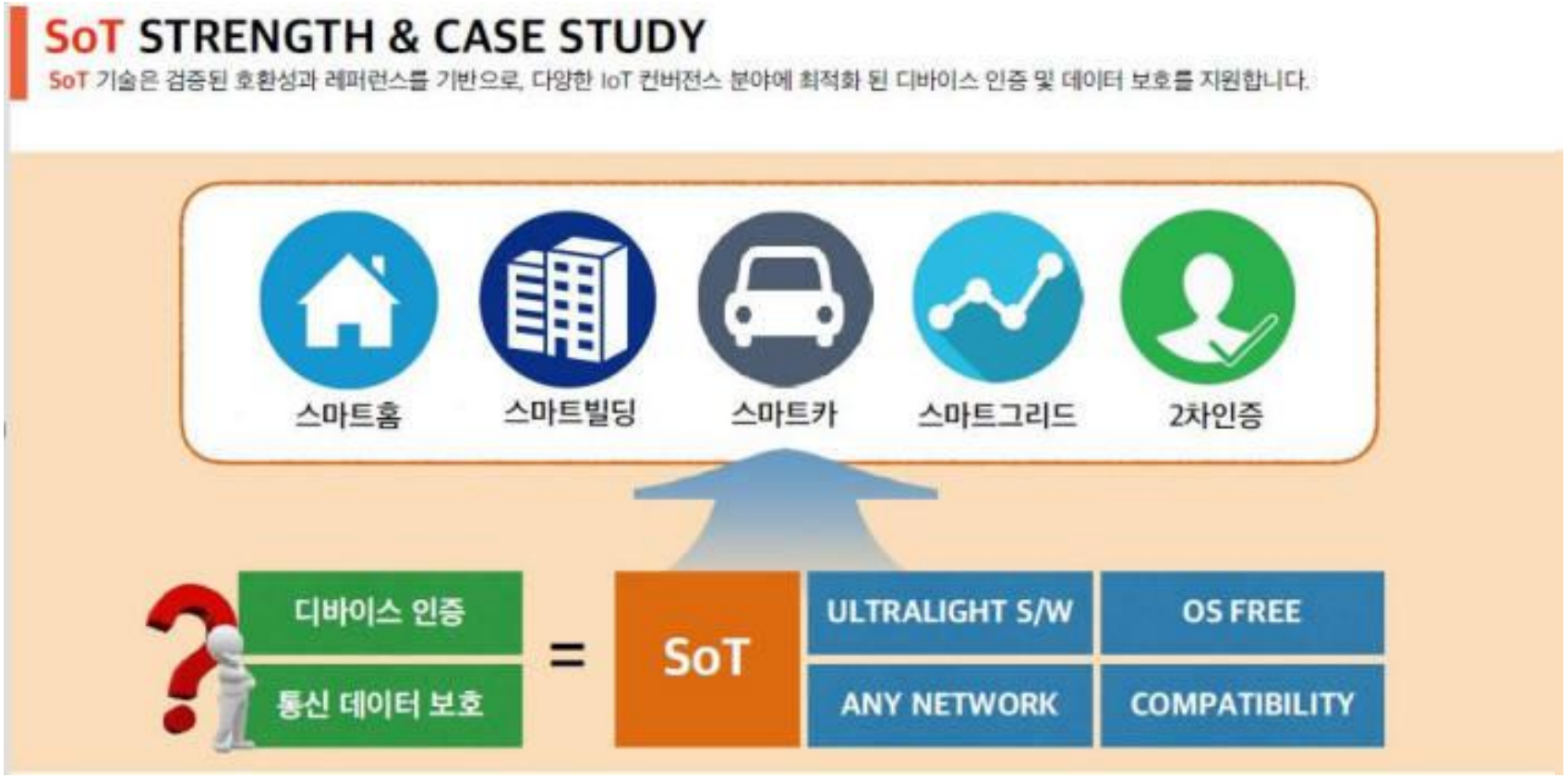
IcT 트랜드 – 순기능:역기능

드론

모바일

자율
자동차

IcT 트랜드 – 순기능:역기능



인식의 차이

정보보호에 대한 인식 부족으로 정보보호 분야의 투자 등이 저조하기 때문에 각종 규제를 통해 정보보호 강화를 의무화하는 추세

※ 기업의 인식(정보보호 지출을 하지 않는 이유)

