온라인으로 함께 하는
제6회 IBM Security Summit

코로나19 그 후:
뉴 노멀 시대의 보안 트렌드 및 전략

김정덕 교수
중앙대학교 산업보안학과
일반대학원 융합보안학과
보안대학원 금융보안트랙

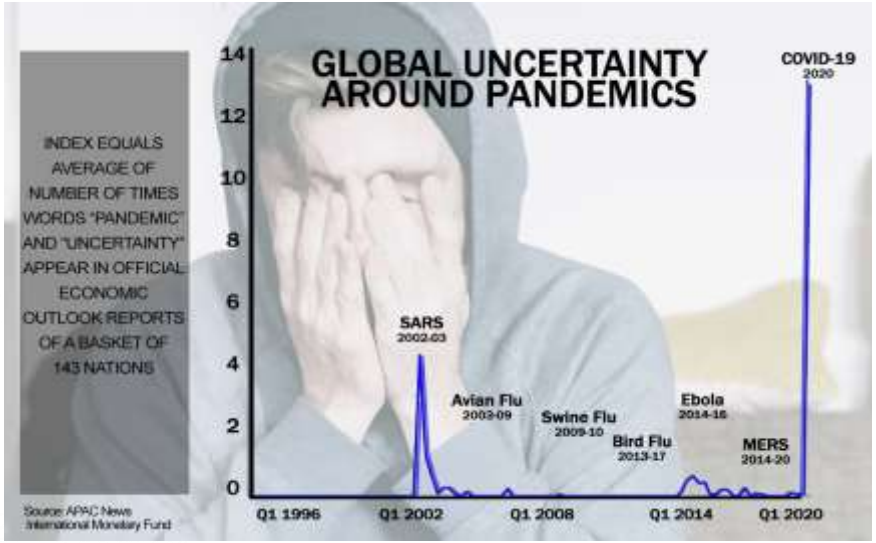
IBM

Agenda

- 포스트 COVID-19 시나리오
- 뉴 노멀 시대에서의 보안 트랜드 및 요구사항 변화
- 뉴 노멀 시대에서의 보안 전략

COVID-19 영향 – 불확실성

불확실성
1.향후 권력 구조
2.기술과 데이터의 미래 역할
3.대응 전략



There has never been so much awareness of our ignorance and of the necessity to have to act and to have to live under conditions of uncertainty

Jurgen Habermas

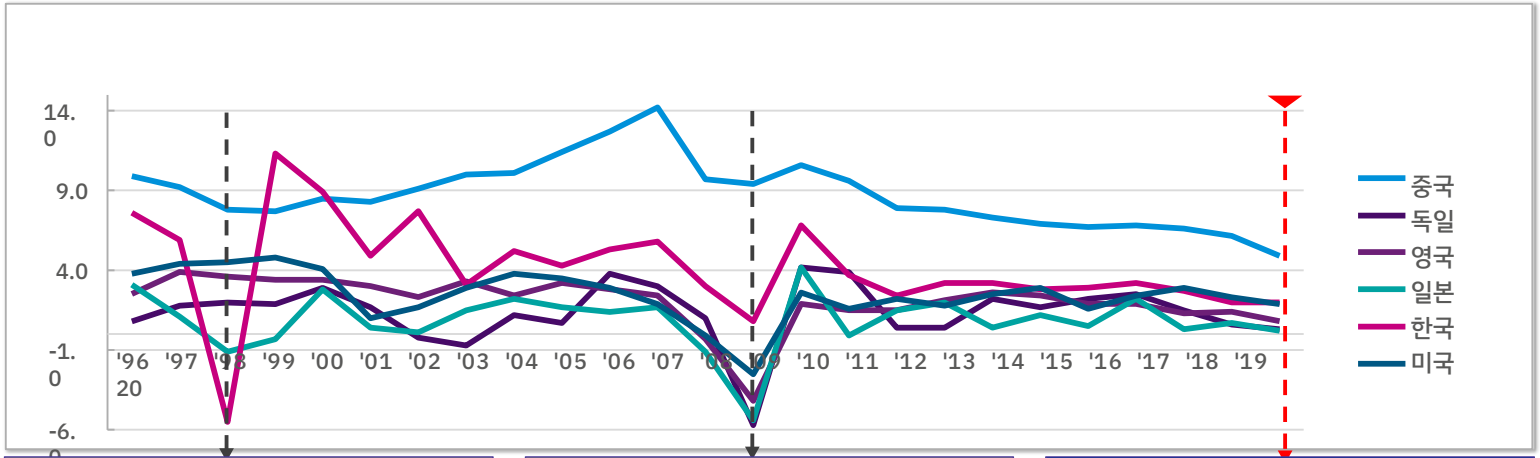
우리의 무지에 대해서 그리고 우리가 불확실성 하에서 행동하고 살아야만 한다는 것에 대해서 이토록 뼈저리게 인식한 적은 이제껏 없었다는 사실뿐

