Deloitte.

정교해진 사이버 공격의 변화 양상과 대응 전략

전 세계 지역별 사이버 위협 및 사고 사례 조사
– 3개 권역 내 20개국가들의 주요 사이버 위협요소 비교

Center for Integrated Research, April, 2024

리더 메시지

유선희 파트너

리스크 자문 본부 | Cyber

기업 조직을 겨냥한 사이버 공격은 정교해지고 빠른 속도로 확산되고 있다. 피싱, 랜섬웨어, 암호화폐 채굴 악성코드, 정교한 산업 멀웨어 등 공격 방식과 용량 그리고 속도 면에서 상당한 진화를 거듭하고 있어, 많은 기업들은 급속히 확산 중인 새로운 공격 방식에 대응하기가 점차 어려워지고 있는 상황이다.

디지털 전환(Digital Transformation)에 따른 글로벌 경제와 산업구조 변화가 불러온 부작용이라 볼 수 있다. 디지털 전환은 비즈니스 모델과 프로세스의 혁신을 가져왔지만, 사이버 범죄자들이 공격할 수 있는 범위와 기회가 확대되었기 때문이다. 이들은 주로 네트워크, 애플리케이션, 임베디드 장치, 엑세스 포인트(AP)등을 공격 대상으로 삼고 있으며, 보다 새로운 방식으로 대담한 공격을 감행하고 있다. 이들도 디지털 전환과 유사한 전환을 경험한 것이다.

현재 만연하고 있는 최신 사이버 공격은 전통적인 보안정책과 전략 및 아키텍처 그리고 개별적으로 동작하는 포인트 솔루션으로는 대응하기가 어렵다. 기업내 IT 전담 조직도 충분한 보안 기능을 제공하지 못하고 있다.

오늘날 사이버 침해 사고는 기업의 신뢰와 운영에 심각한 피해를 주기 때문에 조직내 보안 이슈가 비즈니스 리더들의 최우선 과제가 되고 있다. 이제 리더들은 최신 사이버 공격에 대처하기 위해 사업장이 위치한 지역을 고려해야 하고, 보안 인프라 수준 및 위협 요인을 식별해야 한다. 그리고 이를 대응하기 위한 적합한 보안 솔루션의 도입과 투자를 고민해야 한다.

딜로이트는 2023년 '글로벌 사이버의 미래'를 주제로 조사를 진행했다. 본 조사에는 총 20개국 소속 1,100명이 설문과 인터뷰에 참여했고, 전 세계 지역별(북미, EMEA 및 APAC)로 사이버 위협과 침해 사례를 분석해 특정 지역에 주요한 위협 요인과 우선순위를 확인했다. 딜로이트는 수집된 데이터를 기반으로 비즈니스 리더들과 보안 담당자에게 지역 맞춤화 된 사이버 보안 전략 수립과 사이버 보안 취약점 해소 그리고 보안 솔루션 도입과 인프라 투자 실행과 관련한 시사점을 제공하고자 한다.

Table Of Contents

정교해진 보안 위협과 대응 전략

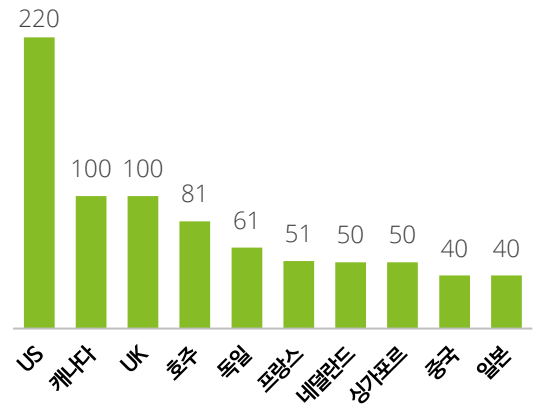
전세계 권역 별 사이버 위협 현황 파악 결과, 유럽 지역에서 개인/범죄 단체들에 의한 피싱/멀웨어/랜섬웨어 공격이 빈번하게 발생하고 있으며, 사이버 공격으로 인한 서비스 중단/지연, 기업 이미지 훼손 및 재무적 손실 방지를 위한 전략적 투자가 필요

조사 목적 및 대상

전세계 권역 별 사이버 보안 위협 유형 파악 및 대응전략 수립

조사 개요	
대상	• 미주, MENA, AP 권역의 글로벌 기업 • 총 20 개국 총 1,100명 참여

주요 10개국 조사 참여자(명)



