삼정 KPMG

초연결사회의 사이버 보안 8대 전략

Cyber security considerations 2022 : Trust through security

February 2022

삼정KPMG 경제연구원

Contents

본 보고서는 KPMG Global이 발간한
"Cyber security considerations 2022" 및
"Securing a hyperconnected world"를
삼정KPMG 경제연구원에서 한글 요약한 자료입니다.

◀ 표지 클릭 시 원문 다운로드 가능

삼정KPMG 경제연구원

이효정
이사
T: +82 2 2112 6744
E: hyojunglee@kr.kpmg.com

김기범
책임연구원
T: +82 2 2112 7430
E: kkim28@kr.kpmg.com

류승희
선임연구원
T: +82 2 2112 7469
E: seungheeryu@kr.kpmg.com

KPMG 선정 '2022년 사이버 보안 주요 고려 사항'

초연결사회의 사이버 보안 8대 전략

보안의 전략적 방향성 재정립

기존의 비용 및 속도 중심 보안 전략에서 비즈니스 가치 창출 및 고객경험 중시 보안 전략으로 방향성 전환

x-Factor로서의 보안 인재 육성

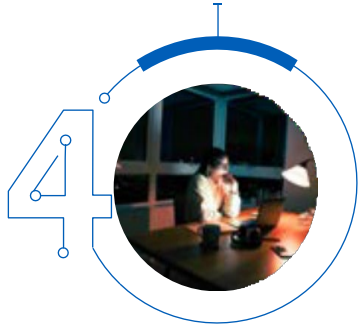
기업 성공에 필수 인자 x-Factor로서 CISO(최고정보보호책임자) 및 사이버 보안 팀을 포지셔닝

클라우드 보안 중대성 부각

자동화를 통해 클라우드 보안을 기존 사이버 보안 모니터링 역할에서 개선(Remediation)의 역할로 재정립

제로 트러스트(Zero Trust) 도입 확대

초연결된 업무 환경에 IAM(권한관리, Identity and Access Management) 및 제로 트러스트(안전한 영역은 전혀 없다는 기본 시각을 지닌 보안 방침) 적용