위르겐 하버마스

COVID-19 영향 – 글로벌 경제위기

현재 글로벌 동시다발적인 코로나19의 확산은 글로벌 공급망과 실물경제에 영향을 주는 수요 및 공급 충격으로 글로벌 경제 위기에 대한 불안 고조

과거 20년 주요국 경제성장률 및 금융위기 원인과 양상



'98년 아시아 외환위기

- 우리나라를 포함한 동아시아의 급격한 자본 유출과 외화 유동성 부족
- 기업 및 금융기관의 리스크 관리 미흡으로 기업 연쇄부도에 따른 신용경색

'태국 → 동아시아로 국지적으로 위기 전이

'08년 글로벌 금융위기

- 선진국 자산(부동산) 버블의 붕괴, 증권화 금융상품의 손실 확대와 확산
- 은행 연쇄도산과 신용경색

'선진국 → 전 세계로 금융위기 전이

'20년 코로나19 팬데믹

- 주요국으로의 전염병 급속한 확산과 감염 확산 방지를 위한 봉쇄·폐쇄 조치
- 글로벌 공급망 훼손, 원유가 폭락, 기업 경제활동 마비 및 소비의 급격한 감소

코로나19 팬데믹으로 인한 경제 하방 위험 증가 및 글로벌 경제위기 발발 가능성 증대

출처: World Bank, 삼정KPMG 경제연구원

COVID-19 영향 – 디지털 경제 가속화

Who led the digital transformation of your company?