사이버 위협 유형 및 비즈니스 영향

유럽 지역에 사이버 공격 빈번, 개인/범죄 단체들에 의한 피싱/멀웨어/랜섬웨어 공격이 다수

사이버 공격 발생 빈번 지역

- (유럽) 독일과 영국이 연간 11건 이상 사이버 침해 경험 (사고 발생율[1] 25%, 글로벌 평균 16%)
- 싱가포르(8%), 캐나나(12%), 일본(13%), 중국(13%) 순으로 사이버 사고 발생률은 글로벌 평균보다 낮음

사이버 공격 행위자 유형

- 개인/범죄 단체의 사이버 공격이 전체 공격의 40% 이상 점유
- 네달란드(56%)와 중국(50%)이 개인/범죄 단체들에 의한 공격 위협 높음
- 영국(41%)과 중국(40%)에서는 사이버 테러리스트와 핵티비스트들의 사이버 공격 위협 높음

사이버 공격 유형

- 전 세계에서 발생하는 대부분의 사이버 공격은 '피싱', '멀웨어(악성 소프트웨어)' 그리고 '랜섬웨어' 방식
- DDoS공격, 지능형 지속 공격(APTs)에 높은 우려를 보이고 있는 사이버 공격 유형

사이버 위협 대응 전략

사이버 공격 위협에 따른 서비스 중단/지연과 이미지 손상 및 재무적 손실 방지를 위한 사이버 전략 수립과 투자 필요

사이버 공격이 미치는 비즈니스 영향

서비스 중단/ 지연 발생 (56%)	기업이미지 손상 (55%)	재무적 손실 (54%)

[사이버 위협 대응전략]

1. 실시간 사이버 위협 탐지 및 사고 대응 계획 수립
2. 사이버 위협 탐지와 신속한 대응을 위한 신기술과 솔루션 도입
3. 인프라와 네트워크 진입 취약점 보완
4. 기술과 프로세스 원칙에 따른 보안체계 설계에 집중
5. 사이버 사고 대응 시나리오 수립 및 임직원 참여 유도

투자 우선순위

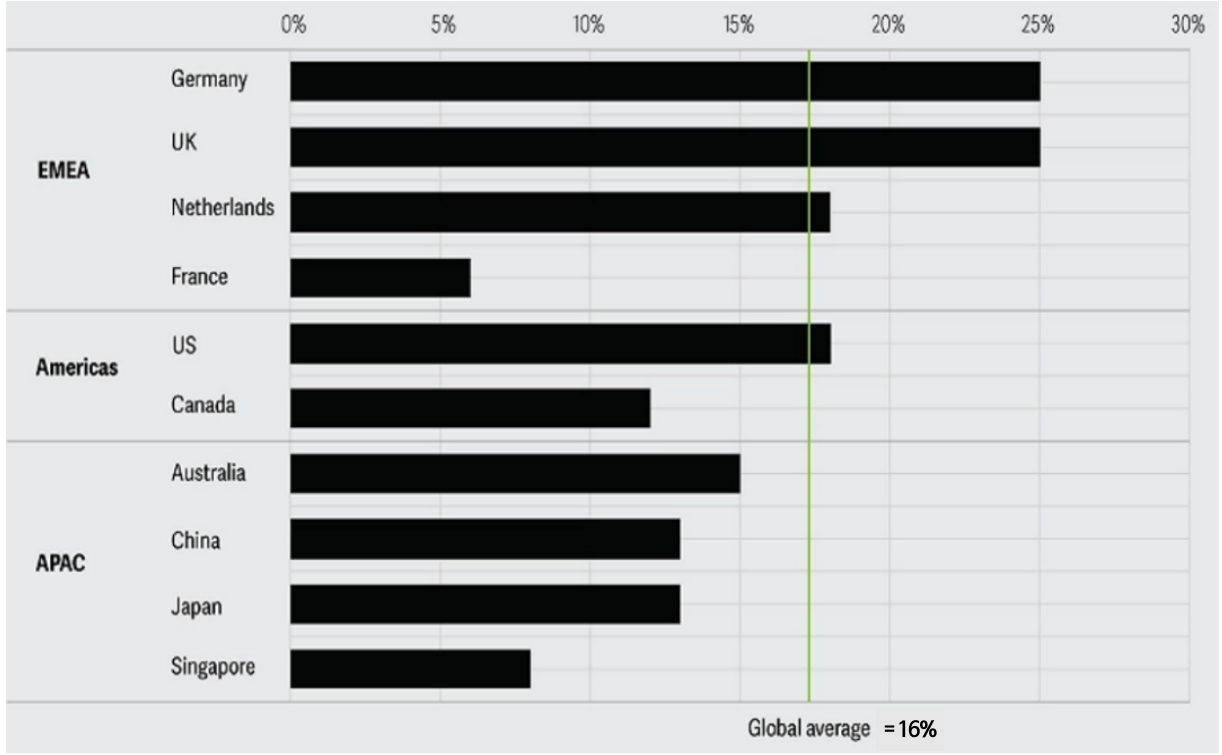
- 사이버 보안전략 수립
- 클라우드, 데이터/개인정보보호 분야 順

1) 국가별 사고 발생율(%) = (사이버 사고를 연 11회~16회까지 경험 했다고 응답한 자수) ÷ (국가별 총 응답자수)