사이버 보안 자동화 방안 다각화

비즈니스의 최우선 가치 실현을 위한 사이버 보안 자동화 도입을 기반으로 보안 전략 강화

개인정보 보안 기법 고도화

개인정보 리스크 관리를 위해 보안 기법의 고도화 및 보안 관리 방안의 다각적 접근법 필요

생태계 협업 기반 공급망 보안

공급망 보안 전략을 트랜스포메이션하여 아날로그 방식을 디지털 자동화 보안 및 생태계 협업 기반 보안으로 전환

사이버 보안 리질리언스 부상

사이버 공격에 대비하여 기업 운영의 리질리언스 극대화 및 공격 발생 직후 경영의 빠른 복원을 위한 선제적 전략 수립

포스트 팬데믹 사이버 보안 전략

사이버 위협 진화 및 팬데믹 기간의 위협 증대

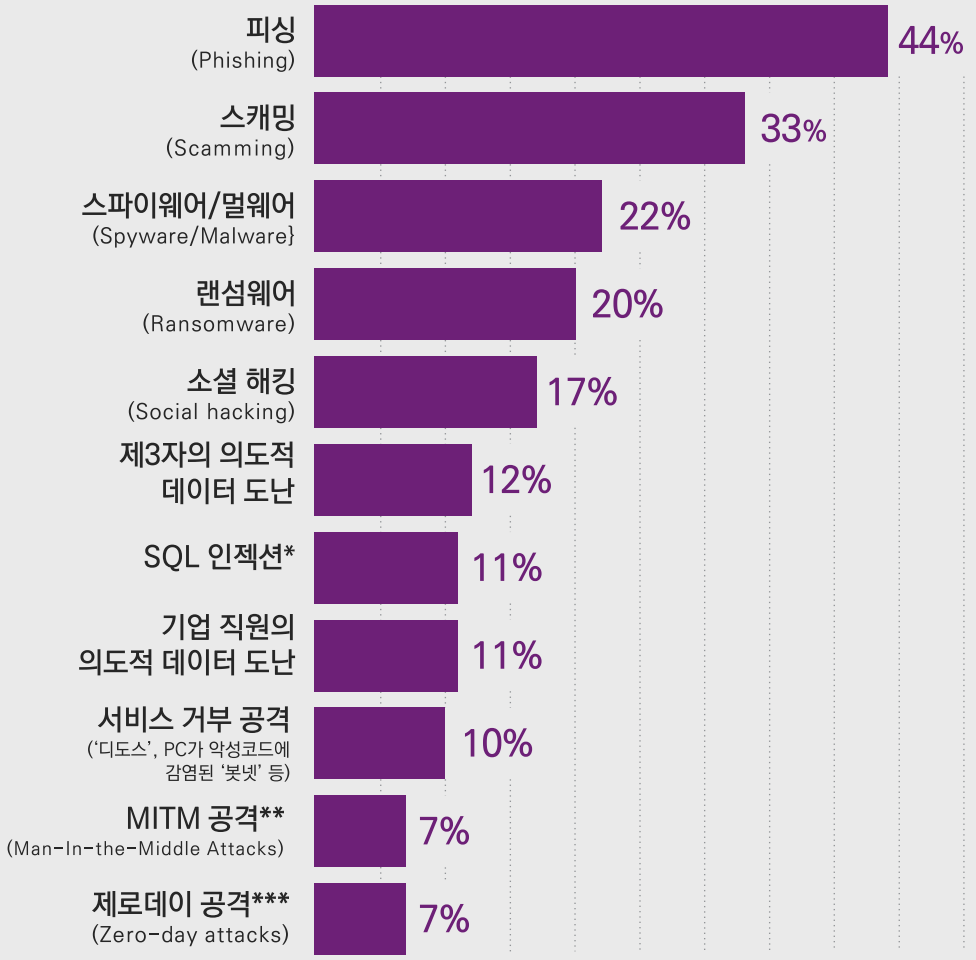
코로나19 발발 이후 팬데믹 기간 동안 사이버 범죄는 강도를 높여가고 있습니다. 비대면 비즈니스가 발전을 거듭하는 디지털 사회로 전환되어 가며 사이버 위협 또한 진화 중입니다.

KPMG가 미주(Americas) 지역 기업 C-level 임원 642명을 대상으로 설문조사를 한 결과, 최근 12개월 동안 기업이 사이버 공격 위협 증대를 경험한 적이 있는 경우, 피싱 공격을 받았다는 기업이 44%에 이르렀습니다. 그 뒤를 이어 실제 기업들이 피해를 입은 또 다른 사이버 공격의 유형으로 스캐밍 33%, 스파이웨어/멀웨어 22%, 랜섬웨어가 20%에 달했습니다. SQL 인젝션이나, 제로데이 공격 등의 신속히 대처하기 어려운 사이버 공격 또한 각각 11%, 7%로 답변되었습니다. 아울러 응답한 기업인의 79%가 적어도 1개 이상의 사이버 공격이 증대하는 모습을 본 적이 있다고 답변했습니다.

사이버 보안에 대한 대응 전략은 이제 기업의 생존과 지속성장을 좌우하는 핵심 어젠다로 부상했습니다.

> “사이버 위협이 고도화되면서 조직의 CISO(최고정보보호책임자)는 기업의 전략 방향성에 영향을 끼치는 Influencer로 역할을 강화해가고 있습니다.”
>
> Akhilesh Tuteja
> KPMG Global 사이버 보안 리더

최근 12개월간 기업이 사이버 공격을 받은 적이 있는 경우, 어떤 유형의 사이버 공격을 받았습니까?



Source: A triple threat across the Americas: 2022 KPMG Fraud Outlook

Note 1: 미주(Americas) 지역 기업의 C-level, 이사진, 부서장 등 임원 642명을 대상으로 조사한 결과
Note 2: *SQL 인젝션은 공격자가 주소창 혹은 ID · PW 창 등에 SQL(Structured Query Language) 명령어를 입력한 후 웹사이트에 침투해 서버를 제어하고, 해당 서버가 공격명령어에 따라 데이터베이스 정보를 출력하는 방식
Note 3: **MITM 공격은 중간자 공격으로 불리며, 네트워크 통신을 조작하는 공격 방법
Note 4: ***제로데이 공격은 보안 취약점이 발견된 뒤 이를 막을 수 있는 패치가 발표되기도 전에 신속하게 사이버 공격을 하는 방식