순위	내용	비율
1	보안사고로 인한 피해가 없어서 필요성 없음	59.5%
2	정보보호에 관심 없음	23.4%
3	예산부족 (ROI 확보 미흡)	23.4%
4	정보보호에 관한 관심 부족	11.7%
5	이미 충분히 투자 했음	4.2%

※ 중복응답 포함

출처 : 한국정보보호진흥원(KISA) 정보보호실태조사

※ 정부 및 감독 기관의 정책

금융고객 정보유출 CEO 해임도 가능

금감원, 금융분야 개인정보보호 유의사항 마련

최대 5억 과징금 부과… 임직원 집중교육 실시

금융감독당국이 금융소비자의 개인정보보호 강화를 위해 금융회사들이 꼭 지켜야 할 유의사항을 마련했다. 실제 개인정보보호법 개정으로 내년 8월 7일부터 금융회사가 고객 주민번호 유출시 최대 5억원의 과징금이 부과된다.

또 최고경영자(CEO)에 대한 해임도 가능해진다. 금융감독원은 3일 '금융분야 개인정보보호 가이드라인'의 후속조치로 금융회사들이 개인정보 처리시 지켜야 할 유의사항을 마련, 금융회사 임직원을 대상으로 집중교육을 실시하기로 했다고 밝혔다.

금감원은 지난달 2일 개인정보의 안전성확보 조치에 대해 신용정보법과 전자금융거래법을 우선적용하고, 주민번호의 암호화는 개인정보보호법을 적용토록 하는 등을 골자로 한 금융분야 개인정보보호 가이드라인을 제정·발표했다.

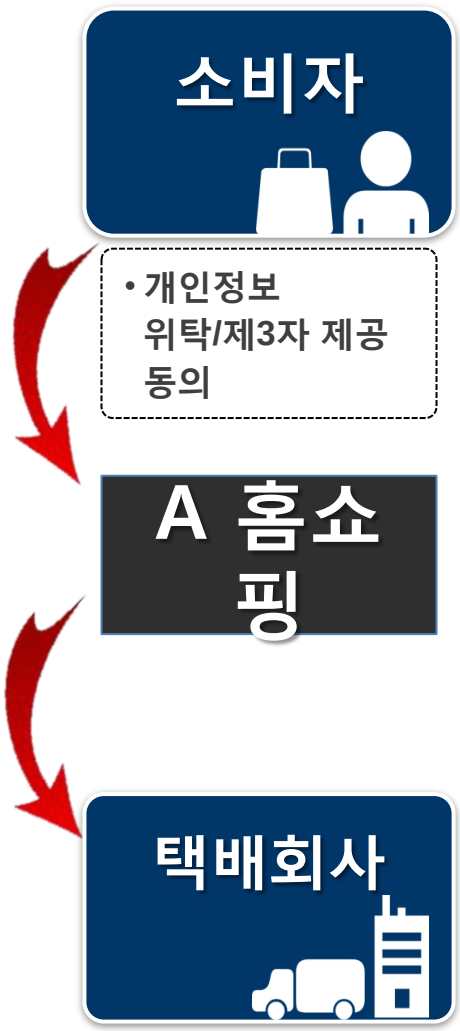
금감원 관계자는 "금융분야 개인정보보호 가이드라인이 제정된 지 한 달이 지났지만 금융회사들의 고객 개인정보보호 실태가 크게 나아지지 않은 데다, 개인정보보호법 등 개정 법률에 대한 이해도 크게 부족하다고 판단, 별도의 유의사항 마련했다"고 설명했다.

