미래 국가안보의 중심축이 될 '사이버 보안'

창과 방패의 싸움은 디지털 영역에서도 계속된다.

글 Pedro Polandrani 사진 SHUTTERSTOCK

코로나 이후 심화된 리스크, 사이버 보안

2020년 초 발생한 코로나 사태를 3년째 겪는 동안 일상에 많은 변화가 있었다. 재택근무가 일상화되고, 대면회의보다 화상회의가 더 자연스러워졌으며, 외부 여가생활보다는 내부 여가생활, 특히 온라인 액티비티가 증가하였다. 식당과 상점은 온라인/비접촉 결제 서비스를 추가하였고 많은 서비스가 비대면으로도 가능하도록 바뀌었다.

현재 세계적으로 매일 약 250경 바이트(2.5×1,018바이트, 영화 하나가 2.5기가 바이트라고 가정 시 10억 편)라는 어마어마한 양의 데이터가 생산/재생산되고 있다.

이 기간 동안 전 산업에 걸쳐 디지털화가 가속화됨을 우리는 피부로 느낄 수 있게 되었고 이에 따라 정부, 기업 그리고 개인에 대한 사이버 공격 역시 급격하게 증가하고 있다.

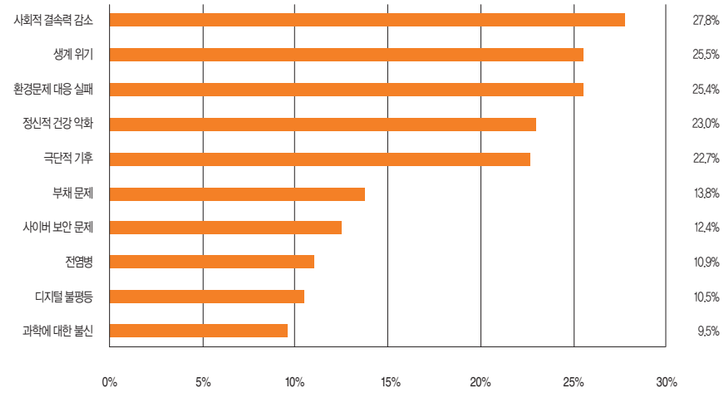
세계경제포럼에 따르면 코로나 이후 심화된 리스크 중에 사이버 보안 문제가 7위를 기록하였다. 이는 전염병보다 더 큰 리스크인 것이다.

팬데믹 이후 락다운 조치가 완화되고 일상생활로 돌아가고는 있지만 설문조사에 따르면 여전히 근무자의 45% 이상이 재택과 출근을 병행하는 하이브리드 형태의 근무를 지속하고 있다

> 세계경제포럼에 따르면 코로나 이후 심화된 리스크 중에 사이버 보안 문제가 7위를 기록하였다. 이는 전염병보다 더 큰 리스크인 것이다.

코로나19 이후 심화된 리스크 순위

자료 : WEF, 미래에셋자산운용



개인, 기업, 정부의 사이버 공격 피해 증가

사이버 보안회사인 노턴(Norton)의 2021년 2월 설문조사에 따르면 10개국 설문자 1만 30명 중 53%가 사이버 공격을 받은 경험이 있다고 밝혔다. 이는 2019년 36% 대비 급격한 상승세를 보인 것이다. 향후 디지털 자산, VR, AR, 메타버스, 사물인터넷(IoT) 등 다양한 혁신 기술이 본격적으로 발전하고 보편화될 경우, 데이터 급증에 따라 개인에 대한 사이버 위협이 더 증가할 것으로 보인다.

사이버 보안의 중요성은 최근 러시아-우크라이나 전쟁, 북한의 해킹에서도 강조되었다. 러시아는 우크라이나의 군, 경찰 등 정부기관과 은행 등에 연쇄적인 디도스 공격을 하여 국가시설의 디지털 보안 체계에 큰 타격을 주었다.

블록체인 데이터 플랫폼 회사인 체인어낼러시스(Chainanalysis)에 따르면 2021년 북한은 암호화폐 거래소 해킹을 통해 비트코인 등 디지털 자산을 4천만 달러 이상 탈취했다. 2022년 4월에는 비디오 게임회사를 해킹하여 한 번에 6천만 달러를 탈취했다고 FBI가 밝히기도 했다. 지금도 전 세계는 총성 없는 사이버 전쟁을 치르고 있다.

국가별 해킹 평균금액을 보면 모든 국가에서 2020년보다 2021년에 피해액이 증가하였다. 그중 미국의 피해액이 가장 크고 그 다음으로 캐나다, 독일, 일본 순이다. 한국의 피해액은 글로벌 평균보다는 조금 적다.

특히 2021년에는 매월 기업에 대한 해킹이 있었다. 미국 최대 송유관 회사인

Pedro Palandrani

현재 Global X에서 성장테마형 ETF와 혁신기술 부문 리서치를 담당하는 리서치 애널리스트로 활동 중이다. 베네수엘라의 UCAB를 졸업하고 세일럼 주립대학교의 버톨론 경영대학원에서 MBA를 취득했다.