A) CEO

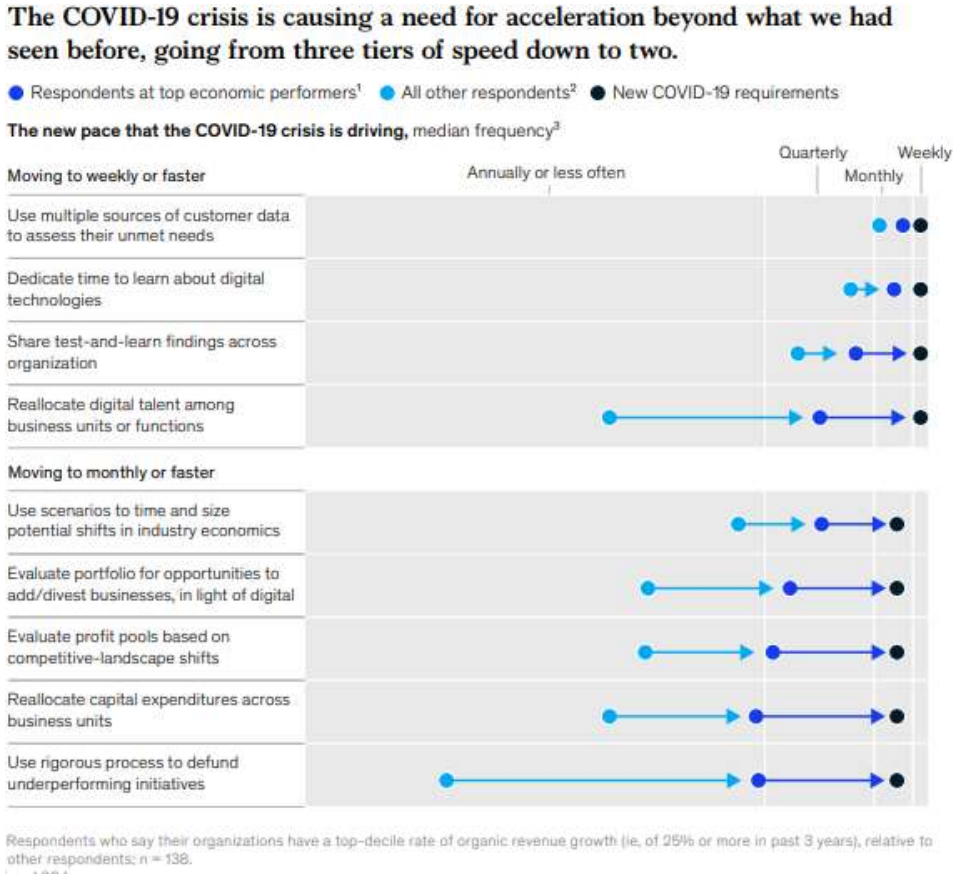
B) CTO

C) COVID-19

가장 큰 변화를 일으키는 섹터

1. Telecommuting
2. On-demand food and services
3. Virtual event
4. Cloud

- Forbes, Apr. 5, 2020



기업의 당면 과제는 Resilience

코로나19는 재무, 고객 수요, 공급망 등 기업의 일상적 비즈니스의 모든 측면에 영향을 미치고 있으며 Resilience 역량을 제고할 필요성 대두

Source: KPMG Global, 삼정KPMG 경제연구원

뉴 노멀 시대에서의 보안 트랜드 및 요구사항 변화

팬데믹을 통한 사이버 보안 교훈

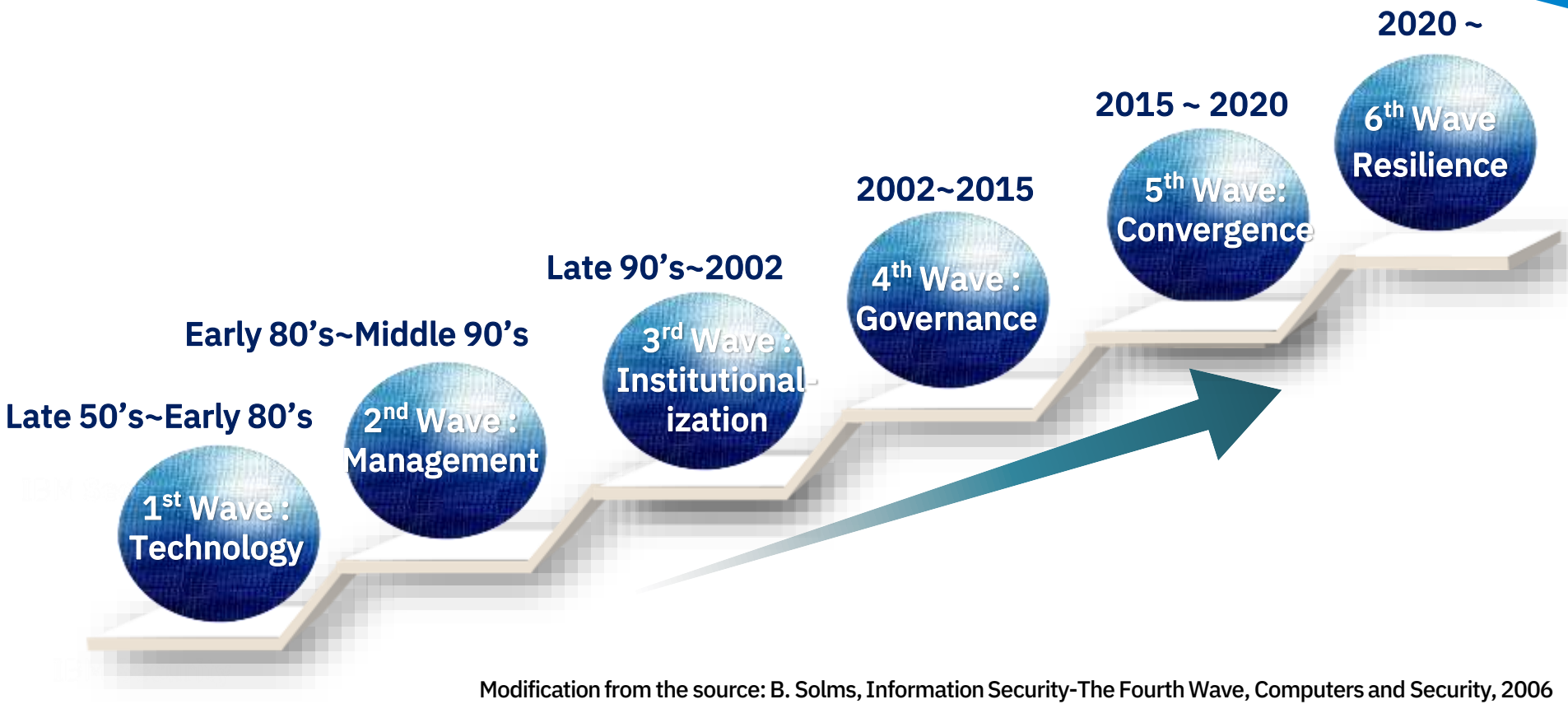
An article in Dark Reading titled 4 Cybersecurity Lessons from the Pandemic, Dr. Mike Lloyd, an epidemiologist-turned-CTO

