

# KISA 정보보호 해외진출 전략거점(동남아 남부) 12월 주요동향

2023. 12. 29(금), 한국인터넷진흥원 보안산업단 글로벌협력팀

이슈	주요내용 및 시사점
[싱가포르] 사이버 침해 사고 대응 훈련	<p>▶ <b>싱가포르 24개국 200명 OT 기반 침해사고 대응 사이버 훈련 개최</b></p> <ul style="list-style-type: none"> <li>✓ 싱가포르 국방장관 Heng Chee How와 통신정보보건부 장관 Janil Puthucheary 박사는 최근 CDeX(Critical Infrastructure Defense Training) 2023을 방문하여 정부의 의지를 강조</li> <li>✓ 디지털 정보국(DIS)과 싱가포르 사이버 보안국(CSA)이 iTrust/SUTD 및 국립 사이버 보안 R&amp;D 연구소(NCL)의 지원을 받아 싱가포르 국립대학교 컴퓨팅 학교에서 조직한 CDeX 2023에 24개 국가 200명 이상의 참가자가 운영기술(OT) 핵심 인프라 방어 훈련에 참여</li> <li>✓ 이번 훈련에는 IT 네트워크와 전력, 물, 통신, 항공 등 6개 분야에서 훈련을 제공</li> <li>✓ CDeX 2023은 사이버보안 관행에서 선두 위치를 유지하려는 싱가포르의 확고하면서도 강력한 의지를 표명</li> </ul>
[필리핀] 사이버 보안 강화 법안 제정 추진	<p>▶ <b>마르코스 대통령은 사이버 보안 노력을 강화하기 위한 세 가지 법안 제시</b></p> <ul style="list-style-type: none"> <li>✓ 지난 화요일 Marcos와의 회의에서 PSAC(민간 부문 자문 위원회)의 디지털 인프라 그룹은 제안된 사이버 보안법, 노새 방지법( Anti-Mule Act) 및 온라인 사이트 차단법을 우선 법안으로 인증할 것을 권고</li> <li>✓ 사이버보안법 또는 상원 법안 No. 1365는 필리핀의 사이버 보안 탄력성을 강화하고, 중요한 정보 인프라를 보호하며, 디지털 자산 보호에 대한 표준 및 관행 준수 측면에서 성과가 저조한 기관에 처벌을 포함</li> <li>✓ 노새 방지법(SB 2039)은 은행 계좌, 전자 지갑 및 기타 금융 계좌와 관련된 돈 노새(bar money mules) 및 사기 행위를 금지하는 것을 목표. 법안은 또한 가짜 신원을 사용하여 계정을 등록하거나 개설하는 행위, 승인되지 않은 사람에게 계정을 판매 또는 양도하는 행위, 소유자가 아닌 계정을 구매 또는 사용하는 행위, 사기를 저지르기 위해 계좌를 개설하도록 사람들을 모집하는 행위를 범죄화</li> <li>✓ 온라인사이트 차단법안은 창작산업과 소비자를 보호하기 위해 불법복제 콘텐츠를 게시하는 사이트의 차단을 제도화</li> </ul>
[인도네시아] 선거관리위원회(KPU) 유권자 데이터 유출	<p>▶ <b>선거관리위원회 데이터 유출에도 체계는 안전</b></p> <ul style="list-style-type: none"> <li>✓ 선거 관리 위원회(KPU)는 2억 4천만 건의 기록 유출 의혹 속에서 유권자 데이터의 안전을 보장하며, KPU 회원인 Idham Holik은 영구 유권자 목록(DPT)의 사본을 출력하는 과정이 해당 문제에 영향을 받지 않았다고 언급</li> <li>✓ 국가 사이버 및 암호화 기관(BSSN)은 의심되는 데이터 유출의 근본 원인을 확인하기 위해 디지털 포렌식을 수행</li> </ul>
[인도네시아] 암호화 서비스 개시	<p>▶ <b>BSSN은 데이터 보안 강화를 위한 데이터 암호화 서비스를 시작</b></p> <ul style="list-style-type: none"> <li>✓ BSSN의 수장 힌사 시부리안은 자바 서부 데콧의 BSSN 사무실에서 데이터 암호화 서비스를 출시</li> <li>✓ BSSN은 정부 부문, 핵심 정보 인프라 부문 및 기타 부문에서 데이터를 관리하거나 처리하는 전자 시스템 운영자(PSE)에게 보호 솔루션 형태로 지원을 제공</li> </ul>

이 슈	주 요 내 용 및 시 사 점
[말레이시아] 사이버 침해 국가 순위 8위	<ul style="list-style-type: none"> <li>✓ BSSN은 데이터 보호를 지원하는 암호화폐 분야 서비스인 샌디데이터(Sandi Data)를 출시</li> <li>✓ BSSN은 국가 사이버 보안 전략의 중점 영역 중 하나로 암호화 독립성을 지정</li> </ul> <p>▶ <b>말레이시아는 2023년 제3분기에 여덟 번째로 가장 많이 침해된 국가로 순위</b></p> <ul style="list-style-type: none"> <li>✓ Surfshark의 2023년 제3분기 보고서에 따르면 말레이시아는 2분기 대비 누출률이 144% 증가하여 유출된 계정이 494,699건으로 기록되어 여덟 번째로 가장 침해받은 국가로 순위</li> <li>✓ 또한, 국가의 인구로 나눈 하루 평균 침해된 계정 수를 침해 밀도로 정의하면, 말레이시아는 하루에 약 5,436개의 계정이 침해되어 5위에 해당</li> <li>✓ 전 세계적으로 제3분기에는 3,150만 건의 계정이 침해되었으며, 미국이 810만 건으로 선두를 차지하였으며 그 뒤로 러시아(710만건), 프랑스(160만건), 중국(140만건), 멕시코(120만건)임.</li> </ul>
[말레이시아] Perkeso 사이버 보안 침해	<p>▶ <b>말레이시아의 사회보장기관(Perkeso)의 12월 2일부터 사이버 보안 침해사고 발생 확인</b></p> <ul style="list-style-type: none"> <li>✓ 말레이시아의 사회보장기관(Perkeso)은 시스템 및 웹사이트에 대한 사이버 공격이 확인되었으며, 이 사건은 12월 2일부터 발생한 것으로 확인</li> <li>✓ Perkeso는 위기 관리 계획을 활성화하고, ICT 부서는 시스템을 성공적으로 다시 통제하며 해커의 초기 시스템 마비 시도를 무력화</li> <li>✓ 다크웹에 유출된 정보의 신뢰성이 의심되었고, Perkeso는 국가 이익을 대상으로 하는 이러한 사이버 공격의 재발을 방지하기 위해 관련 당국과 공유</li> <li>✓ 말레이시아 총리 안와르 이브라힘은 최근 사건들, 특히 사회보장기관 웹사이트 해킹과 같은 사건에 대응하여 정부가 사이버 보안을 강화하기 위한 조치를 취하고 있다고 발표</li> <li>✓ 국가안보회의와 말레이시아 통신 및 다미디어 위원회는 기업들과 협력하여 사이버 보안을 강화하고 사이버 공격을 예방할 계획</li> </ul>
[말레이시아] 사이버 보안 강화	<p>▶ <b>말레이시아 정부는 사회보장기관(Perkeso) 사이트 해킹을 계기로 사이버 보안을 강화할 것을 발표</b></p> <ul style="list-style-type: none"> <li>✓ 말레이시아 총리 안와르 이브라힘은 최근 사건들, 특히 사회보장기관 웹사이트 해킹과 같은 사건에 대응하여 정부가 사이버 보안을 강화하기 위한 조치를 취할 것임을 발표</li> <li>✓ 국가안보회의와 말레이시아 통신 및 다미디어 위원회는 기업들과 협력하여 사이버 보안을 강화하고 사이버 공격을 예방</li> <li>✓ 최근 사회보장기관에 대한 사이버 공격 이후에 나온 것으로, 이에 대한 조사를 위해 사이버 보안 말레이시아, 국가 사이버 안전 기관, 그리고 개인 정보 보호 부서가 참여</li> </ul>
[싱가포르] 데이터 보호를 위한 협력 강화	<p>▶ <b>싱가포르, 데이터 보호를 위한 세계 협력 개척 중</b></p> <ul style="list-style-type: none"> <li>✓ Personal Data Protection Commission (PDPC)과 Mexico's National Institute for Transparency, Access to Information, and Personal Data Protection (INAI)은 두 국가의 국경을 넘어 안전한 데이터의 교환을 위한 협약(MoU)을 체결</li> <li>✓ 이 협력은 싱가포르와 라틴 아메리카 국가 중 처음으로 이루어지는 데이터 보호 기관 간의 협력으로, 호환 가능한 데이터 이전 메커니즘을 개발하고 안전한 데이터 교환을 위한 기술 혁신을 촉진하는 데 중점</li> </ul>