전 세계 권역별 사이버 보안 위협 (1/3)

디지털 인프라가 완비된 유럽과 북미지역에서 사이버 사고가 빈번히 발생했고, 아시아 지역 내 중국이 단기간 디지털 인프라의 확충으로 사이버 공격 대상이 되고 있으며, 사이버 사고 발생율은 낮은 국가는 다수 기업이 공격 대응 전략과 솔루션을 보유

주요국 사이버 침해 사고율



- 국가별 사고 발생율(%) = (사이버 사고를 연 11회~16회까지 경험 했다고 응답한자 수) ÷ (국가별 총 응답자 수)
- 미주, MENA, AP 권역의 글로벌 기업, 총 20 개국 소속 1,100명이 응답에 참여

디지털 인프라가 완비된 국가일 수록 사이버 공격의 대상으로 지목, 사이버 대응 전력과 솔루션 투자가 필요

유럽지역 사이버 사고 발생 빈번

- EMEA 지역에 위치한 기업들 중 연간 11건 이상의 사이버 침해 사고를 경험 기업은 20% (글로벌 평균 16%)
- 독일과 영국에서 연간 25% 이상의 기업들이 사이버 침해 사고 경험

아시아 지역 사이버 공격 타깃

- 사이버 사고 발생율은 싱가포르(8%), 일본(13%), 중국(13%)순으로 글로벌 평균보다 낮으나, 인프라 부재로 사고 발생 인지율 미흡
- (중국) 단기간에 대규모 디지털 인프라와 전자상거래 생태계가 확대되어 사이버 공격 대상으로 부각

사이버 공격 대응 역량 보유국

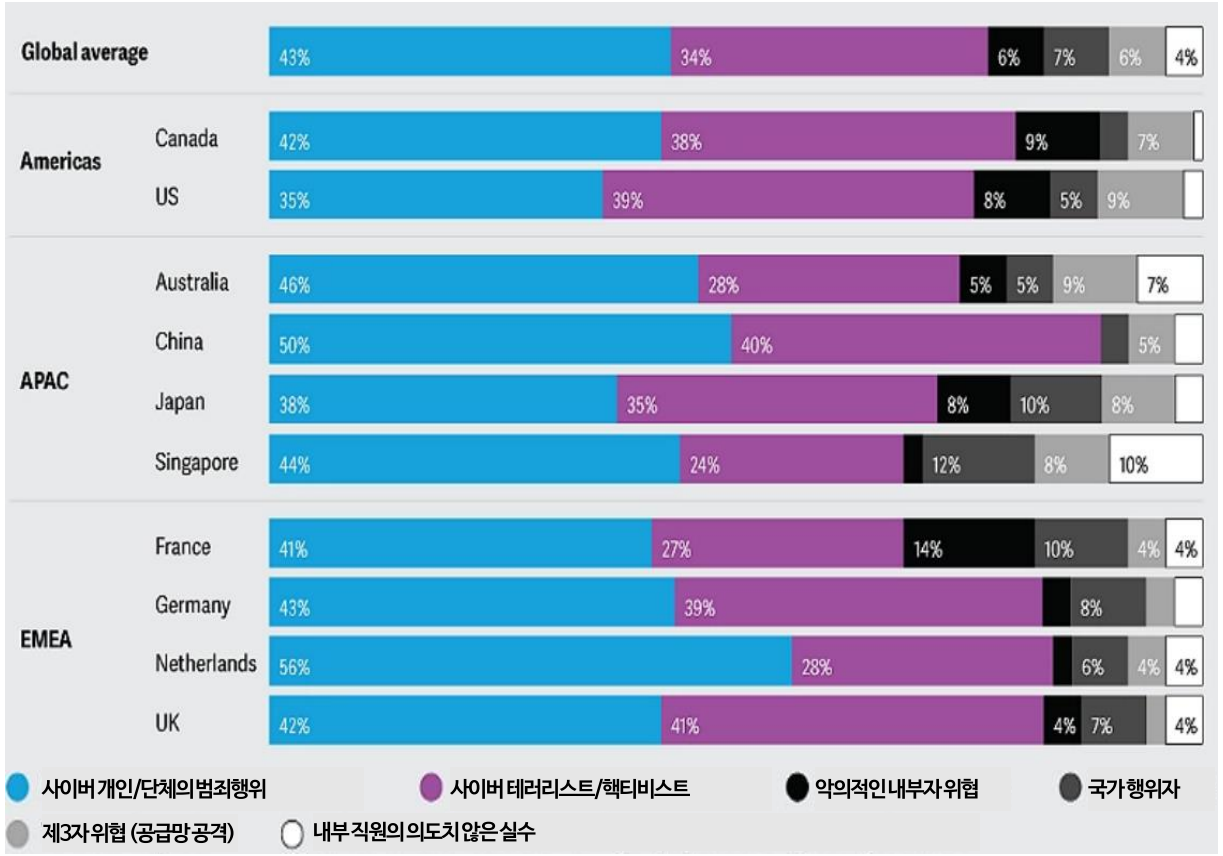
- (프랑스) 프랑스 기업 97%가 사이버 보안 투자 증액 및 67%가 SOAR [1)]에 투자
- (싱가포르) 사이버 성숙도가 높은 기업이 다수이며, 사이버 위협으로부터 방어하기 위한 운영 및 전략적 계획 완비