Consideration 1

Expanding the strategic security conversation

보안의 전략적 방향성 재정립

보안의 전략적 방향성 재정립

Some key actions to consider for 2022

1. 기존의 사이버 보안 관행에서 벗어나 데이터의 보안 및 가용성, 리질리언스(회복탄력성)를 높이기 위한 새로운 시각 필요

2. 기업의 주요 이해관계자가 보안 전략을 수립하고 실행할 수 있도록 하여, 조직 데이터와 고객 데이터를 보호하고, 보안 리스크에 대응하여 기업의 중장기 비즈니스 우선순위에 보안 전략을 연계

3. 기업 C-level의 보안 의식을 견고히 하여, 사이버 보안에 관한 비용과 대처 속도를 넘어선 총체적 보안 전략 필요. 기업이 실질적으로 직면할 수 있는 보안 리스크에 대응할 수 있도록 해야 함

4. 업계의 데이터 관리 동향에 예의주시하며, 기업이 데이터를 활용하여 성과를 도출할 수 있는 비즈니스 종류, 데이터 유출 사고의 종류 등을 유형화해야 함

5. 비즈니스 영역별 직면할 수 있는 데이터 유출 피해를 선제적으로 분석하며, 사이버 사고 발생 시 대처할 수 있는 속도를 사전적으로 파악해야 함

See other articles

Weave cyber security into the company's DNA

CISO(최고정보보호 책임자)는 기업의 DNA에 사이버 보안을 접목시키고, 보안을 비즈니스의 우선순위에 포함시켜 모든 임직원의 책임으로 만들어야 함

Securing the new business reality

새로운 비즈니스 현실을 보호하기 위해, 글로벌 CEO들은 사이버 보안 위험을 두려움으로 맞서야 함

Breaking the illusion of cyber security

사이버 보안의 환상을 깨기 위해, '신뢰(Trust)'가 그 어느 때보다 중요함

▲ 사진 및 제목 클릭 시
KPMG 사이버 보안 Article로 link

Consideration 2

Achieving the x-factor: Critical talent and skill sets

x-Factor로서의 보안 인재 육성

x-Factor로서의 보안 인재 육성

Some key actions to consider for 2022

1. 사이버 보안에서 근원적으로 중요한 부분이 무엇인지 재정립하여, 보안 기술에만 치우친 전략이 아닌, 보안을 비즈니스와 어떻게 긴밀히 연계할지에 대한 전략을 수립해야 함

2. 사이버 보안의 전통적인 정의에 자사를 제한시켜 놓지 않도록 유의하며, 자사에 적합한 사이버 보안 모델을 마련해야 함. 기업 조직의 다양한 부문 간 긴밀한 협력이 이뤄질 수 있도록 협업 체계 구축

3. 기업의 사이버 보안 조직의 정례적 업무에 시나리오 싱킹(Scenario Thinking)을 결합하여, 발생 가능한 사이버 보안 업무 및 보안 사고를 사전적으로 시뮬레이션하고 대응책을 마련해야 함

4. 기업의 사이버 보안 컴플라이언스 방침을 수립한 이후에도 실질적으로 가동될 수 있도록 사이버 보안 프로그램의 성과와 컴플라이언스를 연계해야 함

5. 사이버 보안의 중요성을 조직 내 인력에게 폭넓게 알리고 충분히 설명하여, 조직의 인재들이 보안의 중대성을 내재화할 수 있도록 함

6. 임직원이 사이버 보안을 조직의 중요 DNA로 인지할 수 있도록 사이버 보안의 역할 및 위상 증진

See other articles

Shape the future cyber security workforce

아웃소싱, 긱 근로자 (Gig worker, 단기계약근로자) 및 자동화를 통합하여 보안역량을 집결시키고, 사이버 보안 인력의 미래 방향성을 정립해야 함