이 슈	주 요 내 용 및 시 사 점
[싱가포르] 디지털 미래 안전하게 보호	<ul style="list-style-type: none"> <li>✓ 이 협정은 또한 정보 교환, 모범 사례 공유, 신형 개인정보 및 데이터 보호 문제에 대한 공동 연구를 포함</li> </ul> <p>▶ <b>ISC2 Secure APAC에서 사이버 보안의 중요성 강조</b></p> <ul style="list-style-type: none"> <li>✓ ISC2 SECURE 아시아 태평양 컨퍼런스에서 싱가포르의 수석 국무장관 Janil Puthucheary는 사이버 보안의 중요성을 강조. 그는 디지털 생태계 간 의존성으로 인한 공급망 리스크의 증가, 주요 인프라를 위협하는 고급 악성 코드의 증가, 그리고 취약점을 해결하기 위한 적시의 보안 패치 적용의 필요성을 강조</li> <li>✓ Puthucheary는 또한 AI 도구를 활용한 사이버 보안 역량을 강화하는 중요성을 언급</li> <li>✓ 싱가포르의 5천만 싱가포르 달러 규모의 Cybersecurity Talent, Innovation, and Growth(Cyber TIG) 계획은 사이버 보안 역량을 전문화하고 사이버 보안 허브로의 지위를 강화하는 것을 목표</li> </ul>
[말레이시아] 할랄 포털 해킹	<p>▶ <b>할랄 포털이 지난 토요일 해킹</b></p> <ul style="list-style-type: none"> <li>✓ 말레이시아의 공식 Halal Portal이 2023년 12월 9일 해킹되어 일시적으로 다운됨</li> <li>✓ 이 사건은 말레이시아 이슬람 개발국(Halal division of the Department of Islamic Development Malaysia, JAKIM)의 할랄 부서에 의해 확인되었으며 신속한 조사와 보안 조치를 위해 사이트는 즉시 다운됨</li> <li>✓ JAKIM은 사이버 보안 사건이 할랄 인증 프로세스에 영향을 미치지 않았으며, 산업 참가자들은 평소처럼 인증 신청을 제출할 수 있다고 재확인</li> </ul>
[싱가포르] 사이버 보안 파트너십 강화	<p>▶ <b>DART와 OffSec, 사이버 보안 환경을 발전시키기 위한 협력 파트너십 체결</b></p> <ul style="list-style-type: none"> <li>✓ DART(Defence Against Real Threats)와 OffSec(Offensive Security)은 사이버 보안 기술을 향상시키기 위한 전략적 협력을 발표</li> <li>✓ 사이버 역량 강화 및 맞춤형 교육 프로그램으로 알려진 DART는 OffSec의 공식 교육 파트너가 됨</li> <li>✓ 이 협력은 사이버 보안 전문가들의 기술과 전문 지식을 혁신적으로 개선하여 정교한 사이버 위협에 효과적으로 대응하는 것을 목표</li> <li>✓ DART는 OSCP(Offensive Security Certified Professional) 자격증을 포함한 OffSec의 자격증을 기업들에게 교육 프로그램의 일부로 제공할 예정</li> </ul>
[말레이시아] 아세안-일본 사이버 보안 협력 강화	<p>▶ <b>말레이시아는 아세안의 사이버 보안 수준 제고를 위하여 일본과의 협력을 강화할 것을 촉구</b></p> <ul style="list-style-type: none"> <li>✓ 말레이시아 총리 Datuk Seri Anwar Ibrahim은 일본의 사이버 공간 전문 지식을 인정하면서 테러, 인신매매 및 기타 국경을 초월하는 범죄와 관련된 사이버 위협으로부터 시민을 보호할 필요성을 강조</li> <li>✓ 그는 일본에게 지적재산권 보호, 데이터 프라이버시 및 위협 인텔리전스와 같은 분야에서 지식과 기술을 공유할 것을 촉구</li> <li>✓ 이 협력 요청은 동남아시아 국가 연합과 일본이 친선과 협력의 50주년을 기념하는 아세안-일본 기념 정상회담의 일환으로 나온 것임</li> </ul>
[싱가포르] 사이버 보안 법 개정안 제안	<p>▶ <b>제안된 사이버 보안법 개정안에 따르면 클라우드 및 데이터 센터 운영자들이 해당 법의 적용 대상에 포함될 예정</b></p> <ul style="list-style-type: none"> <li>✓ 싱가포르의 사이버 보안법 개정안에 따르면 클라우드 서비스 업체와 데이터 센터 운영자는 법 준수 대상에 포함됨</li> </ul>