- 전염/이동경로 이해
  - 초연결사회, 내부망 이동공격(lateral movement)
  - 조직 생태계 전반의 디지털 자산(클라우드, 원격근무)에 대한 가시성 확보

- 위협 정보공유와 위험관리 필요
  - 재택/원격근무, 비대면 거래 확대 등 디지털 위협요소(Attack surface) 확대
  - 최소 1개의 악성코드 가질 확률이 3.5배 증가, 최소 5개의 악성코드 가질 확률이 7.5배 증가_BitSight, 2020.4.14

- 사이버물리공간 청정화
  - 기본 보안면역 역량 확보 노력
  - Back to the Basics

보안 패러다임의 변화



Modification from the source: B. Solms, Information Security-The Fourth Wave, Computers and Security, 2006

뉴 노멀 시대에서의 보안 가치 변화

미래산업융합환경에서의 보안 가치는 조직내 중요 자산보호라는 전통적 보안가치 외에 안전한 디지털 제품/서비스를 제공함으로써 경쟁력 제고를 가능하게 할 수 있는 차별화 가치를 포함

Asset Protection

중요 산업 자산 보호

- 기술, 정보, HR, 설비 등
- 외부 사이버/물리 공격
- 자연재해
- 내부 유출
- 임직원 실수

정보/시스템 등 ICT 자산의 기밀성, 무결성, 가용성 보장

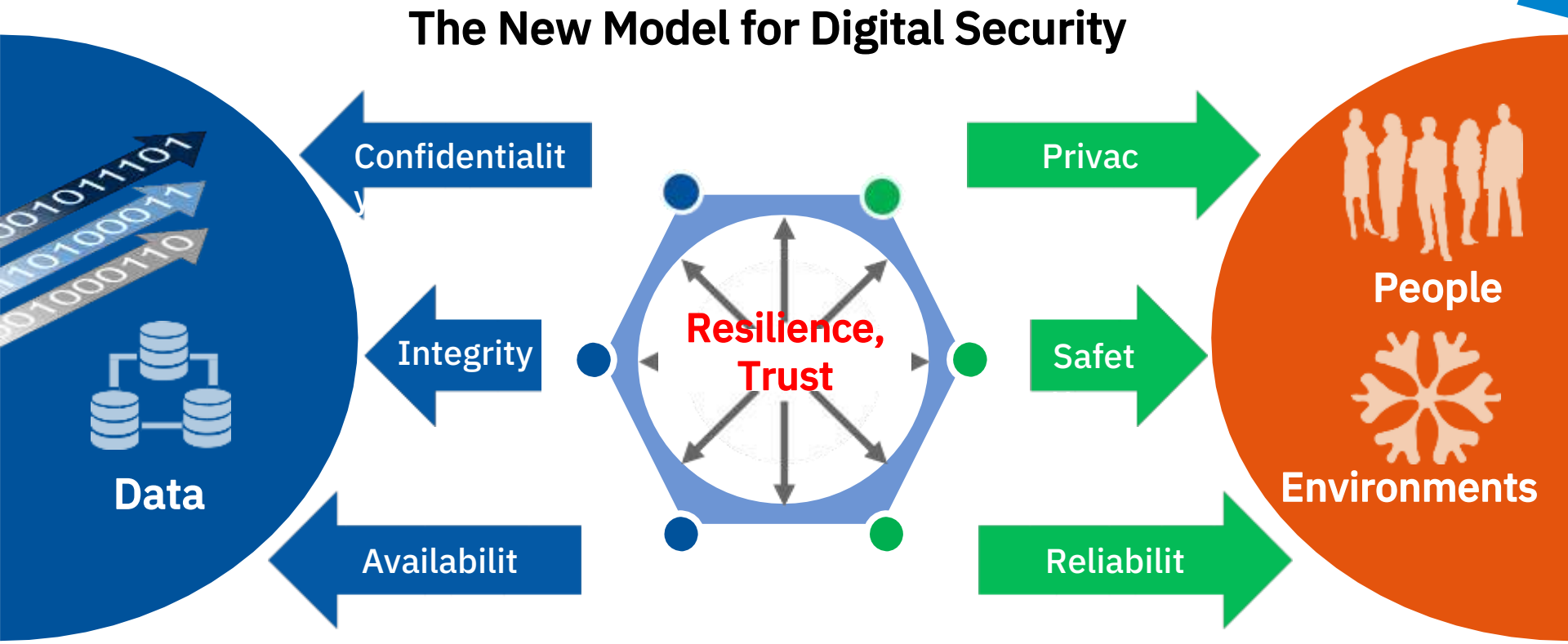
Value Differentiator/ Business Enabler

안전한 디지털 제품/서비스 제공

- 안전한 자율주행차 개발
- 안전한 의료서비스 제공
- 프라이버시 보호
- Trust 기반 고객 경험

인간, 환경 포함 안전 및 신뢰성 보장

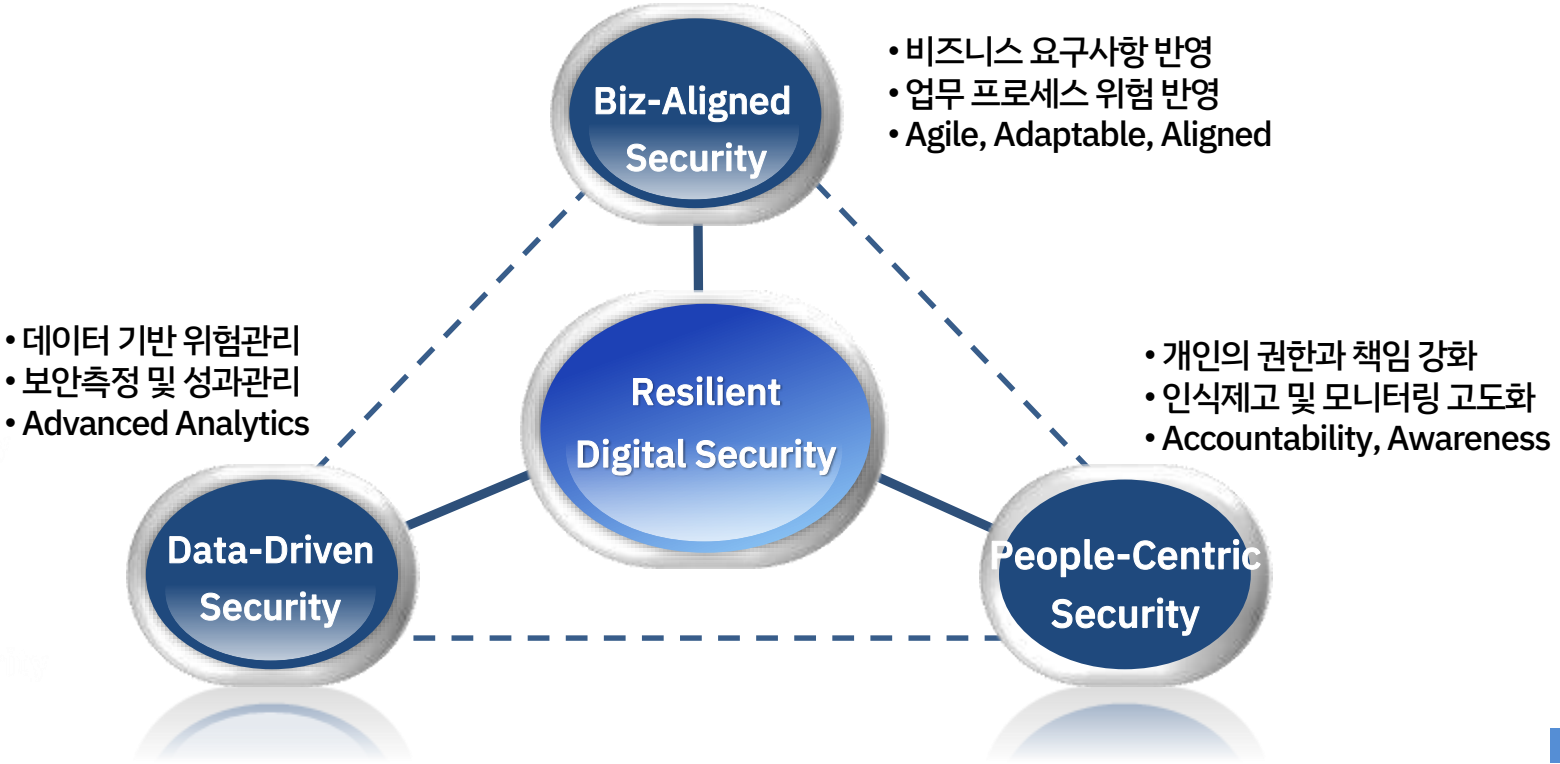
뉴 노멀 시대를 위한 새로운 보안 요구사항



뉴 노멀 시대의 보안 전략 및 과제

뉴 노멀 시대에서의 보안 전략

디지털 전환의 가속화로 인해 보안위험이 다양해지고 고도화됨에 따라 업종의 특성을 고려하면서 위험관리 기반의 자율적 보안을 추구하는 **면역 회복력(Resilience)을 갖춘 디지털 보안체계**를 구축해야 함