Human firewalling

'휴먼 방화벽'을 통해, 사이버 보안의 인적 위험 요소를 극복해야 함

Exploiting the agile team culture

애자일 팀 문화를 활용한, 책임성 있는 보안문화 구축의 4가지 전략

▲ 사진 및 제목 클릭 시
KPMG 사이버 보안 Article로 link

Consideration 3

Adapting security for the cloud

클라우드 보안 중대성 부각

클라우드 보안 중대성 부각

Some key actions to consider for 2022

1. 클라우드 보안의 자동화를 고도화하여, 클라우드 보안의 도입과 모니터링, 복구의 자동화 프로세스를 강화해야 함
2. 보안 전략 방침을 숙지하고 업무 방향성을 공감하고 있는 중앙화된(Centralized) 클라우드 보안 팀을 구축하여, 보안 스킬과 더불어 보안 문화 또한 함께 공유하는 팀으로 운영
3. 상호 연동성이 중요한 클라우드 보안에서는, 보안 관련 책임 소재를 기업의 각 부문에서 개별적으로 찾기보다는 공동 대응 방침을 폭넓게 공유하고 서로 연계하여 대처해야 함
4. 국가 간, 산업 간 클라우드 보안 정책의 유사점과 차이점을 파악하여, 보안 매니지먼트 툴(Tool)에 각기 다른 정책 및 규제를 반영해야 함
5. 클라우드 전략에 발생 가능한 클라우드 리스크를 반영하여 개별 보안 이슈 발생 시 즉시 대응하도록 함

See other articles

Securing the cloud — the next chapter

최근 클라우드 기반 솔루션이 어떻게 잠재적 비즈니스 효익을 실현하고 있는지 방법을 제시

Are you a cyber pragmatist?

사이버 실용주의자들은 포스트 팬데믹 세계에서의 비즈니스 보호를 위한 새로운 접근법(Approach)을 채택함

Cloud data protection

클라우드 보안 강화를 위한 데이터 보호 역량 제고 방안

▲ 사진 및 제목 클릭 시
KPMG 사이버 보안 Article로 link

Consideration 4

Placing identity at the heart of zero trust

제로 트러스트(Zero Trust) 도입 확대

제로 트러스트(Zero Trust) 도입 확대

Some key actions to consider for 2022

1. 보안에서 안전한 영역은 전혀 없다는 것을 전제로 하는 '제로 트러스트'로 보안 방침을 전환할 때 강력한 인증 설정이 중요함. 복잡성을 제거하면서도 보안성이 높어야 하는 '암호없는 인증(Passwordless Authentication)' 등 신규 전략 수립 시 제로 트러스트를 토대로 삼아야 함

2. 보안의 신원 확인(Identity) 프로그램 가동 시 신뢰성 높은 데이터 및 데이터 분석 체계를 근간으로 지녀야 함

3. 다양한 사이버 위협 발생에 대비할 수 있도록 '아무 것도 신뢰하지 않는다'는 관점의 제로 트러스트를 기업의 사이버 보안 전략 마인드셋(Mindset)에 내재화해야 함

4. 인증 및 신원 확인 기능을 강화하여 사용자 경험(UX, User Experience) 및 고객 경험(CX, Customer Experience)을 향상시키는 데 주안점을 둬야 함

5. 기업의 숙련된 전문가들이 전략적 사고가 필요한 업무에 보다 집중할 수 있도록, 기업에서 항시 가동되어야 하는 보안 기능은 자동화할 필요가 있음

6. 기업 임직원들이 제로 트러스트 관점을 수용하고 내재화하기 위해서는 시간이 필요하므로, 중장기적 여정으로 제로 트러스트 도입 절차를 진행

See other articles

Is authentication a future enabler?

디지털 인프라에 완전한(Seamless) 인증이 필요한 이유

Everyone can embrace 'zero trust'