이 슈	주 요 내 용 및 시 사 점
	<ul style="list-style-type: none"> <li>✓ 사이버 보안법 개정안은 사이버 보안 커미셔너의 업무를 주요 정보통신 기반시설 (CII) 보호 뿐만 아니라 핵심 디지털 인프라 보호 업무를 포함하는 방향으로 확대</li> <li>✓ 이러한 조치는 싱가포르의 연결성, 컴퓨팅 및 데이터 저장에 중요한 역할을 하는 시스템 및 엔티티를 강화하기 위한 것임</li> <li>✓ 제안된 개정안은 Equinix와 Microsoft와 같은 데이터 센터 운영자뿐만 아니라 Google과 Amazon Web Services와 같은 클라우드 서비스 제공업체에도 적용</li> <li>✓ 해당 법안은 사이버 보안법 검토의 일환으로, 1월 15일까지 1개월간의 공개 의견 수렴 기간을 포함</li> </ul>
	<p>▶ <b>[시사점]</b></p> <ul style="list-style-type: none"> <li>✓ 싱가포르는 다양한 사이버 훈련 개최 및 다양한 국가 기관들과의 협력체계를 구축하면서 아세안 지역의 사이버 보안 리더로 자리매김 <ul style="list-style-type: none"> <li>- OT 인프라 보호를 위하여 24개국 200명 이상을 초청하여 침해사고 대응 훈련 개최</li> <li>- Personal Data Protection Commission (PDPC)과 Mexico's National Institute for Transparency, Access to Information, and Personal Data Protection (INAI), DART(Defence Against Real Threats)와 OffSec(Offensive Security)간의 MOU 체결</li> <li>- ISC2와 아시아 태평양 컨퍼런스 개최 등</li> </ul> </li> <li>✓ 말레이시아가 아세안 국가들 중 가장 많은 사이버 침해사고를 당한 것으로 조사됨 <ul style="list-style-type: none"> <li>- 12월에만 사회보장기관(Perkeso), 할랄 포털 등이 침해사고를 경험</li> <li>- Surfshark에 의하면 말레이시아가 2023년 3분기에 세계 8번째 국가로 많은 사이버 공격을 당한 것으로 조사됨</li> </ul> </li> </ul>

# KISA 정보보호 해외진출 전략거점(동남아 북부) 12월 주요동향

2023. 12. 29(금), 한국인터넷진흥원 보안산업단 글로벌협력팀

이슈	주요 내용 및 시사점
[베트남] 사이버 침해 사고	<p>▶ <b>2023년 베트남에서 13,900건의 사이버 공격 발생</b></p> <ul style="list-style-type: none"> <li>✓ 2023년에 베트남에서는 13,900건의 사이버 공격이 발생. 이는 전년 대비 9.5% 증가한 수치임(12월 12일 국가사이버안전센터_NCSC)</li> <li>✓ "gov.vn" 도메인을 가진 국가 기관 및 "edu.vn" 도메인을 가진 교육 기관 등 550개 이상의 웹사이트가 해킹되어 도박 및 베팅 광고 코드가 삽입</li> <li>✓ 랜섬웨어 공격은 전년보다 8.4% 증가한 83,000대 이상의 컴퓨터 및 서버 공격, 주로 정부 기관, 은행 시스템, 금융 기관, 산업 시스템 및 국가 전역의 중요한 시스템을 목표로 함</li> <li>✓ 이 중 대다수는 피싱 공격으로, 전체 공격 횟수의 32.6%를 차지했으며, 27.4%는 컴퓨터 및 서버에 설치된 플랫폼 및 소프트웨어의 취약성을 공격하였고, 25.3%는 기관에서 개발한 웹사이트를 목표로 함</li> <li>✓ 사이버 공격을 방지하기 위해 기관 및 단체는 자체 사이버 보안을 검토하고 네트워크 기기의 안전성을 평가하며, 24/7 모니터링 시스템 도입 필요</li> </ul>
[베트남] 디지털트랜스포메이션 지속 추진 필요	<p>▶ <b>디지털 트랜스포메이션과 지속적인 혁신을 통한 기회 창출 중요성</b></p> <ul style="list-style-type: none"> <li>✓ 베트남 디지털 기술 비즈니스 포럼 2023에서 쩌ن 홍하(Tran Hong Ha) 부총리는 디지털 경제가 4차 산업혁명 시대에 베트남 인적 자원의 품질, 잠재력 촉진의 중요성 강조</li> <li>✓ 부총리는 "디지털 전환은 베트남과 같은 개발도상국과 후진국이 통신 및 디지털 기술 산업이 달성한 성공을 따라잡고 능가할 수 있는 드문 기회"라고 언급</li> <li>✓ 포럼에서 쩌ن 홍하(Tran Hong Ha) 부총리는 경제 및 사회 생활의 모든 측면에서 디지털 전환을 촉진하기 위한 동시적인 정책과 솔루션을 통해 기업이 정부와 함께 디지털 경제를 주도하고 창출해야 한다고 그 중요성을 강조</li> </ul>
[베트남] 디지털 전환 컨퍼런스 개최	<p>▶ <b>디지털 트랜스포메이션을 위한 기업의 경험 공유</b></p> <ul style="list-style-type: none"> <li>✓ 2020년 6월 디지털 정부, 디지털 경제 발전, 경제 경쟁력 향상을 목표로 하는 국가 디지털 전환 프로그램을 공포(~2030년)</li> <li>✓ 중앙은행(SBV)의 통계에 따르면 2022년 말까지 은행 업계는 디지털 전환 활동에 15조 VND 이상을 투자했으며 베트남을 선도적인 디지털 뱅킹 채택국 중 하나로 현재까지 베트남 은행의 최대 96%가 디지털 전환 전략을 개발해 왔으며 은행의 92%가 인터넷과 모바일에서 애플리케이션 서비스를 개발(지난 3-4년 동안 디지털 결제 성장률 40%)</li> <li>✓ MBBank의 2018년부터 IBM Technology Corporation(미국)과의 전략적 협력을 통해 '사람-자원-속도'라는 세 가지 기둥을 통해 개선되고, 그룹의 창의적 문화를 촉진하며, 지속 가능한 디지털 생태계를 발전시켜 옴.</li> <li>✓ MB의 상품은 '셀프서비스'와 '올인원앱'의 트렌드를 따르고, 개인용 MBBank 앱과 기업용 BIZ MBBank 앱의 편의성, 사용 편의성 및 유연성이 확보가 목표</li> <li>✓ MB의 디지털 트랜스포메이션 노력은 고객 규모의 도약으로 인정받아 25년 만에 500만 명이던 고객 수가 2023년에는 2,500만 명으로 증가했습니다(2023년 10월 30일 기준). MB는 디지털 채널에서 16억 건의 거래에 도달했으며, 그 중 MBBank 앱만 하루에 2천만 건의 거래를 기록하였음</li> </ul>