이번 유의사항은 ▲암호화 등 안전성 확보조치 마련 ▲개인정보보호법 개정에 따른 책임강화 ▲개인정보의 수집·이용·제공 등 처리 단계별 보호기준 준수 ▲개인정보 문서의 안전한 관리 ▲CCTV설치·운영 기준 준수 등 5개 항목으로 구성됐다.

금감원은 안전행정부의 지원을 받아 은행·증권·보험 등 금융권역별로 특성화된 교육을 실시할 예정이다. 특히 신협·대부업자 등을 대상으로 지방순회 교육을 실시하는 등 중소형 금융회사를 위한 교육지원을 확대할 계획이다.

교육과정은 이번에 마련한 유의사항을 전달하고, 가이드라인 및 실무사례를 설명하는 방식이다.

판례에 나타난 사고 사례



수원지방법원 2005. 7. 29. 선고 2005고합160 판결 (1)

- A회사는 택배회사와 **택배위수탁계약을 체결**하고 A회사로부터 위탁받은 택배화물을 고객들에게 운송하는 일을 담당한 택배회사 직원 B가 A회사가 관리하는 **개인정보를 유출**
- 양벌규정에 있어서 **법인의 사용인 그 밖의 종업원**에는 법인과 고용계약이 체결되어 근무하는 자 뿐만 아니라 **법인의 사업경영과정에 있어서 직접 또는 간접적으로 법인의 통제, 감독하에 그 사업에 종사하는 자도 포함**된다고 할 것
- A 회사가 B의 위반행위를 방지하기 위하여 당해 업무에 대하여 상당한 주의와 감독을 하였다고 보기 어려워 A 회사 역시 형사책임을 면할 수 없다고 판시

✓ **정보통신망법**

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제75조 위반

정보보호 분야의 변화

금감원의 감독 방향이 『신규 보안기술에 대한 제도마련, 상시 감시강화 등 사전규제에서 사후점검 및 책임강화 등 자율보안체계 확립』함에 따른 컴플라이언스 대응강화

정부의 대책 및 법령 시행에 따른 체계적인 대응

- 금융회사의 자율적 IT리스크 관리 및 보안체계 확립 도모
  → 전자금융감독규정 시행세칙 정비
- 주민번호 변경에 대비한 종합 대응방안 마련

보안 주요 영역별 전문화 및 분업화

- 간편결제, 생체인증 등에 적용되는 신규 인증기술
- IoT, Cloud, BigData, Mobile 트랜드에 따른 대응

자율보안/ 핀테크 역량 강화

- 비식별화를 통한 빅데이터 활용
- 수탁자의 개인정보 노출사고 재발방지 위한 위수탁 현황 점검
- 주민번호 암호화 작업을 기한 내 완료 독려(개인정보보호법)
  ※ 100만건 미만은 '17.1.1일, 100만건 이상은 '18.1.1한

개인정보 통합 관리

- IT실태평가를 위한 검사는 모두 "건전성 검사" 형태로 운영
- 상시감시 결과 취약 부문에 대한 기획/테마 검사
- 해외점포 정보유출 해킹 등에 대한 보안관리 실태 점검