경계 없는 사이버 보안 모델은 진화하는 위협 환경에서 유망한 설계이며, 모든 조직은 제로 트러스트를 채택할 것임

Achieving cost efficiencies in identity and access management

사이버 보안의 비용 효율성 강화를 위한 IAM(권한관리, Identity and Access Management)을 둘러싼 전략적 접근법 소개

▲ 사진 및 제목 클릭 시 KPMG 사이버 보안 Article로 link

Consideration 5

Exploiting security automation

사이버 보안 자동화 방안 다각화

사이버 보안 자동화 방안 다각화

Some key actions to consider for 2022

1. 사이버 보안 사건 자체가 아닌, 사이버 보안 사건이 발생하기 이전에 항시 존재하는 사이버 위협에 초점을 맞춘 보안 자동화가 필요함
2. 기업의 임직원이 보다 고도화된 인지 능력을 발휘할 수 있는 여지를 만들기 위하여, 일상적인 루틴 보안 업무를 자동화해야 함
3. 기업 내 존재하는 기술 인력 및 자동화 전문가들이 사이버 보안 자동화 전략 수립에 기여할 수 있도록 함
4. SDLC(Software Development Life Cycle, 소프트웨어 개발 주기)와 관련하여 보안 자동화를 진행할 수 있는 영역의 자동화가 중차대함
5. 보안 자동화에서 이미 가능한 영역을 한계를 넘어, 한층 더 나아가는 자동화를 실현하기 위하여 지속적인 시도와 실행을 해야 함
6. 기업이 맞닥뜨리는 문제를 해결할 수 없는 보안 자동화 툴 및 기업의 가치 창출에 도움이 되지 않는 보안 자동화 툴은 오버엔지니어링(Over-engineering, 필요한 것보다 과하게 설계하는 것)하지 않도록 함

See other articles

Embrace automation as the rising star

자동화를 토대로 사이버 보안의 효율성 강화 및 업무 기여도 증대

Agile security in cloud DevOps

개발(Development)과 운영(Operations)을 결합한 데브옵스(DevOps) 방법론을 토대로 한 클라우드 보안 고도화

Security monitoring for software build pipelines

비즈니스 환경의 사이버 보안 증진을 위한 보안 모니터링 방안

▲ 사진 및 제목 클릭 시
KPMG 사이버 보안 Article로 link

Consideration 6

Protecting the privacy frontier

개인정보 보안 기법 고도화

개인정보 보안 기법 고도화

Some key actions to consider for 2022

1. 기업의 임직원에게 보안 교육을 진행하여, 개인정보 데이터 수집에 대한 각 고객의 동의는 매우 중요하며, 이를 소홀히 하여 소비자 권리가 침해되는 경우 기업에 막대한 부정적 영향을 끼칠수있음을숙지하도록 함

2. 개인정보 보호 프로그램이 기업의 C-level과 비즈니스 부문장들의 우선순위에 부합하도록 하여, 개인정보 보호에 관한 수집과 개인의 동의, 개인정보 사용 등에 대한 기업 방향성이 일관성을 지니도록 함

3. 개인정보 보호에 대한 규칙, 규정을 정비하여 개인정보 보안 리스크를 사전적으로 관리하며 예방조치를 마련하는 PbD(Privacy-by-Design, 제품 및 서비스의 기획부터 폐기까지 전 주기에 걸쳐 프라이버시를 고려한 기술 및 방침) 기준을 도입해야 함

4. 고객 권리와 데이터 보호를 위한 기업의 방향성을 소비자와 정책 입안자가 인지하고 기업의 방향성을 높이 평가하도록, 기업의 보안 업무와 전략을 입증 가능한 형태로 전환해야 함

5. 개인정보 보안 절차를 자동화하며, 이를 정책 및 규제에 부합하도록 하며, 개인정보 보안 대응 속도를 향상시키는 동시에 휴먼 에러는 줄이도록, 개인정보 관리 기술을 위한 툴을 도입해야 함

See other articles

Privacy technology: What's next?