이슈	주요 내용 및 시사점
[베트남] 데이터센터 수요 급증 예상	<p>▶ <b>국내 및 외국기업이 디지털 전환에 따라 데이터센터 수요를 급증시킬 것으로 예상</b></p> <ul style="list-style-type: none"> <li>✓ 컨설팅 회사 아리즈톤은 베트남 DC 시장 규모가 22년 5억 6천만 달러에서 2028년에는 10억 4천만 달러로 2배 가까이 증가할 것으로 예상</li> <li>✓ 베트남 최초의 기술 유니콘인 VNG 코퍼레이션은 호치민의 Tier-III VNG 데이터 센터에 약 1조동(4300백만달러)을 투자 후 향후 더 늘릴 것으로 발표</li> <li>✓ VNG는 데이터스토리지 및 데이터 솔루션 서비스를 제공하는 3대 최신 DC 중 하나로 작년 12월에 오픈(랙당 최대 10KW 용량의 서버를 설치가능한 410개의 랙 보유)</li> <li>✓ 한편, FTP, 비엠텔, VNPT 등은 22년부터 필리핀, 브루나이, 아시아 등 해외 케이블 설치와 DC를 구축하고, 아태 지역의 초고속 인터넷 연결과 데이터 전송을 지연할 계획</li> </ul>
[베트남] 중국 주석 하노이 방문 및 36개 협정 서명	<p>▶ <b>중국 시진핑 주석, 베트남 하노이 공식 방문(23.12.12~13)</b></p> <ul style="list-style-type: none"> <li>✓ 베트남 응우옌 푸 쯑 총서기와 중국 시진핑 국가주석은 베트남 국빈 방문 기간에 중앙 및 지방정부간 36개 협력 협정에 서명</li> <li>✓ 양국 당 부서와 외무성 간 협력에 관한 정치-외교(4개 문서),</li> <li>✓ 범죄 예방, 해상 협력 및 정의에 관한 안보-국방(4개 문서), 정부, 장관 및 기관 차원의 실질적 분야 협력에 관한 문서 24건과 양국 지역 간 협력 4건</li> <li>✓ (주요) 베트남 정보통신부와 중국 상무부의 디지털 경제 분야 투자 협력에 관한 협력 각서</li> <li>✓ 베트남 정보통신부와 중국 공업정보화부 간 통신, 정보기술, 통신 및 디지털 전환 협력에 관한 양해각서</li> <li>✓ 베트남 사회주의 공화국 정보통신부와 중화인민공화국 국가정보관리부 간의 디지털 경제 및 디지털 데이터 협력 강화에 관한 양해각서</li> <li>✓ 베트남 사회주의 공화국 기획투자부와 중화인민공화국 국가발전개혁위원회 간의 양해각서</li> <li>✓ 베트남 기획투자부와 중국 국가국제개발협력총국 간의 인적자원 개발 협력 강화에 관한 양해각서</li> </ul>
[베트남] 디지털 인보이스 관련 세관 포럼 개최	<p>▶ <b>상공연합회(VCCI), 관세청과 2023년 세관 포럼 개최</b></p> <ul style="list-style-type: none"> <li>✓ 재무부는 지난 7년 연속 정보통신기술개발·응용준비지수(ICT Index) 순위에서 선두. 특히 세무 및 관세 분야에서 디지털 전환을 선도</li> <li>✓ 전자세금 신고 시스템은 63/63개 성 및 시와 100% 제휴 세무 부서에 배치. 99% 이상의 기업이 전자 세금 신고, 납부 및 환급을 사용 중. 또한, 세관 분야의 250개의 행정 절차가 국가 원스톱 메커니즘을 통해 수행</li> <li>✓ 관세청은 향후 투명한 관세 법률 시스템을 지속 개선할 것이며 통관 절차 시스템은 스마트 세관의 아키텍처에 따라 디지털 세관 모델을 구축하기 위한 기반으로 재설계될 것임</li> <li>✓ 2025년까지 통관 절차의 100%를 디지털화하고 전자화 예정. 세관 서류문서의 95%가 2025년까지 디지털 데이터로 변환 목표(2030년까지 목표는 100%)</li> </ul>
	<p>▶ <b>시사점</b></p> <ul style="list-style-type: none"> <li>✓ 베트남 디지털 전환 정책에 따라 은행, 데이터센터 등 다양한 서비스 개발이 이루어지고 있으나 실질적인 효과를 보는 사례는 많지 않기 때문에 이런 부분의 컨설팅을 추진하고, 사업화 하는 전략이 필요</li> <li>✓ 베트남 디지털 전환 전략에 맞춰 국내 우수 기술을 전수·전파 시 한국의 국가 보안 기술 유출 우려에 대한 검토도 필요</li> </ul>

## KISA 정보보호 해외진출 전략거점[중남미] 12월 주요동향

2023. 12. 29(금), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[카리브해] 카리브해-미국 고위급 안보협력 공동성명	<p>▶ <b>미국, 카리브 공동체 (CARICOM) 사이버보안 부문을 포함한 안보 협력 협력 사항 재확인</b></p> <ul style="list-style-type: none"> <li>✓ 워싱턴 D.C.에서 열린 카리브해-미국 안보 협력 대화에서 카리브 해역 안보 구상(CBSI) 파트너십(2010년 서명)에 대한 협력을 재확인</li> <li>✓ CBSI를 통한 파트너십을 유지하여 불법 인신매매를 실질적으로 줄이고, 공공 안전 및 보안을 강화하고, 카리브해에서 청소년 범죄 및 폭력을 예방하는 세 가지 공동 목표를 추진</li> <li>✓ 2023-2024년 카리브해에서 불법 인신매매를 줄이기 위한 보다 효과적인 파트너십과 구체적인 조치를 구축하기 위해 계속 협력</li> <li>✓ 동 세부 협력 내용은 MDA(Maritime Domain Awareness) 기술을 사용하여 불법 네트워크를 식별 및 중단하고 마약, 총기, 인신매매, 이주민 밀수를 포함한 지역 전역의 불법 해양 활동을 보다 효과적으로 탐지하는 등 사이버 범죄를 대응하기 위한 정보 공유 및 협력 등을 포함</li> <li>✓ 또한 범죄 조직 대응을 위해 국가 사이버보안 전략을 개발하고 제정하도록 장려하며 사이버 보안 인식, 정책 입안, 네트워크 방어 및 사고 대응 능력을 강화하기 위해 사이버 보안 교육 및 훈련을 촉진 예정</li> <li>✓ 기존 법률, 국가 및 지역 전략을 검토하고 필요에 따라 업데이트 및/또는 개선하여 기존 및 새로운 사이버 위협에 대처할 수 있는 능력을 강화하기 위한 협력 내용도 포함</li> <li>✓ CARICOM IMPACS가 사이버 범죄 및 사이버 주요 기반시설 보호와 관련된 문제를 해결하기 위한 협조 및 특별 가상 회의를 개최할 것을 포함</li> </ul>
[칠레] 시민 안전위원회 사이버 보안 기본법 승인	<p>▶ <b>주요기반 시설 보호방안을 포함한 사이버 보안 기본법 승인</b></p> <ul style="list-style-type: none"> <li>✓ 시민안전위원회(Citizen Security Commission)는 사이버 보안 및 주요기반 시설에 관한 기본법(Framework Law on Cybersecurity and Critical Information Infrastructure) 제정 시작</li> <li>✓ 동 법안은 안보에 관한 정부의 우선 입법 순위를 반영한 프로젝트의 일부이며 국가 기관의 사이버 보안 조치를 구조화, 규제 및 조정하기 위한 제도적 프레임워크, 원칙 및 일반 규정을 정립</li> <li>✓ 또한 사이버 보안 사고에 대한 예방, 억제, 해결 및 대응을 위한 최소 요구 사항을 설정</li> <li>✓ 이와 함께 국가 기관의 권한과 의무를 설정하고 있으며 또한 민간 기관의 의무와 침해에 대한 통제, 감독 및 책임 메커니즘을 정의</li> <li>✓ 이 제도적 틀의 목적은 개인과 그 가족의 사이버 보안에 대한 권리의 보호, 증진 및 존중을 보장하기 위함</li> <li>✓ 이를 위해 암호화 도구를 포함하여 네트워크 및 컴퓨터 시스템에 포함된 정보의 무결성, 기밀성, 가용성 및 복원성을 보장하기 위해 내용을 포함</li> <li>✓ 동 법안은 현재 하원 재정위원회에서 검토 중임</li> </ul>