1) SOAR(Security Orchestration, Automation and Response)는 보안 인력들이 보안 오케이스트레이션((Security Orchestration), 자동화(Automation) 및 IT 보안사고 대응(Response)을 지원하는 소루션으로 이를 통해 보안팀은 프로세스를 간소화 하고 사고 대응 프로세스를 가속화 할 수 있다.

전 세계 권역별 사이버 보안 위협 (2/3)

사이버 위협 행위자 또는 악의적인 행위자라고 불리는 이들은 디지털 디바이스나 시스템에 고의로 피해를 입히는 개인 또는 집단으로 시스템, 네트워크 및 소프트웨어의 취약점을 악용하여 피싱, 랜섬웨어, 멀웨어 공격 등 다양한 사이버 공격을 지속

사이버 공격자 유형



개인/범죄 단체의 사이버 공격이 전체 사이버 위협의 40% 이상 점유
사이버 테러리스트/핵티비스트(34%), 내부자 위협(6%) 순

사이버 범죄 단체

- 금전적 이득을 목적으로 사이버 범죄를 저지르는 개인이나 집단
- 랜섬웨어 공격과 사람들을 속여 송금을 유도, 신용카드 정보, 로그인 자격 증명, 기타 개인 정보나 민감한 정보를 유출하는 피싱 사기

사이버 테러리스트 및 핵티비스트

- 정치적 또는 사회적 의제를 홍보 및 국가의 안보 위협 및 폭력을 초래하는 집단
- 개인, 조직 또는 정부 기관을 표적으로 삼아 기밀이나 기타 민감한 정보를 폭로 (e.g. 국제 해킹 집단 Anonymous)

내부자 위협

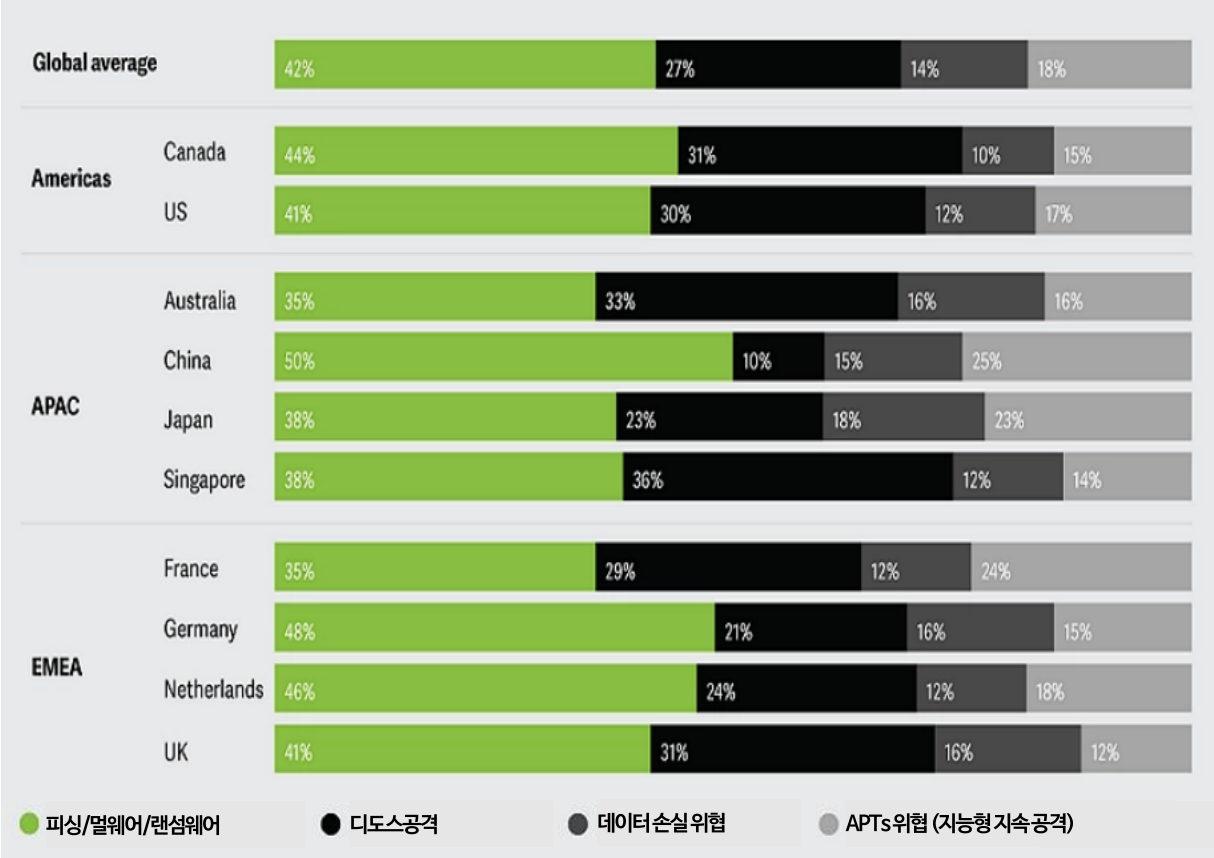
- 내부 시스템에 접근권한이 있는 직원으로 의도지 않게 멀웨어 설치하거나, 악의적인 의도로 데이터/애플리케이션 손상