해결과제 : 프레임워크 – People+Process+Production

IBM X-Force

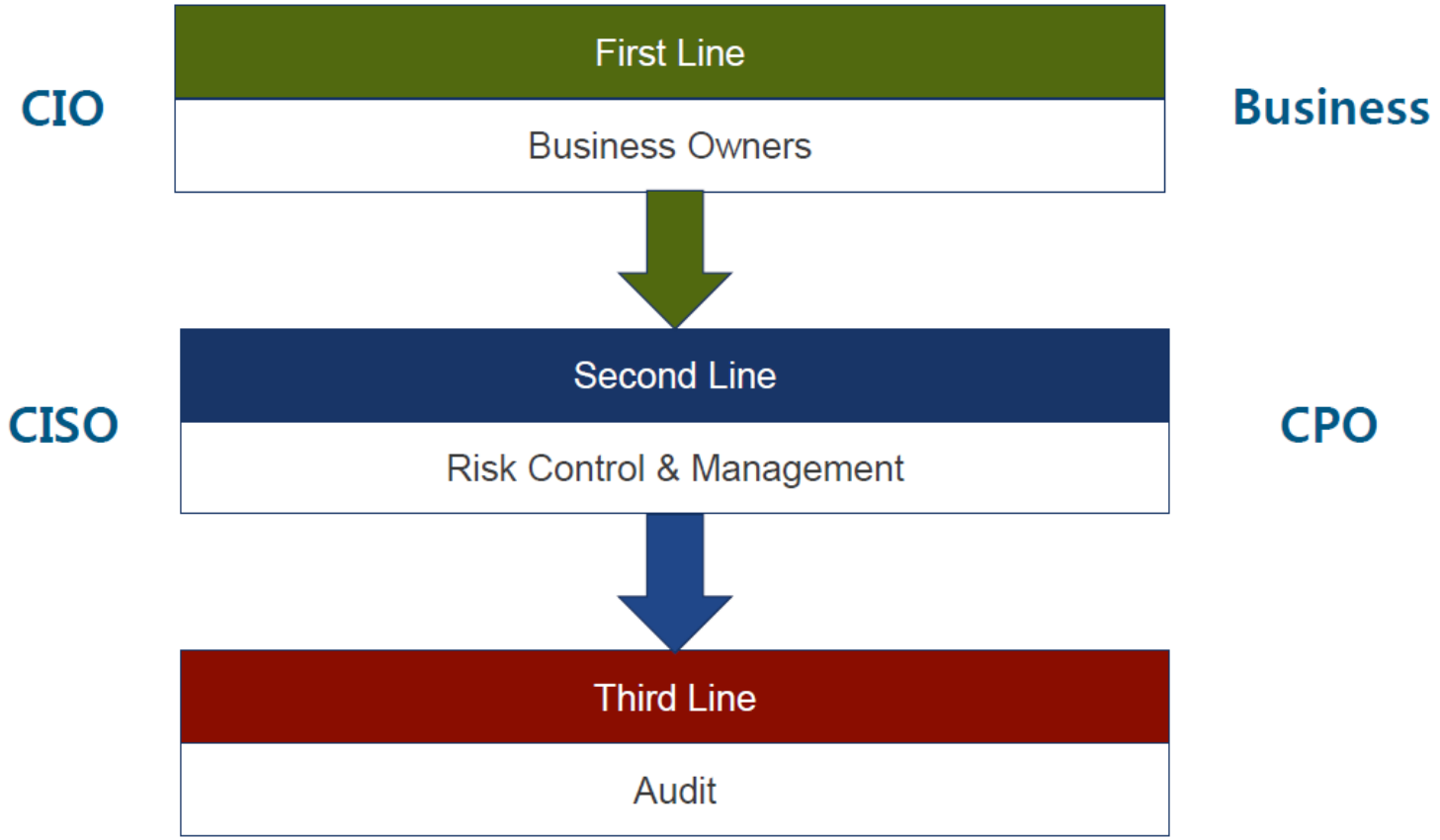
IBM의 보안 연구소이며 IBM Security Framework (보안 프레임워크)의 가장 중요한 기반이 되는 보안위협들에 대한 연구를 수행하는 조직

※ 출처: SC Bank, 김홍선 부행장

C-Level Resp.

CISO's Position – Three Lines of Defense

Standard Chartered



※ 출처: SC Bank, 김홍선 부행장

인식 vs 행동

내부자 위협으로 인한 위험의 이해 및 최소화

❖ **실제 행동 : 인터넷 안전교육을 제대로 실천되고 있는가?**

직원들이 본인의 행동으로 인해 자사를 사이버 공격의 위험에 빠뜨릴 수 있다는 사실을 잘 알고 있습니다.

73%

출처가 검증되지 않은 이메일을 여는 행동이 비즈니스 위험을 초래한다고 생각합니다.

65%

IT부서의 승인을 받지 않고 새로운 앱을 사용하는 행동이 심각한 위험이 된다는 사실을 알고 있습니다.