이 슈	주 요 내 용 및 시 사 점
[쿠바] 통신 사이버 보안 워크숍 개최	<p>▶ <b>쿠바 통신 회사 및 정부기관은 공동으로 통신 기술 보안 인증 구현을 위한 사이버 보안에 관한 워크숍 개최</b></p> <ul style="list-style-type: none"> <li>✓ 11월 29일(ACN) 쿠바 하바나에서 악성 프로그램의 확산에 의한 사이버 위협이 증가함에 따라 전문가와 정보 통신 기술의 보안 인증을 구현하고 쿠바 기관의 더 효율적인 메커니즘과 통제를 구현하기 위해 사이버 보안 워크숍 개최</li> <li>✓ 쿠바 통신 회사(Telecommunications Company of Cuba)가 후원하고 제2차 국가 사이버 보안 회의(II National Cybersecurity Conference)의 일환으로 진행된 이 행사는 모로-카바냐(Morro-Cabaña) 단지에서 3일에 걸쳐 진행</li> <li>✓ 동 회의는 네 가지 1.암호화, 2.통신 사기, 3.디지털 보안 및 4.법적 프레임 워크를 주요 주제로 다룸</li> <li>✓ 사이버 보안을 강화하기 위한 디지털 인증서와 서명 및 기업이 사이버 보안과 관련된 사건을 다루고 위험성에 대한 인식을 제고해야하며, 경제 수익을 창출하기 위해 이 분야에서 수출할 수 있는 서비스를 설계할 것을 권장</li> <li>✓ 통신부 장관 Mayra Arevich Marin은 바이오 정보 보안과 관련된 조직, 회사 및 단체의 광범위한 참여를 강조하고 특히 컴퓨터 공학 및 사이버 보안 경력을 쌓은 인력의 필요성을 강조</li> <li>✓ 사이버 보안 역량을 강화하기 위해 지속적인 촉진 방안 및 인프라와 정보 기술의 효율적이고 책임 있는 사용에 대한 교육 및 훈련 등 인식 제고를 강화하기 위해 무엇보다 올바른 문화 형성이 필요하다고 강조</li> </ul>
[칠레] 화웨이 클라우드 회의 개최	<p>▶ <b>2022년 라틴아메리카 기업의 62%가 공공 클라우드 서비스에 예산의 최대 25%를 투자</b></p> <ul style="list-style-type: none"> <li>✓ Huawei Cloud Chile는 회의 개최를 통해 클라우드와 AI를 도구로 사용하여 기업의 디지털 변혁을 가속화할 수 있는 방안에 대해 논의</li> <li>✓ Huawei Cloud Chile의 총책임자인 Jason Jin은 "Huawei Cloud에서는 클라우드와 AI 사용 솔루션은 효율성, 비즈니스 창출 및 성장을 보장한다."라고 언급</li> <li>✓ 한편, Aisén Etcheverry 과학기술지식혁신부 장관은 라고스 대통령 정부가 디지털 기술에 대한 중요성을 강조하고 관련된 이니셔티브를 지속적으로 개발해옴에 따라 칠레가 중남미 지역 디지털화 강자가 될 수 있었음을 강조</li> <li>✓ 컨설팅 회사 IDC(International Data Corporation, 정보 기술 전문 출판사)가 수행한 연구에 따르면 칠레를 포함한 중남미 기업 예산의 상당 부분이 클라우드에 사용되었으며, 이는 향후 몇 년 동안 증가할 것으로 예상</li> <li>✓ IDC의 중남미 통신 관리자 겸 제품 리더인 José Ignacio Díaz는 "이 지역 기업의 62%가 2022년에 예산의 1~25%를 퍼블릭 클라우드 서비스에 투자했습니다"라고 설명</li> <li>✓ 또한 중남미 AI 소프트웨어 시장이 2026년까지 CAGR 24.8%로 성장할 것이며 규모와 성장 측면에서 상위 3대 AI 산업은 금융, 보험, 소매라고 언급</li> <li>✓ EY 칠레의 데이터 컨설팅, 분석, 인공지능 파트너인 파트리시오 코프레(Patricio Cofré)는 Cloud with AI 덕분에 개발 기회와 수익 개선 기회에 대해 "분석 도구를 활용해 수익을 최적화하고 최첨단 생태계에 투자해 운영과 경험을 개선하고 있다"고 언급</li> </ul>