1) SOAR(Security Orchestration, Automation and Response)는 보안 인력들이 보안 오케이스트레이션((Security Orchestration), 자동화(Automation) 및 IT 보안사고 대응(Response)을 지원하는 소루션으로 이를 통해 보안팀은 프로세스를 간소화 하고 사고 대응 프로세스를 가속화 할 수 있다.

전 세계 권역별 사이버 보안 위협 (3/3)

사이버 범죄자들은 엔터프라이즈 IT 시스템, 네트워크, 개인 디바이스 등 기업의 물리적 자산을 대상으로 공격을 시도하며,
피싱 ·멀웨어 ·랜섬웨어, 디도스 공격(DDoS, 분산서비스 거부 공격) 및 지능형 지속 공격(APTs)방식이 다수의 공격 유형에 해당

사이버 공격 전술



전 세계에서 발생하는 대부분의 사이버 공격은 '피싱', '멀웨어(악성 소프트웨어)' 그리고 '랜섬웨어' 방식

피싱 ·멀웨어 ·랜섬웨어
글로벌 평균: 42%

- 중국(50%)과 독일(48%)에서 가장 위협적인 사이버 공격
- 악성 소프트웨어가 시스템 을 작동 불능 상태로 만들거나 민감 정보 유출/유포

DDOS 공격[1)]
글로벌 평균: 27%

- 싱가포르(36%)와 호주(33%)에서 가장 위협적인 공격으로 보고
- 대상 시스템을 사기성 트래픽으로 가득 채우고, 시스템을 압도하여, 합법적인 요청을 방해하고 시스템 수행능력을 저하시키는 공격

APT 위협
글로벌 평균: 18%

- 프랑스(24%), 일본(23%)에서 가장 위협적인 공격유형으로 보고
- 네트워크에 은밀하게 잠복해 있는 사이버 위협으로 대부분의 경우 목표는 몇 개월 또는 몇 년에 걸쳐 지속적으로 꾸준히 데이터 누출