1. 왜 비즈니스 연계 보안인가

❖ 보안의 실존적 가치 재조명

- ➢ 보안은 보안을 위해 존재하는 것이 아니라 조직의 비즈니스를 위해 존재
- ➢ 비즈니스 Enabler, Differentiator로서의 역할 변화 필요
- ➢ 그들만의 리그 함정에서 벗어나야

❖ 환경 변화로 인한 새로운 보안 **접근방법** 필요

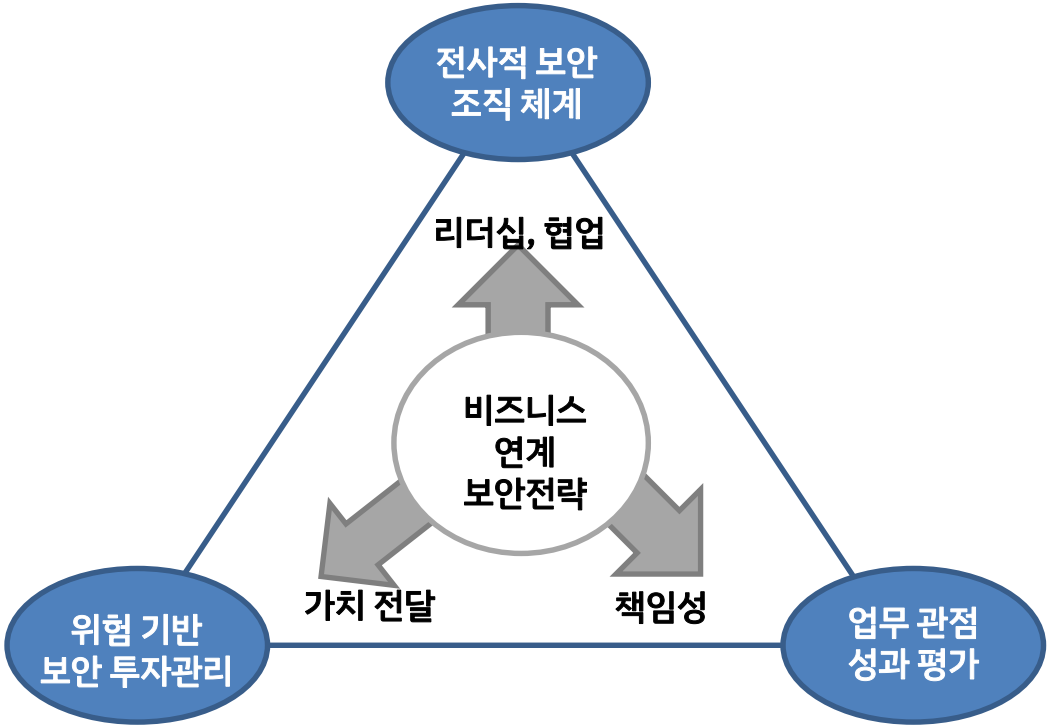
- ➢ 디지털 비즈니스의 확대
- ➢ 보안사고로 인한 경제적, 법적 피해 규모 증가, 최고경영층의 사퇴 등
- ➢ 비즈니스 적 이슈로의 관점 변화

❖ 비즈니스 성과와 연계된 **보안 활동** 필요

- ➢ 비즈니스 측면의 보안 가치에 대한 부재
- ➢ 보안투자를 이끌어내기 어려움
- ➢ 보안성과가 비즈니스에 어떤 영향을 주는지 분석 필요

1. 왜 비즈니스 연계 보안인가

전사적 보안을 위한 전략과 조직체계를 수립하고, 위험관리 기반의 투자활동이 수행되고 이를 비즈니스 관점에서 성과 평가하는 선순환 활동이 수행되어야 함