자동화 시대의 개인정보 보호를 위한 사이버 보안 기술의 진화 방향성 제시

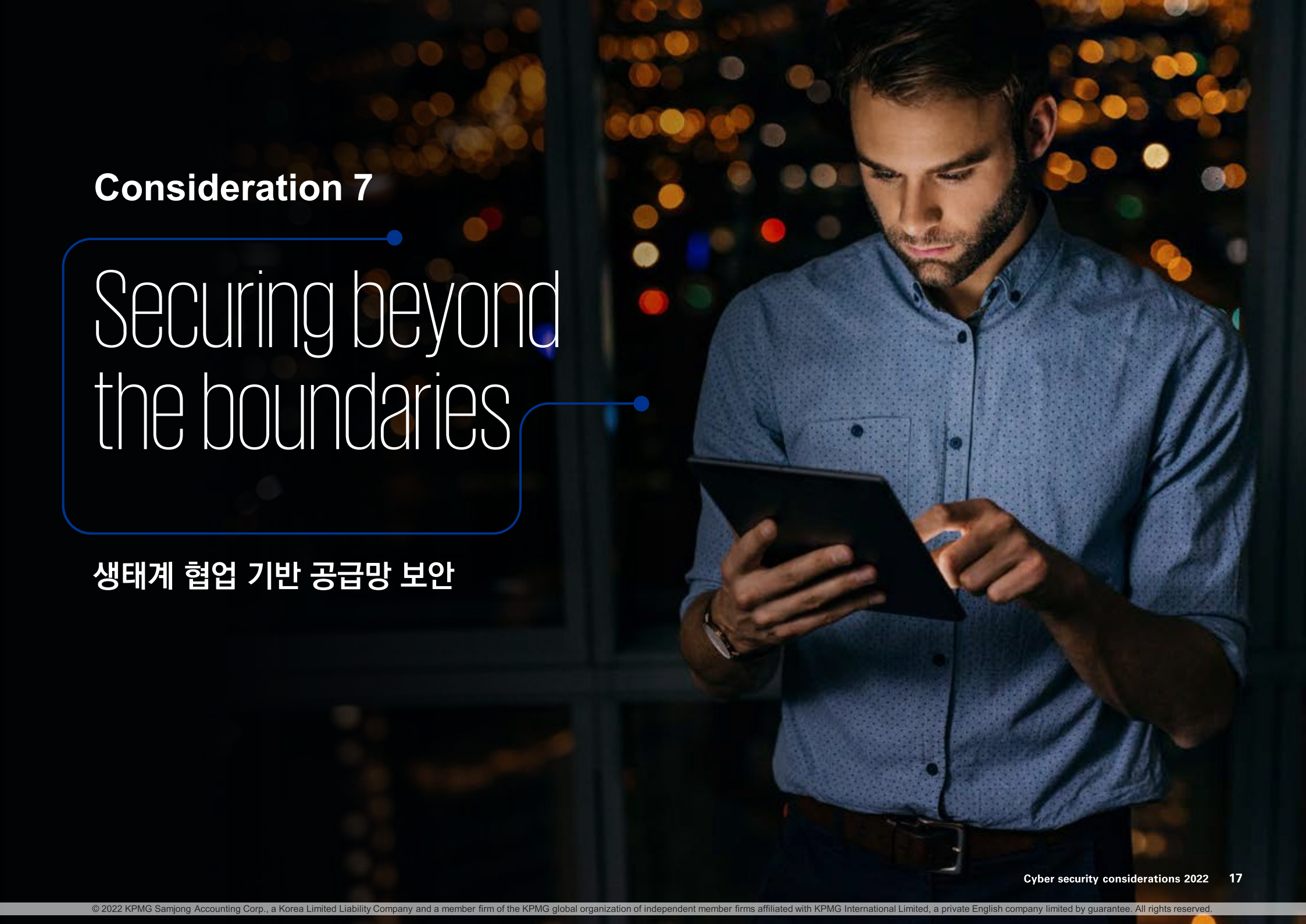
A balancing act: Privacy, security and ethics

개인정보, 보안 및 윤리에 대한 균형 있는 실행이 필요하며, 올바른 데이터 관리가 비즈니스의 성장을 촉진시킴

Corporate data responsibility: Bridging the consumer trust gap

기업이 보다 많은 개인 데이터를 보유하게 되었다는 소비자의 우려가 커짐에 따라, 소비자의 우려를 경감하고 신뢰를 높이기 위한 방안 제시

▲ 사진 및 제목 클릭 시
KPMG 사이버 보안 Article로 link



Consideration 7

Securing beyond the boundaries

생태계 협업 기반 공급망 보안

생태계 협업 기반 공급망 보안

Some key actions to consider for 2022

1. 공급망 보안에 초점을 둔 규제가 지속적으로 강화되는 가운데, 규제 동향 및 방향성을 지속적으로 모니터링 해야 함

2. 클라우드 보안 관련 국제단체인 클라우드보안협회(CSA, Cloud Security Alliance)의 클라우드 보안 프레임워크인 CCM(Cloud Controls Matrix) 등을 보안을 둘러싼 생태계를 원활히 조성하는 가이드라인으로 삼아야 함

3. 공급망 보안에 AI/ML(인공지능/머신러닝)을 적용하여 보안을 강화하는 동시에, 숙련된 보안 인력은 보다 전략적 사고를 요구하는 업무로 배치할 수 있도록 함