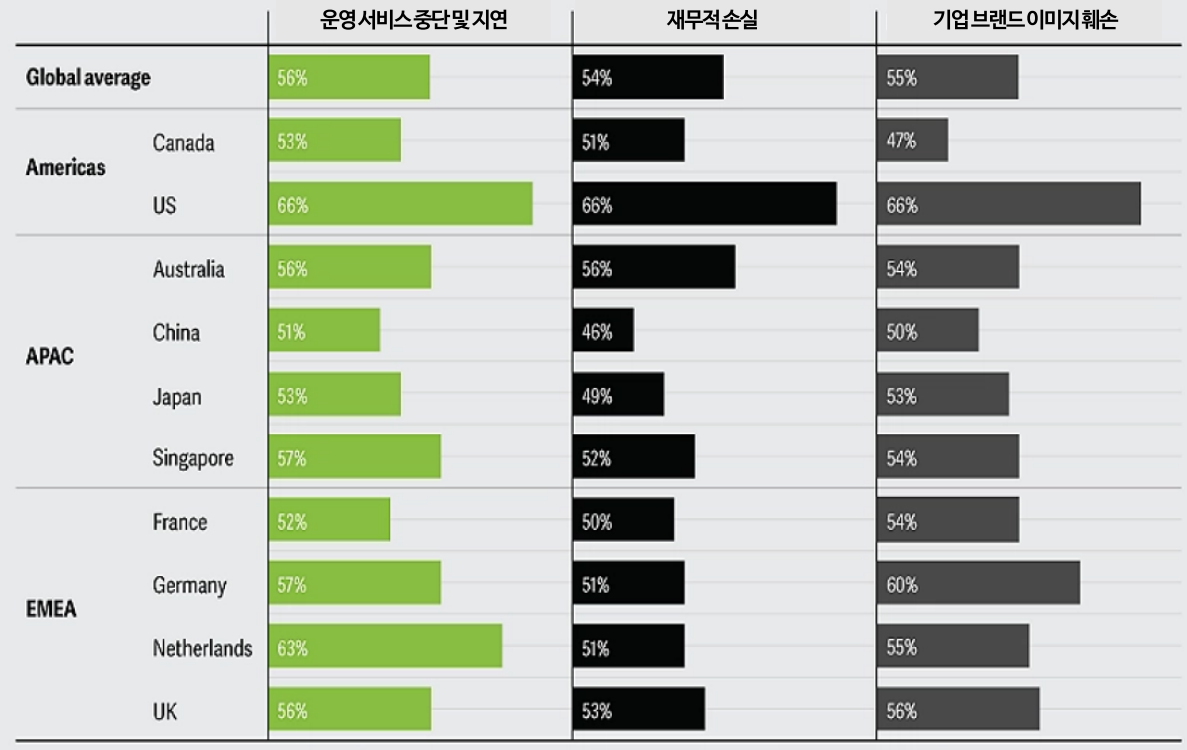
1) 디도스 공격(DDOS, Denial-of Service attacks, 분산 서비스 거부 공격) : 특정 서버(컴퓨터)나 네트워크 장비를 대상으로 많은 데이터를 발생시켜 장애를 일으키는 방식

사이버 공격이 비즈니스에 미치는 영향 및 대응 전략 (1/2)

기업들은 그들이 위치한 지역에서 빈번한 발생하는 사이버 공격 유형을 파악하고, 보유한 인프라와 대응 역량을 고려한 사이버 위협 대응 전략 수립이 필요

사이버 침해 영역 및 손실 정도

디지털 성숙도가 높은 국가일 수록 (북미, 유럽, 아시아 순)
사이버 침해 영역/손실 정도를 높게 인지



사이버 위협 대응 전략

기업이 소속된 지역의 위협 인텔리전트[1]를 활용하여 대응 전략 수립

1. 실시간 사이버 위협 탐지 및 사고 대응 계획 수립
2. 사이버 위협 탐지와 신속한 대응을 위한 신기술과 솔루션 도입
3. 시스템 인프라와 네트워크 진입 지점의 취약점 보완
4. 기술과 프로세스 원칙에 따른 보안체계 설계에 집중
5. 사이버 사고 대응 시나리오 수립 및 임직원 참여 유도

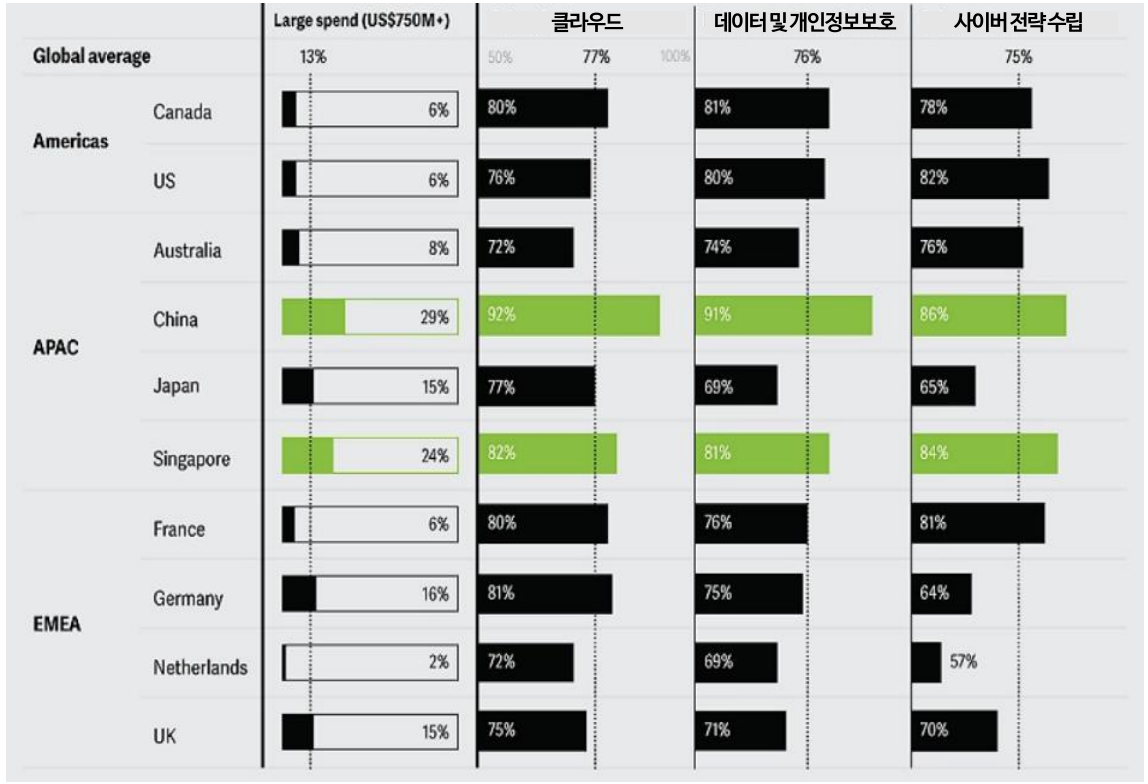
1) 위협 인텔리전스는 위협 행위자의 동기, 대상, 공격 방식을 이해하기 위해 수집, 처리, 분석되는 데이터를 말한다.