1. 어떻게 비즈니스 연계 보안을 구축하나

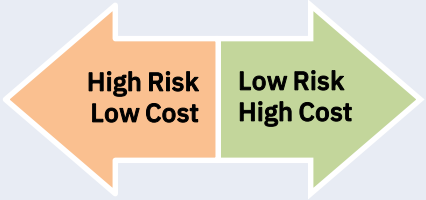
비즈니스 연계 보안을 구현하기 위해서는 조직에 적절한 보안 거버넌스 체계 구축 필요

비즈니스 연계 보안전략 및 조직

- 조직 대내외 환경 이해, 이해관계자 요구사항과 고객의 경험에 대한 분석
- 비즈니스 전략과 보안전략과의 연계
- 전사적 협업을 위한 보안 거버넌스 체계 구축 필요

위험기반 자원 할당 및 관리

- 보안은 비용 관점이 아닌 투자 관점으로의 변화 필요
- 컴플라이언스는 보안이 아니고 여러 위험 중 하나
- 위험관리 기반으로 투자 운선순위 결정 및 자원할당



비즈니스 관점 보안성과 관리

- 보안활동의 동기부여를 위해 비즈니스 관점에서의 성과평가 기준 개발 및 관리
- 보안활동의 효과성/효율성 뿐만 아니라 비즈니스 영향 측정과 성과관리에 반영
- 보안 위험을 조직 성과에 직접 결합하는 위험연계 가치관리(Risk-Adjusted Value Management, RVM) 방법론 접목

2. 왜 데이터 기반 보안인가

❖ 이벤트 기반 보안 솔루션의 한계

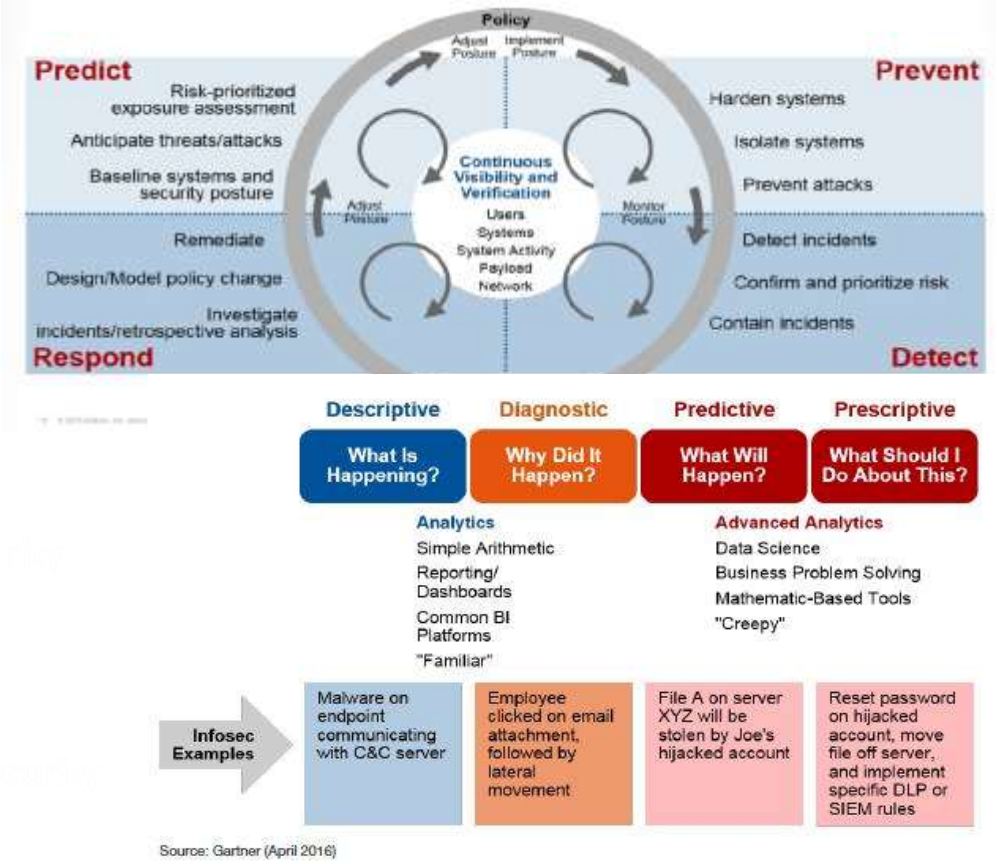
- 대응적인 활동에는 효과적이나 사전적 활동에는 한계 존재
- 다양한 보안 데이터 수집 및 분석과 보안프로세스의 자동화 필요
- 단순 관제(monitor)가 아닌 측정(measure)을 기반으로 보안현황의 정확한 분석과 신속한 의사결정 필요