4. OT(Operational Technology, 생산운영기술) 관련 공급망 보안 관리의 중요성을 인지해야 함. IT(정보기술) 시스템과 OT 시스템의 지속적인 융합이 진행되며, 사이버 공격자들의 OT 시스템 공격을 통한 비즈니스 데이터 해킹이 증대될 수 있음을 숙지해야 함

5. 비즈니스 자원이 방대한 대규모 기업의 경우, 기업 공급망 전반의 협력 업체들의 보안에도 중점을 둬야, 기업이 속한 산업 생태계 환경을 근원적으로 보호할 수 있음

See other articles

The extended enterprise — securing the future

산업 생태계에 참여하는 주체가 증가함에 따라, 제3자(Third-party) 업체를 포함한 다양한 업체의 사이버 보안을 공동 증진시키는 방안

The changing third-party ecosystem

비즈니스 생태계가 고도화됨에 따라 사이버 보안은 기업 내부뿐만 아니라 외부의 제3자 업체까지 포함하여 포괄적으로 관리해야 함

Streamlining third-party risk management with AI

인공지능(AI) 기술이 고도화되며, 'AI 디지털 근로자' 또한 사이버 보안의 제3자 리스크 관리에 포함해야 함

▲ 사진 및 제목 클릭 시
KPMG 사이버 보안 Article로 link

Consideration 8

Reframing the cyber resilience conversation

사이버 보안 리질리언스 부상

사이버 보안 리질리언스 부상

Some key actions to consider for 2022

1. 사이버 공격으로 기업의 중요 기능이 중단된 경우, 비즈니스를 얼마나 오래 유지할 수 있는지, 아울러 고객 입장에서 기업이 받은 사이버 공격의 의미가 무엇인지를 선제적으로 고려해야 함
2. 중대한 사이버 공격으로 자회사 및 협력사들이 받을 영향에 대해 분석해 놓아야 함
3. 사이버 보안 및 사이버 리질리언스(회복탄력성)가 기업 이사진의 주요 어젠다로 논의되어야 함
4. 사이버 공격 유형별 기업의 리질리언스 전략 및 복구 계획, 비즈니스 정상화 프로세스에 대해 적절한 조치를 취해야 함
5. 사이버 공격 및 사이버 보안에 대한 조직의 가설과 가정에 오류가 존재할 수 있음을 인정하고, 가설 오류에 대비해 신속하게 운영할 수 있는 대체 계획을 수립해야 함
6. C-level의 위기 관리 역량 개발에 사이버 보안 관점이 적용되도록 하며, 사이버 공격 대비를 위한 시뮬레이션을 정례화하는 동시에 각 C-level 임원의 역할을 사전적으로 정립해야 함
7. 사이버 보안 리질리언스를 위한 기본 토대를 구축하는 동시에, 사이버 공격 시도를 선제적으로 탐지할 수 있는 모니터링 시스템을 구축하며, 사이버 공격에 대한 대응력과 복원력을 고도화해야 함
8. 기업 내부에 보안 관련 산업 전문가가 부재할 경우, 기업 외부의 전문가들과 협업하여 사이버 보안 리질리언스 역량을 강화해야 함

See other articles

The changing shape of ransomware

사이버 공격 강도를 높이고 있는 랜섬웨어를 방어하는 대처법

Securing a hyperconnected world

상호 연결성이 높아진 초연결 사회에서 기업의 중요 인프라를 대상으로 한 사이버 공격에 대응하는 방안

How to safeguard your OT during the 'ransomware pandemic'

랜섬웨어의 공격에 따른 피해가 이어지며, OT 보안의 중대성 부상

▲ 사진 및 제목 클릭 시
KPMG 사이버 보안 Article로 link

사이버 위협 대응을 위한 7가지 체크포인트

1 기업의 보안 관련 통합 네트워크 관리를 위한 체계적 전략을 수립하고 실행하고 있습니까?

2 기업 자산을 보호하기 위한 최신 보안 기법을 채택하고 있습니까?

3 OT(생산운영기술)와 기업 네트워크의 융합 레벨이 분석되어 있으며, 정밀한 OT 보안 전략 방향성을 보유하고 있습니까?

4 보안 통합 콘트롤 네트워크에 대한 원격 접속 등 리스크 관리를 위한 방안을 선제적으로 마련해 놓았습니까?