이 슈	주 요 내 용 및 시 사 점
	<ul style="list-style-type: none"> <li>✓ 같은 맥락에서 화웨이는 '모든 것을 서비스로'라는 개념을 통해 클라우드 활용을 극대화하고 새로운 비즈니스 기회를 모색할 수 있다고 설명</li> <li>✓ Huawei Cloud Latam의 CTO인 Eduardo Hernández는 클라우드를 집중적으로 사용하고 있는 사람들은 위기 상황을 최소화할 수 있다고 언급</li> <li>✓ 이미 클라우드 및 AI와 협력하고 있는 기업으로는 Unimarc, Alvi, Mayorista 10 및 Super 10 슈퍼마켓을 소유한 칠레 소매 회사인 SMU 등이 있음</li> <li>✓ SMU의 디지털 및 기술 리더인 Eduardo Herrera는 클라우드 기반 전자 상거래 기술은 고객의 요구에 따라 성장 가능했음을 언급하며 화웨이는 최고 수준의 보안, 낮은 대기 시간, 좋은 응답 시간을 갖추고 있다고 설명</li> <li>✓ 화웨이는 전 세계 날씨를 예측하는 최초의 AI 모델인 Pangu Weather를 출시했으며 이 모델은 지난 40년 동안 수집된 정보를 바탕으로 클라우드에 저장된 데이터 기반으로 예측 결과 도출</li> <li>✓ 이번 회의에는 250명이 넘는 인원이 참석하여 디지털 혁신에 대해 논의</li> </ul>
[파나마] 사이버 보안 주간 행사 개최	<p>▶ <b>정보보안 주간을 찾아 사이버 보안 기술 및 정보, 모범사례 공유</b></p> <ul style="list-style-type: none"> <li>✓ 카를로스 곤잘레스 (Carlos González) 파나마 경제부 차관은 2023년 정보보안 주간을 맞아 워크숍 개막식에서 "당신은 사이버보안에서 첫 번째 방어자"라는 슬로건 아래 컴퓨터 보안, 기밀 유지 및 데이터 보호에 대한 모범 사례를 공유하고 구현하는 문화를 직원들에게 심어주는 것이 중요 강조</li> <li>✓ 데이터 보호, 사회 공학, 사이버 위험 및 이를 방지하고 완화할 수 있는 조치에 대한 중요성을 인식하고 마주하고 있는 위험성 관련 기본적이고 유용한 도구와 지식을 제공하기 위해 동 워크숍 진행</li> </ul>
[도미니카공화국] 소외 지역 대상 디지털 교육실 개관	<p>▶ <b>소외 지역 내 디지털 교실 개관을 통해 디지털 격차 축소</b></p> <ul style="list-style-type: none"> <li>✓ HISPASAT(스페인 위성통신 기업)는 도미니카 공화국 정부에 세 가지 원격 교육 시범 프로젝트를 제공하여 산 페드로 데 마코리스 소외 지역 내 위성 연결을 통해 디지털 격차를 축소하기 위한 교육을 활성화함 <ul style="list-style-type: none"> <li>※ HISPASAT : 광대역 및 연결 서비스를 제공하는 통신 회사로 DTH (Direct-to-Home Television) 및 HDTV(High Definition Television)의 디지털 플랫폼을 포함하여 스페인어와 포르투갈어로 된 시청각 콘텐츠의 보급 및 배포를 주도</li> </ul> </li> <li>✓ 이 협력은 글로벌 기업과 Dominican Institute of Telecommunications (Indotel) 간에 관리되었으며, 위성과 연결 가능한 디지털 교실을 개관하여 앞서 언급한 지방의 300명의 학생들에게 혜택을 줄 예정</li> <li>✓ 이 원격 교육 파일럿 프로젝트를 위해 소외 지역에 위치하고 인터넷 연결이 되지 않은 학교가 선택되었으며 디지털 교실에는 교사용 노트북, 기기 보관 및 충전용 캐비닛, SmartTV, 교육 관리 소프트웨어, 학생용 태블릿, 교사용 디지털 기술 과정 등이 포함됨</li> <li>✓ 동 프로젝트는 HISPASAT의 기부를 통해 진행되었으며 도미니카 공화국 교육부(MINERD)에서 제공하는 교육 콘텐츠를 저장하고 장소에 구애받지 않고 교육 진행 가능</li> <li>✓ 또한 HISPASAT는 학교 디지털 교육 시설 설립 뿐 아니라 지역 사회를 위한 WiFi 연결 서비스를 가능하게 하여 학교가 문을 닫는 경우 학생과 교사가 인터넷 및 교육 콘텐츠에 더 쉽게 접근할 수 있도록 지원</li> </ul>

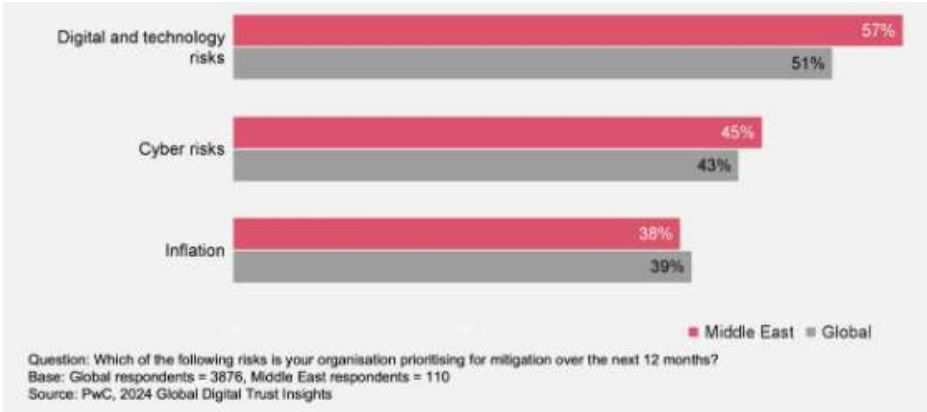
이 슈	주 요 내 용 및 시 사 점
	<ul style="list-style-type: none"> <li>✓ Indotel의 이사회 회장인 Nelson Arroyo는 디지털 교실을 통해 젊은이들이 가상 도구를 배우고 활용을 통해 더 나은 기회를 창출할 수 있기를 희망</li> <li>✓ HISPASAT의 CEO인 미겔 앙헬 판두로(Miguel Ángel Panduro)는 "우리의 원격 교육 솔루션은 중남미 지역 내 교육의 디지털 전환을 보장하고 새로운 세대를 정보 사회와 연결할 것이며, 동 이니셔티브의 성공적인 운영 및 수요가 있는 타 지역 내 추가 지원할 수 있기를 희망합니다"라고 언급</li> <li>✓ 인터넷 연결성은 사회의 평등한 발전을 촉진하는 근본적인 도구이나 도시와 농촌 간 인프라 배치 비율차이가 커짐에 따라 디지털 격차가 벌어지고 있음</li> <li>✓ IDB의 2022년 광대역 개발 지수(IBDA) 연례 보고서에 따르면 도미니카 공화국의 초등학교 중 23.16%만이 인터넷에 접속할 수 있는 반면, 중미와 카리브해는 28.30%, 이베로아메리카 전체는 39.48%가 인터넷에 접속할 수 있음</li> <li>✓ 농촌 지역에서는 전반적 인터넷 접속 비율이 더 낮음에 따라, 교육의 디지털 전환을 위한 공공 정책을 시행이 필요</li> </ul>
<p><b>[카리브해] 12월1일 부터 데이터보호 법률 시행</b></p>	<p>▶ <b>기업 내 데이터 보호를 강화하기 위한 기업 정책 필요</b></p> <ul style="list-style-type: none"> <li>✓ FBI로부터 기술 승인을 받은 Simply Secure Group 사이버보안 기업 CEO인 Kevin Gordon는 카리브해 기업의 데이터보호를 강화하기 위해 정부 정책이 필요하다고 강조</li> <li>✓ 그는 최근 개최된 TechBeach Retreat 이벤트에서 카리브해, 라틴 아메리카 및 북미 전역에서 69억 달러 이상의 사이버 위협을 차단했으며 카리브해에 지역에서만 38억 달러의 위협을 대응했음을 강조</li> <li>✓ 그는 독일의 독립 기관인 AV Institute의 데이터를 인용하여 전 세계적으로 매일 거의 300,000건의 사이버 위협이 생성되고 있으며 그 중 282,000건은 위협 인텔리전스 데이터베이스에서 식별되지 않다보니 기업들은 감염여부를 인지하지 못하는 것이 위험하다고 경고</li> <li>✓ 고든은 많은 기업 중 상당수가 랜섬웨어 공격으로 데이터를 도난 당하기 6개월 전 바이러스에 이미 감염되었다고 언급</li> <li>✓ 그는 이들 중 다수가 12월1일 부터 시행된 데이터 보호법의 시행에 대한 준비가 되어 있지 않다고 설명</li> <li>✓ 이에 기업들은 우선 사이버 보안 계획을 수립하고 사고 대응을 위한 대응방안 절차가 필요하다고 언급</li> <li>✓ 또한 명확한 계획 및 정책을 통해 기업은 사이버 보안을 위한 통제와 적절한 커뮤니케이션 계획, 적절한 법적 계획, 위기 발생 시, 대응 절차 문서화 마련 등을 촉구</li> <li>✓ 기업이 내부적으로 자체 내부 사이버 보안 통제 및 정책을 개발하고 사고 발생 시 책임이 있음을 인지한 후 데이터 유출 피해자에게 고지 하는 시스템 및 데이터 접근 권한에 대한 명확한 기준 마련이 필요</li> <li>✓ 위기가 닥치거나 랜섬웨어 공격이 발생 시 취하는 조치 및 사고를 신고하는 기관, 피해 최소화를 위한 방안 마련 등이 중요</li> <li>✓ 공격을 받을 시, 가장 잘 대응하고 회복할 수 있는 기업은 첫째, 어떤 일이 발생했을 때 무엇을 해야 하는지 정의하는 정책을 가지고 있는 회사라는 것을 강조하며 카리브해 환경에 맞는 내부 정책 마련을 권장</li> </ul>