직원들은 언행일치를 보여주지 않고 여전히 위험한 행동을 마다하지 않습니다.

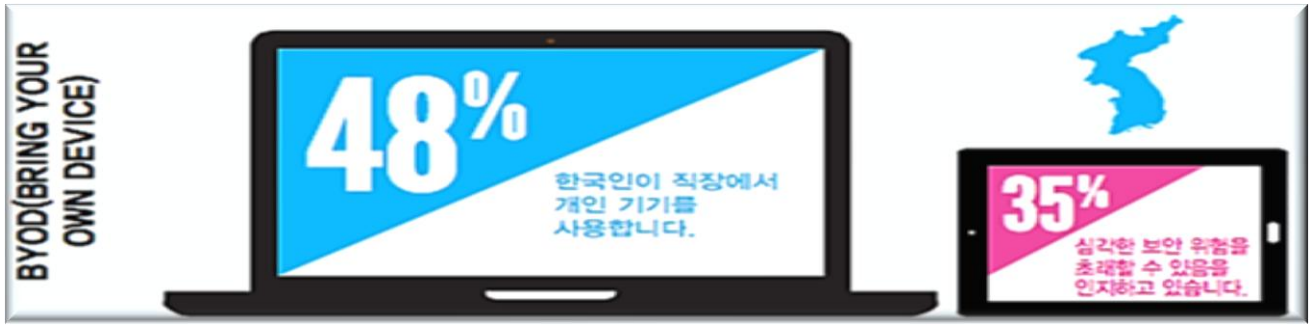
실제로 비즈니스 의사결정권자는 사이버 보안위험을 IT 의사결정권자에 비해 더 심각하게 받아들이고 위험한 행동을 저지르는 경우도 적습니다.

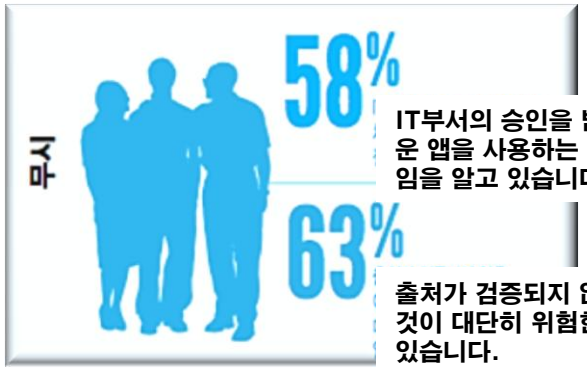
출처 : 블루코트코리아 15.6.23(TheBlue Coat Global Cyber Security Study 2014)

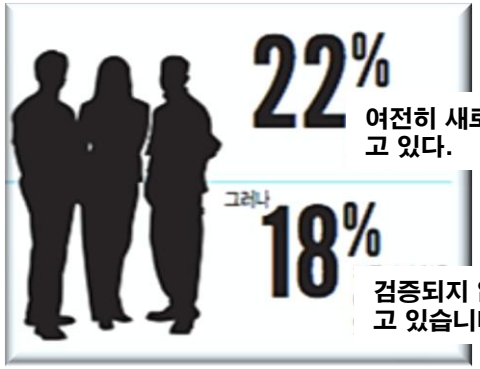
인식 vs 행동

내부자 위협으로 인한 위험의 이해 및 최소화

❖ 인식 VS. 행동 : 한국 사용자의 위험한 행동







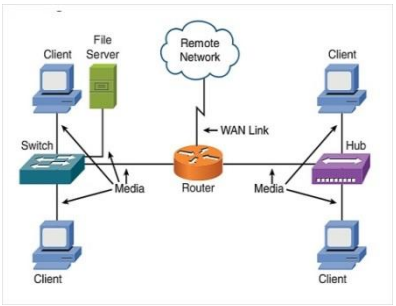
출처 : 블루코트코리아 15.6.23(TheBlue Coat Global Cyber Security Study 2014)