5 사이버 공격 대응을 위한 백업 메커니즘(Backup Mechanism)이 일관성 있게 수립되어 있습니까?

6 시큐리티 패치(보안성을 높이기 위한 소프트웨어·프로그램)를 기업에 도입하기 위한 방법론을 정립하였습니까?

7 기업의 안티-멀웨어 (Anti-Malware) 솔루션을 보유하고 있습니까?

기업 임직원의 사이버 보안에 대한 의식을 높이며, 보안 관련 위협을 임직원이 지속적으로 인지하도록 보안 전략을 통합적으로 수립해야 함

- ✓ **사이버 보안 중요성 항시 인지**: 사이버 보안의 중요성을 통감하도록 임직원의 행동 변화 필수
- ✓ **보안 교육 방법 혁신**: 영상을 통한 교육, 자료 공유 방식 등 과거의 교육법에서 벗어나, 임직원의 몰입도와 참여도를 높인 사이버 보안 교육 필요. 게이미피케이션(Gamification, 게임의 요소를 접목해 지식 전달, 관심 유도) 등의 방법을 교육에 적용할 수 있음
- ✓ **사이버 위협과 임직원 삶의 연계성 부각**: 사이버 위협을 받을 경우, 기업 조직뿐만 아니라 임직원의 일상생활, 가족 등 개인의 영역까지 영향을 받을 수 있다는 부분을 알려야 함

How KPMG can help – KPMG 사이버 보안 서비스

삼정KPMG 사이버 보안 서비스팀은 국내 최대 규모의 보안 자문 조직을 보유하고 있으며, 정보보안을 비롯하여 OT 보안, 클라우드 보안, 자동차 보안 등 디지털 기술 기반 Cyber Risk 대응 차원의 보안 자문 및 전략 수립을 지원하고 있음

	보안 서비스 내용	핵심 서비스 상품
보안 컴플라이언스 지원	**국내외 보안 규제 대응 자문** – 개인정보보호법, 정보통신망법, 신용정보보호법, 영업비밀보호법, 정보보호공시제도, GDPR/미국/중국/영국 등 글로벌 보안 법규 대응 **정보보안 관련 컴플라이언스 및 인증 자문** – ISMS, ISMS-P, ISO27001, ISO27701, PCI-DSS, SOC Report 등 국내외 보안 컴플라이언스/인증 대응	**1 국내외 보안 규제 대응 자문** • 보안 규제 대응 체계 구축 및 관리 지원 **2 보안 인증 및 컴플라이언스 대응 지원** • 국내외 보안 인증 획득 지원 자문 • 클라우드 보안 안전성 평가 자문
사이버 보안 리스크 대응	**Cyber 공격 및 신기술 보안위협 대응 자문** **Cyber Risk Data Analytics 자문** – 모의해킹 기법 활용한 Cyber 위협 대응 – IoT, 클라우드, 핀테크 보안 체계 자문 – 빅데이터 기반 Cyber Risk 분석 서비스	**3 Emerging Tech. Risk 보안 자문** • OT, AI, 클라우드, 메타버스, 블록체인 보안 자문 • 연간 사이버 보안 지원 서비스 **4 Biz 프로세스 기반 Cyber Risk 자문** • Biz Risk 기반 사이버 범죄/사고 가능성 진단 • 데이터 라이프 사이클 기반 보안 거버넌스 자문
보안 전략	**대규모 IT 시스템 보안 아키텍처 수립 자문** – 글로벌 경쟁력 강화 및 신기술 4차 산업혁명 대비 중장기 보안 발전 전략 수립 지원 **전사/그룹사 보안 마스터플랜 수립 자문**	**5 디지털 보안 전략 수립 지원** • 디지털 전환을 위한 보안 마스터플랜 수립 자문 • 산업 시스템 안전을 위한 OT/ICS 보안 전략 • 사이버 보안 성숙도 평가 및 벤치마킹 • 사이버 GRC 체계 구축 자문 • 제로 트러스트 기반의 IAM 구축 자문

삼정 KPMG

Business Contacts

사이버 보안 전문팀

김민수
전무
T: 02-2112-7010
E: mkim9@kr.kpmg.com

고영대
상무
T: 02-2112-7098
E: youngdaiko@kr.kpmg.com

home.kpmg/kr
home.kpmg/socialmedia