❖ 데이터 기반 보안 전략의 필요성

- 빅데이터 기술로 실시간 분석, 탐지 및 대응 까지 자동화
- 위협을 탐지 뿐 아니라 사전 예측 할 수 있는 첨단분석(Advanced Analytics) 요구
  - 데이터 상관관계 분석, 머신 러닝 등
- 전사적 보안 인텔리전스(Enterprise Security Intelligence) 관점에서 통합적인 보안 분석 필요
  - 보안사고대응, 위협 및 취약점 관리, 보안운영 자동화
  - 보안 솔루션의 데이터 뿐만 아니라 비즈니스 데이터까지 분석 범위 확대

2. 왜 데이터 기반 보안인가

Adaptive Security Architecture



- 보안사고대응
- 위협 및 취약점 관리
- 보안운영 자동화

Security Analytics & Intelligence

2. 어떻게 데이터 기반 보안을 구축하나

데이터 기반의 보안전략 수립을 위한 과제

데이터 분석 목적에 적절한 데이터 수집과 준비 작업

- 데이터 과학지식 외에 보안 영역내의 지식 및 경험을 통한 데이터 수집 및 준비
- 외부 전문기관의 보안 인텔리전스 정보 적극 활용

데이터 거버넌스 체계 수립

- 분석의 정확성을 확보하기 위해 이벤트 데이터와 상태(state)데이터와 결합
- 현업부서의 참여 중요, 데이터 소유권, 제공권 등 권한과 책임 명확화

데이터 기반 문화형성을 위한 변화관리 관점에서 접근

- 보안 성과지표를 개발하여 보안분석 효과 가시화
- 샌드박스 접근법을 통한 학습 문화 조성

3. 왜 인간 중심 보안인가

대부분의 보안사고는 인간 행동의 결과 (Weakest link)이며 기술 중심의 보안대책만으로는 한계 존재
Trust no one 패러다임에서 Trust but verify 패러다임으로의 변화 필요

3. 인간 중심 보안은 무엇인가

인간중심 보안(People-Centric Security, PCS)은 원칙과 신뢰를 기반으로 강압적/예방적 보안대책을 최소화하고 이상징후의 신속한 탐지와 지속적 교정을 강조하는 접근방법

- 원칙 및 신뢰를 기반으로 개별 사용자의 권한과 이와 관련된 책임을 할당
- 사용자의 책임과 자발성을 유도할 수 있는 보안 인식교육 프로그램을 수립
- 사용자의 예외적 행동을 모니터링 및 분석하고 교정활동을 수행

3. 어떻게 인간 중심 보안을 구축하나

Usable Security: 편의성과 보안성 간의 균형 추구

인간중심 보안 (People-Centric Security, PCS) 구현을 위한 두 가지 프로그램

보안문화 변화관리 프로그램

- 개별 사용자의 태도 및 실제 행동에 영향을 줄 수 있는 정교한 교육 프로그램
- 개별 사용자의 책임과 자발성을 유도

(사회과학 이론을 접목한 커뮤니케이션 프로그램 /게임 및 심리학을 이용한 재미 유발)

- 장기적이고 긍정적인 보안문화 형성

정교한 모니터링 프로그램

- 보안탐지 기술을 통한 투명성 제고

(DLP, SIEM, DAM)

- 사용자 행위분석(UBA)과 기존의 전사적 보안솔루션과의 연계
- 이벤트 기반 메시지 시스템

(보안정책이나 지침에 대한 경각심 강화)

마치면서

- 성찰의 시간 필요
- 환경 변화에 올바른 선택
- 새로운 보안 역량 개발

This storm will pass. But the choices we make now could change our lives for years to come

Yuval Noah Harari, 2020.03

Questions or Comments?

김정덕 교수
중앙대학교 산업보안학과
jdkimcau@gmail.com
http://security.cau.ac.kr