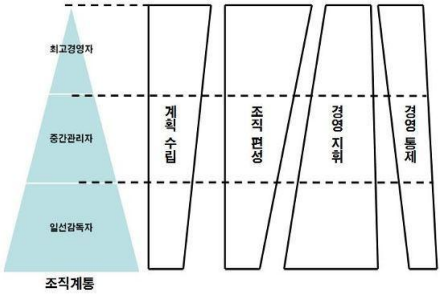
기업의 정보보호 관점

기업의 정보보호 활동이나 통제적 관점을 시간적 흐름에서 볼 때, 외부로부터 침입을 방지하기 위한 네트워크 통제로 시작하여, 내부망에 대한 인원 및 자산에 대한 통제, 향후로는 모바일 및 외부적 관점의 통제로 관점을 확산하여야 한다.

Company

Time





외부망 보안, 해킹방어

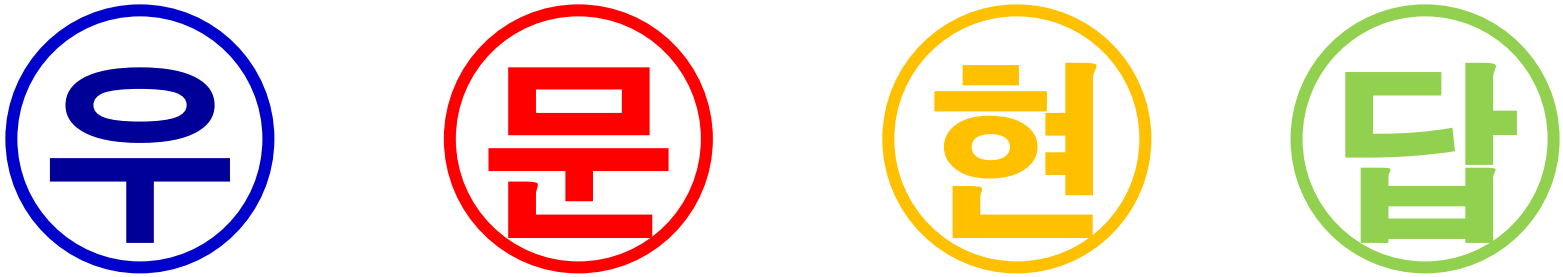
내부 인원,자산 통제

외부 인원 및 자산통제

모바일 통제

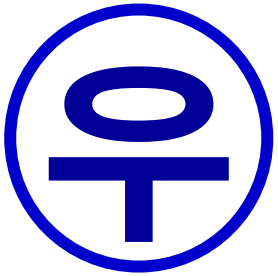
사자성어 원래의 뜻은,
어리석은 질문에 대한 현명한 대답

愚 問 賢 答



우리의 문제는 현장에 답이 있다.

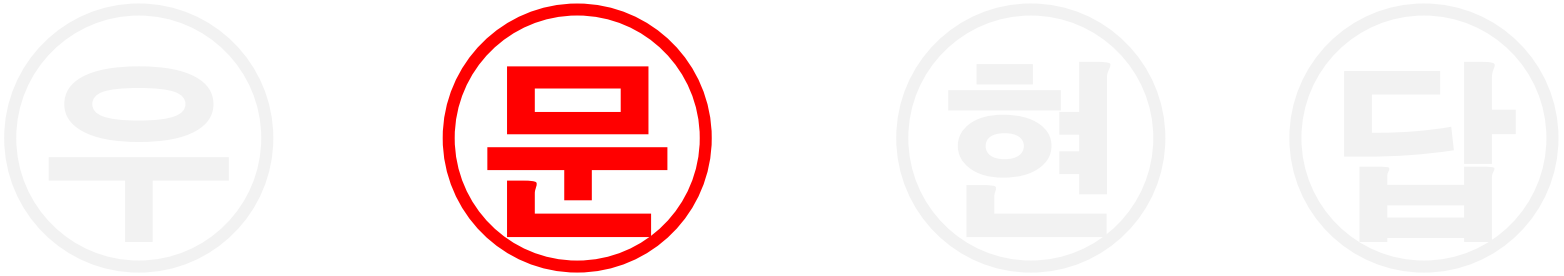
우리 기업(조직)은...