이 슈	주 요 내 용 및 시 사 점
[파나마] 사이버 보안 주간 행사 개최	<p>▶ <b>정보보안 주간을 찾아 사이버 보안 기술 및 정보, 모범사례 공유</b></p> <ul style="list-style-type: none"> <li>✓ 카를로스 곤잘레스 (Carlos González) 파나마 경제부 차관은 2023년 정보 보안 주간을 맞아 워크숍 개막식에서 "당신은 사이버보안에서 첫 번째 방어자"라는 슬로건 아래 컴퓨터 보안, 기밀 유지 및 데이터 보호에 대한 모범 사례를 공유하고 구현하는 문화를 직원들에게 심어주는 것이 중요 강조</li> <li>✓ 데이터 보호, 사회 공학, 사이버 위험 및 이를 방지하고 완화할 수 있는 조치에 대한 중요성을 인식하고 마주하고 있는 위험성 관련 기본적이고 유용한 도구와 지식을 제공하기 위해 동 워크숍 진행</li> </ul>
[칠레] 상원, 사이버 보안 관련 법적 프레임 워크 승인	<p>▶ <b>정보보안 주간을 찾아 사이버 보안 기술 및 정보, 모범사례 공유</b></p> <ul style="list-style-type: none"> <li>✓ 칠레 상원은 사이버 보안 및 주요기반시설 보호에 대한 새로운 법적 프레임 워크를 만드는 법안을 승인</li> <li>✓ 찬성 42표로 동 법안은 가브리엘 보릭 대통령의 서명을 받은 후 제정 예정</li> <li>✓ 동 법안의 기반이 된 이니셔티브는 2022년 통과했으며, 사이버 보안을 강화하고, 대응 작업의 확대 및 강화, 디지털 보안에 대한 공공 문화 형성, 공공 및 민간 부문의 긴급 상황 훈련, 사이버 공간에서 사람들의 안전을 보호하기 위한 제도적 틀을 구축하는 것을 목표로 함</li> <li>✓ 칠레는 글로벌 사이버 보안 지수에서 74위를 차지했으며 미주 지역에서는 미국, 캐나다, 멕시코, 브라질, 우루과이, 도미니카 공화국에 이어 7위를 차지</li> <li>✓ 종 법안은 규제, 감독 및 제재 권한을 가진 국가 사이버 보안 기관(ANCI)의 창설을 규정하고 있으며 사이버 보안에 관한 다부문 위원회(Multisectoral Council on Cybersecurity) 및 CSIRT(National Computer Security Incident Response Team), 부문별 CSIRT 구현에 대해 포함</li> <li>✓ 합동 국방 및 안보 위원회 의장인 케네스 퓨(Kenneth Pugh) 상원의원은 이 법안이 공공-민간 협력을 기반으로 사고에 대한 예방, 억제, 해결 및 대응을 개선하기 위해 위험 관리 및 사이버 보안 표준 구현을 촉진하는 거버넌스 모델 구축을 포함하여 사이버 보안과 관련된 의무 및 처벌을 규정할 것이라고 설명</li> <li>✓ 또한 최근 정부는 2028년부터 시행될 사이버보안전략을 발표했으며, 탄력적인 인프라 구축, 국민을 위한 권리 강화, 사이버 보안 문화 형성, 국제 협력, 과학 연구 촉진이라는 다섯 가지 구체적인 목표를 제시</li> </ul>
[파나마] 당국, 물류 부문 사이버보안 위원회 창설 제안	<p>▶ <b>물류 및 운송 부문 사이버 범죄 대응을 위한 위원회 창설 논의</b></p> <ul style="list-style-type: none"> <li>✓ 사이버 범죄에 맞서 물류 및 운송 부문을 강화하기 위해 ANA(National Customs Authority)는 민간 부문 구성원과 함께 물류 및 운송 부문의 기업과 정보, 경험 및 모범 사례를 공유하기 위해 사이버 보안 위원회를 구성할 필요성을 제기</li> <li>✓ 성명서를 통해 동 이니셔티브가 세관의 안전한 무역을 돕기 위한 의사 결정에 기여할 수 있다고 강조</li> <li>✓ 발보아 항구에서 동 목적을 위한 첫 번째 회의가 개최되었으며 항구 대표, 파나마 기업 임원 협회(APEDE), 정부 혁신 기관(AIG), 해양 당국 및 Fortinet 회사 경영진은 침입 및 공격으로부터 비즈니스 네트워크를 보호하는 것의 중요성 및 최적의 네트워크 성능을 보장할 수 있는 방안을 논의</li> </ul>
[코스타리카] '24년 금융 부문 사이버 보안 규칙 적용 예정	<p>▶ <b>물류 및 운송 부문 사이버 범죄 대응을 위한 위원회 창설 논의</b></p> <ul style="list-style-type: none"> <li>✓ 2024년 금융 부문 고객을 보호하기 위해 은행 사이버 보안에 대한 새로운 규칙을 만드는 것을 포함하는 일련의 규제 개혁이 시행될 예정</li> </ul>

이 슈	주 요 내 용 및 시 사 점
	<ul style="list-style-type: none"> <li>✓ 또한 투자 펀드 운영에도 근본적인 변화가 있을 예정</li> <li>✓ Rocío Aguilar, 금융 기관(Sugef) 및 연금(Supén)의 일반 감독 책임자 및 증권 총괄 감독(Sugeval) 및 보험 감독(Sugese)의 Tomás Soley는 월요일 기자 회견에서 내년에 시행될 수정 사항의 세부 사항을 공개</li> <li>✓ 특히 컴퓨터 보안 측면에서 코스타리카의 모든 감독 기관, 즉 은행, 연금 운영자, 보험 회사, 중개 회사 및 투자 펀드에 새로운 규칙이 적용될 것이라고 설명</li> <li>✓ 이 개혁안은 금융 기관이 사이버 보안 사고의 탐지, 예방 및 대응을 위한 모니터링 및 조기 경보를 위한 인프라를 개발하도록 의무화할 예정</li> <li>✓ 사이버 보안 결정은 기업 지배 구조에서 결정되는 만큼 조직에 대해서도 규정</li> <li>✓ 또한, 국가 금융 시스템 감독 위원회(Conassif)가 디지털 뱅킹 채널을 사용할 때 사람들을 인증하는 방법을 통합하여 사이버 사기에 대처하는 도구에 대해 논의할 것이라고 언급</li> </ul>
	<p>▶ <b>시사점</b></p> <ul style="list-style-type: none"> <li>✓ 칠레, 멕시코, 브라질과 같은 중남미 내 강대국은 클라우드 서비스 및 AI 솔루션 도입 등을 고려한 인식제고 및 법안 마련이 활발</li> <li>✓ 상대적으로 경제규모가 작은 중미 국가들의 경우 디지털 격차 해소 등을 위한 인식 제고 워크숍을 개최</li> <li>✓ 중남미 지역 내 사이버보안 및 데이터보호 관련 법률이 이행되고 있으나, 이를 준수하기 위한 가이드가 부족한 상황. 이에, 향후 중남미 국가 대상 협력 시, 사이버 보안 뿐 아니라 개인정보보호 정책 및 인식 제고에 관련된 협력 고려 필요</li> </ul>