사이버 공격이 비즈니스에 미치는 영향 및 대응 전략 (2/2)

사전에 위협 식별과 사이버 공격 시 재무적 위험과 손실을 최소화를 위해서는 사이버 대응 전략 방향에 따라 클라우드, 데이터 보호 및 개인정보 보호 분야에 집중 투자 필요

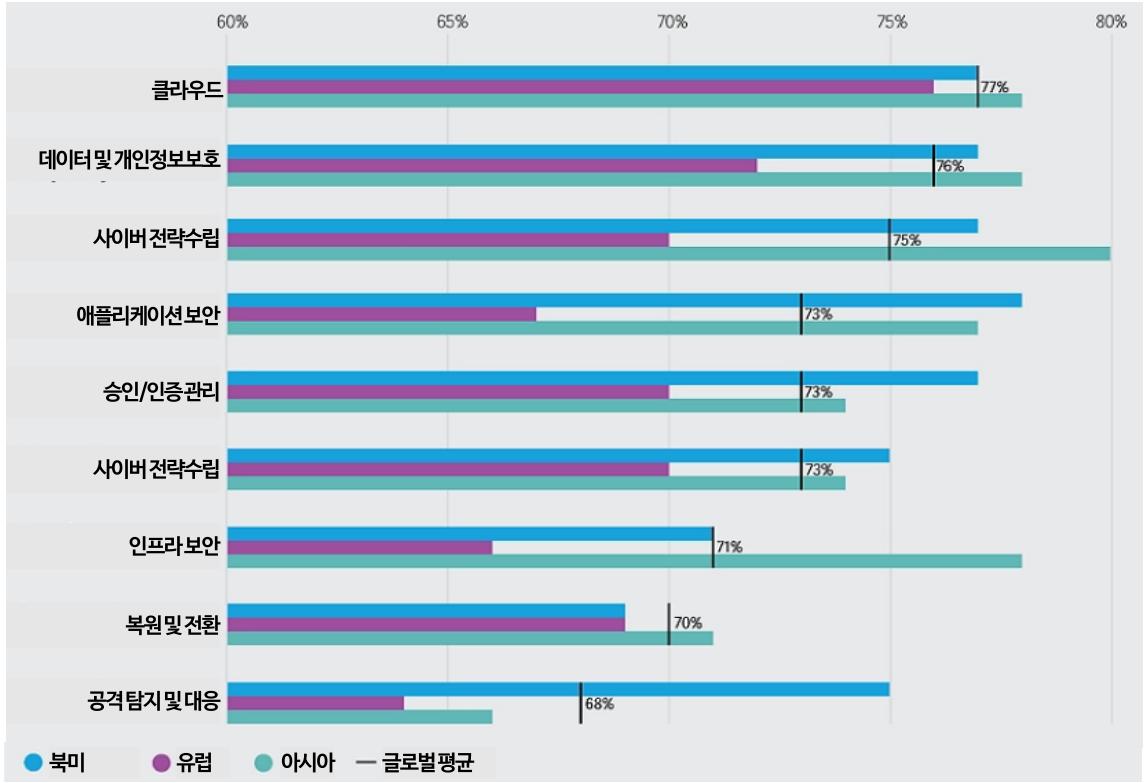
사이버 투자 우선 순위

조사 참여 기업 중 약 13%가 사이버 보안 분야에 연간 약 7.5억 달러 이상(약 9천억원)의 대규모 투자를 실행



지역별 사이버 집중 투자 영역

전 세계 다수의 기업들의 사이버 투자 방향은 사이버 보안 전략, 사이버 클라우드, 데이터 보호 및 개인정보 보호 분야에 집중



사이버 위협 대응을 위한 제언

기업은 사이버 전략 실행과 보안 시스템 구축으로 사이버 공격에 대응할 수 있지만 시스템 의존방식에는 한계가 있으며,
기술, 프로세스, 인적자원 요소가 적절히 조합될 때 중요한 시스템과 민감 정보가 보호되고, 기업의 사이버 보안이 실현 가능

사이버 위협 대응을 위한 주요 실행 과제

- 최소 권한 액세스, 다중 인증, 강력한 비밀번호 정책을 포함한 ID 및 액세스 관리(IAM) 플랫폼과 운영 정책이 필요
- 방화벽 강화 및 종합 데이터 보안 플랫폼 및 DLP(Data Loss Prevention) 툴 도입
- 사용자 보안인식 교육 및 정기적인 사이버 모의 테스트 실행
- 공격 표면 관리(ASM) 툴과 통합 엔드포인트 관리(UEM) 툴 도입으로 기업내 모든 네트워크의 보안정책 제어

- 지속적인 보안 모니터링 및 조기 탐지 프로세스와 솔루션 도입으로 진행 중인 사이버 공격을 식별
- 사전 예방적 위협 헌팅 프로세스 도입으로 지능형 지속 공격(APT)과 같이 네트워크에 은밀하게 잠복해 있는 사이버 위협 추적

- 기업은 진행 중인 사이버 공격 및 기타 사이버 보안 이벤트에 적절히 대응하기 위한 조치사항 사전 정의
- 보안 오케스트레이션, 자동화 및 대응(SOAR) 솔루션을 도입으로 사이버 공격에 실시간 대응
- 확장탐지 및 대응(XDR) 솔루션 도입으로 사전 예방적 위협 헌팅과 사이버 공격 예방, 탐지, 조사 및 대응 프로세스 자동화

Risk Advisory – Cyber

딜로이트 Cyber 서비스는 고객이 복잡한 사이버 위협으로 부터 조직의 정보자산을 보호하고 조직의 전략적 성장, 혁신 및 성과 목표를 이룰 수 있도록 지원합니다.

Professionals

- 정보보안 전략 수립 및 마스터플랜 수립