- 우리 조직의 정보보호 범위는 어디까지 일까?
- 어느 수준까지 정보보호(개인정보보호) 대응을 하여야 하는 걸까?
- 우리조직의 정보보호 Issue는 어떤 것들이 있을까?
- CEO, CIO 및 他 임원들과 CISO와의 관계는 우리 조직의 정보보호 수준을 높이는 데 매우 잘 소통하는가?

※ CISO (Chief Information Security Officer)

정보보호 문제(Issue)는...



- 우리 조직의 정보보호 Issue는...
  - ✓ 어떤 것들이 있을까?
  - ✓ 누가 앞장서 해결하여야 하는 걸까?
- 정보보호 인력, 투자를 비용으로 여기시나요?
- 정말로, 정보보호와 편리성, 효율성 등은 반비례하는가?
- 우리 조직은 보안성 검토를 위한 인력, 장비 등 준비를 갖추고 있을까요?

현장이 중요하다...

- **현장의 소리**를 직접 가서 듣고, 정보보호 이슈를 적어 보았는가?

  - 보고만 받고, 챙긴 적이 없다면, 현장은 정보보호가 되고 있을까?

  - 현장은,

    ✓ 고객접점
    ✓ 외부업체 직원
    ✓ 위수탁업체 임직원
    ✓ 외부 프로젝트 개발인력
    ✓ 고객

답을 찾아서...

- 그럼 무엇을 하여야 하는 걸까?
- 어떻게 하여야 하는 것일까?
- 정보보호는 매년 투자를 다시 해야 하는 것인가?
- 모든 임직원이 정보보호에 대해 본인의 일처럼 책임감을 가지고 일하고 있을까?

  - 마케팅, 리스크 분석, 개발, 현업 비즈니스, 홍보, 총무, 인사, 재무 등등
- 조직의 컴플라이언스 준수는 어느 조직이 맡아야 하는 것인가?

IoT 에 따른 보안대책

핀테크, 빅데이터, 생체인증, 온/오프라인 연결서비스 등 급속히 발전/변화하는 차세대 기술에 비례하여 보안위협의 다양성 증가에 대비하여야 한다.

핀 테 크

- 유형 : 지급결제, 금융데이터 분석, 금융소프트웨어, 플렛폼
- 인터넷 전문 은행 핀테크 활성화
- 금융기관 없이 자유로운 금융거래 가능한 플랫폼 마련

빅 데 이 터

- 정부차원 빅데이터 활성화와 융합신기술 사업 창출 도모
- 빅데이터 시범사업

생 체 인 증

- 모바일 기기에 생체인식 모듈 탑재 경향
- 생체인증 표준개발 컨소시엄(FIDO)에서 표준화 작업
- 홍채와 정맥으로 생체인증 확대

온/오프라인 연결 서비스

- 스마트폰앱 중심 온라인과 오프라인 연결서비스 다양화
- 근거리 무선통신 기술 NFC 이용서비스
- 태블릿 브린치, 옴니채널 등 채널 간 융합 서비스 및 스마트 워크 환경 강화

최고경영진의 3가지 제언

사이버 보안 역량을 강화하려는 최고경영진을 위한 3가지 제언

1. 위험에 대한 이해
2. 협업, 교육, 역량 강화
3. 경계심을 갖고 신속하게 위험 관리

※ 출처: IBM CISO Forum

급변하는 패러다임...어디로?

뭔가 중요한 것들이 이동하고 있다!

1. *Hardware보다 Software가 더 중요해진다.*
2. *Embedded보다 Cloud가 더 중요해진다.*
3. *제품자체보다 서비스가 더 중요해진다.*

감사합니다.

롯데카드(주)

최 동 근 상무 / 정보보호부문장, CISO

LOTTE CARD