# KISA 정보보호 해외진출 전략거점(중동아프리카) 12월 주요동향

2023. 12. 29(금), 한국인터넷진흥원 보안산업단 글로벌협력팀

이슈	주요 내용 및 시사점
<b>[중동] 중동지역 디지털 신뢰관련 조사결과</b>	<p>▶ <b>Digital Trust Insights 2024 결과 사이버보안의 중요성 강조</b></p> <ul style="list-style-type: none"> <li>✓ 중동 지역의 응답자 110명을 포함하여 일부 최대 글로벌 기업의 비즈니스 및 기술 임원 3,876명을 대상으로 한 2024년 Global Digital Trust Insights 설문조사에서는 사이버 위험 문제의 완화 등이 중요하다고 함</li> <li>✓ 중동 지역은 그 어느 때보다 기업이 디지털 비즈니스 모델로 전환 중에 있고 이에 따라 조직, 파트너 및 고객 간에 더 많은 데이터가 생성되고 공유되고 디지털화가 증가한다는 것은 기업이 새로운 디지털 취약성에 노출된다는 것을 의미하며, 사이버 보안과 디지털 신뢰에 대한 효과적인 접근 방식이 그 어느 때보다 중요해짐</li> <li>✓ 응답자 중 77%는 2024년 사이버 예산 증액 예정</li> <li>✓ 53%가 주로 연결된 장치에 대한 공격을 우려하고, 45%가 사이버 위험 감소를 최우선 과제로 삼고 있음</li> <li>✓ 중동 지역 응답자의 45%는 사이버 위협의 위험성을 우선과제로 삼고 있으며 (전 세계 43%보다 우려) 이는 경제적 변동성, 인플레이션 및 지정학적 위험보다 높게 나타남</li> <li>✓ 전년도 PwC 글로벌 CEO 설문조사에서는 4위 였으나 이번 조사에서는 위험 우선순위에서 디지털 및 기술 위험에 이어 두 번째를 차지</li> <li>✓ 그리고 응답자들의 생각에는 디지털 및 기술 위험이 사이버 위험과 불가분의 관계에 있다고 생각</li> <li>✓ 오늘날의 비즈니스 환경에서는 주요 사이버 위협을 조명하지 않고는 디지털 혁신이나 재창조를 논의할 수 없다고 함</li> <li>✓ 중동의 급속한 경제 성장, 향상된 사이버 인식, 중요 인프라 보호를 위한 투자로 인해 중동은 계속해서 더욱 정교해지고 발전되는 사이버 공격에 대한 탄력성을 갖게 되었고 이에 대한 대비가 필요하다고 여김</li> </ul>  <p>출처: pwc.com</p>
<b>[이란] 이란 주유소 해킹으로 서비스 중단</b>	<p>▶ <b>이스라엘과 연관된 해커들이 이란 전역의 주유소 서비스 중단</b></p> <ul style="list-style-type: none"> <li>✓ 이스라엘과 관련이 있는 해커들이 이란 전역의 주유소 서비스를 방해하는 사이버 공격을 수행했다고 이란 국영 TV와 이스라엘 현지 언론이 보도</li> </ul>

이 슈	주 요 내 용 및 시 사 점
<p>[사우디] 주요 IT기업이 사우디의 사이버보안 등 디지털화를 지원</p>	<ul style="list-style-type: none"> <li>✓ 이란 주유소의 약 70%에서 서비스가 중단됐으며 외부 간섭이 원인일 수 있다고 함</li> <li>✓ 이란 국영 TV 뉴스는 프레데토리 스파로우(Predatory Sparrow) 그룹이 이번 혼란의 배후에 있다고 주장했다고 보도</li> <li>✓ 이란 국영 언론은 과거에도 해커 그룹이 이란의 주유소, 철도 네트워크, 철강 공장에 대한 사이버 공격을 했다고 덧붙였으며, 주유 중단은 이란에서 발생한 대규모 사이버 공격으로 인해 연료 판매가 중단된 2021년 이후 첫 번째 사건이라고 함</li> <li>✓ 이스라엘은 아직 이란의 사이버 공격에 대해 공식적 언급은 하지 않은 상태</li> <li>▶ 미국의 IT기업 델은 기술 포럼 개최를 통해 사우디아라비아의 혁신을 지원</li> <li>✓ Dell Technologies는 사우디아라비아에서 포럼을 11월 19일 리야드에서 개최하여 사우디아라비아의 조직이 새로운 디지털 우선 기회를 포착하고 인공 지능, 멀티 클라우드, 데이터 센터, 사이버 보안 등의 분야에서 최신 기술 솔루션을 탐색할 수 있도록 지원</li> <li>✓ 이는 디지털 혁신이 사우디 내 기업의 중심 무대로 계속 자리잡고 있는 시기에 적절히 개최되었으며 Dell의 최신 혁신 지수 연구에 따르면 사우디아라비아 기업의 대다수(93%)가 혁신 목표를 실현하는 데 도움이 되는 기술을 적극적으로 찾고 있다고 함</li> <li>✓ 델은 사우디의 기업과 조직이 비즈니스 혁신 이니셔티브를 가속화하도록 도울 것이며 보다 나은 미래를 만들어 가는 과정에서 고객과 함께 새로운 영역을 탐색할 수 있는 기회를 제공할 것이라고 함</li> </ul>
	<p>▶ 시사점</p> <ul style="list-style-type: none"> <li>✓ 중동지역은 급속한 디지털화 등에 대비한 사이버 위협의 우려가 커지고 있으며 이에 대한 대비가 필요한 시점</li> <li>✓ 이스라엘-이란 간 분쟁 등에 사이버 공격이 지속적으로 이루어지고 있어 사이버 보안을 위한 적극적인 대응이 필요</li> <li>✓ 델 등 주요 IT기업은 사우디의 디지털 전환과 사이버 보안 등 기술적인 부분에 있어 혁신을 지원하고 있고 이를 통해 사우디에서 해당 분야를 선점하고자 하는 노력을 지속적으로 하여 우리 기업도 지속적인 진출 기회를 마련할 필요가 있음</li> </ul>