- 정보보안 관리체계 고도화
- TPCRM (Third Party Cyber Risk Management)
- 정보보안 인증 지원 및 상시 보안 자문; ISMS-P, PCI-DSS, ISO 27001, SOC(System and Organization Controls), Webtrust 등
- 개인정보보호 자문
- 전자서명인증평가
- EVA (External Vulnerability Assessment); 취약점 점검 및 모의해킹
- GDPR (General Data Protection Regulation) 대응
- 침해사고대응 모의훈련 컨설팅
- 사이버 침해사고 분석 및 대응

서영수 파트너
리스크자문본부 | Cyber
Tel : 02 6676 1929
E-mail: youngseo@deloitte.com

유선희 파트너
리스크 자문 본부 | Cyber
Tel : 02 66762956
E-mail: sunhyou@deloitte.com

이상훈 이사
리스크자문본부 | Cyber
Tel : 02 6676 2937
E-mail: sanghunlee@deloitte.com

조성규 이사
리스크 자문 본부 | Cyber
Tel : 02 6676 2978
E-mail : sungkcho@deloitte.com

한호규 이사
리스크자문본부 | Cyber
Tel : 02 6676 1922
E-mail: hhahn@deloitte.com

신진환 이사
리스크 자문 본부 | Cyber
Tel : 02 6676 4675
E-mail: jinshin@deloitte.com

이재웅 이사
리스크자문본부 | Cyber
Tel : 02 6676 2918
E-mail: jaewoonlee@deloitte.com

김유철 이사
리스크 자문 본부 | Cyber
Tel : 02 6676 3076
E-mail : yuckim@deloitte.com

김용환 이사
리스크 자문 본부 | Cyber
Tel : 02 6676 2099
E-mail : yonghwkim@deloitte.com

Deloitte.
Insights

딜로이트 안진회계법인·딜로이트 컨설팅
성장전략 본부

손재호 Partner
고객산업본부 본부장
jaehoson@deloitte.com

정동섭 Partner
딜로이트 인사이트 리더
dongjeong@deloitte.com

김사헌 Director
딜로이트 인사이트 편집장
sahekim@deloitte.com

HOT LINE
02) 6099-4651