GLOBAL X

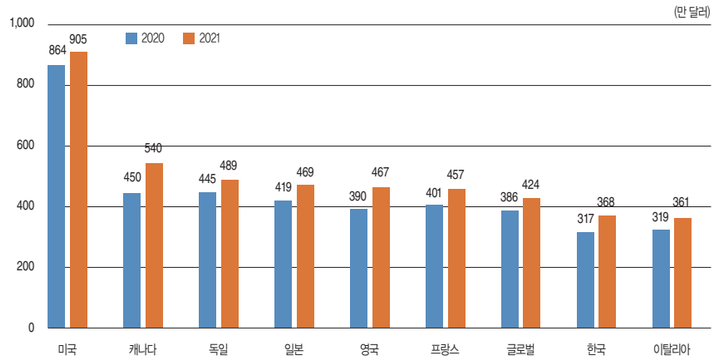
Global X는 전 세계 ETF시장의 70% 이상을 차지하는 미국에서 라이징 스타로 주목받는 대표적 ETF운용사 가운데 하나로, 2008년 설립되었다. '평범한 ETF를 넘어서'(Beyond Ordinary ETF)란 모토 아래, 로봇 및 인공지능 종목에 투자하는 BOTZ ETF, 빠르게 성장하는 클라우드 산업에 투자하는 CLOU ETF 등 테마형, 인컴형, 액티브 채권형으로 다양하게 차별화된 상품을 공급하고 있으며, 2020년 말 기준 230억 달러의 자산을 운용하고 있다.

컬로니얼 파이프라인(Colonial Pipeline)은 사이버 공격으로 인해 440만 달러의 피해를 입었고, 세계최대 육류가공업체인 JBS도 사이버공격으로 인해 공장 여러 곳을 폐쇄해야 했다. 그 외에도 사이버공격은 크고 작게 계속 이어지고 있다.

최근 가장 많은 해킹 공격 패턴 중의 하나가 랜섬웨어다. 랜섬웨어는 그럴싸한(예를 들어 넷플릭스 서비스 연장 유무 확인) 이메일을 보내서 첨부파일 또는 피싱 링크 클릭을 유도한 후 클릭할 경우 악성코드가 해당 컴퓨터에 다운로드되도록 만든다. 해커는 컴퓨터 시스템을 감염시키고 파일을 암호화시켜 접근을 제한한다. 그리고 이들은 암호를 풀어주는 대가로 기업에 금전적 요구를 한다. 앞서 예를 들었던 컬로니얼과 JBS도 랜섬웨어의 피해자다.

이러한 랜섬웨어 공격에 따른 피해액은 최근 3년간 급격하게 증가하였다. 2021년 피해액은 약 200억 달러로 추정이 되는데, 이는 5년 전인 2016년 대비 무려 20배가 많은 액수다. 더욱 위협적인 것은 현재 파악된 규모만 200억 달러라는 것이다. 투자자금 이탈 또는 주가 하락 등의 이유로 사실 공개를 꺼리는 기업이 많기 때문에 공개된 사이버 공격 사례는 일부에 지나지 않을 수 있고, 실제 피해액은 집계된 것보다 훨씬 많을 수 있다는 점에 유의해야 한다.

국가별 해킹 피해 평균금액



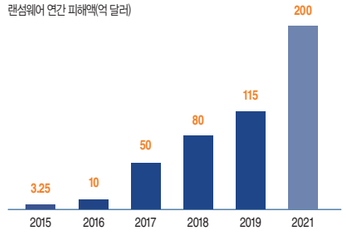
자료: IBM

Web 3.0시대, 핵심 인프라, 사이버 보안

요즘 가장 많이 듣는 IT용어 중 하나가 Web 3.0시대이다. Web 1.0시대는 초기 인터넷 출현, 인터넷 포털 검색 등 아주 기초적인 단계를 말한다. Web 2.0시대는 지금의 인터넷시대를 말한다. 인터넷 속도가 빨라지면서 메신저, 소셜 미디어, 영상 공유 등 양방향 소셜 네트워크가 가능해졌다. 이 시기를 겪으면서 소위 FAANG이라고 불리는 빅테크 기업들의 비약적인 발전이 있었다.

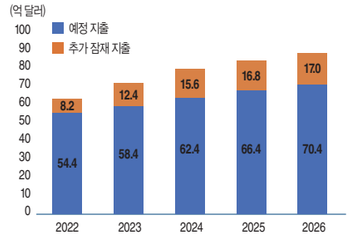
Web 3.0시대는 여기에서 한 단계 더 진화한 것으로 향후 5G, 6G등의 인터넷 속도 발전과 더불어 데이터가 개인 맞춤화되고 단순히 글과 영상으로 보는 평면적인 경험이 아니라 VR(가상현실), AR(증강현실) 등을 활용한 입체적인 가상현실세계(메타버스) 경험을 가능하게 하면서 사물인터넷(IoT)과 스마트시티 등의 구축에 큰 역할을 할 것이다. Web 3.0시대가 되면 수많은 인공지능, 로봇기술이 함께 개발될 것이다. 이러한 무궁무진한 발전을 위해서는 그만큼 엄청난 양의 데이터 생산이 수반되며 안전한 처리가 필요하다. 이런 방대한 데이터 생산 및 관리를 위해 블록체인(탈중앙화) 기술이 점진적으로 자리를 잡을 것이다. 또한 디지털 자산이 자산군으로 자리를 잡으면서 암호화폐, 디파이(탈중앙화 금융), NFT 등이 활발해질 것이다. 결국, 정보가 개별 맞춤화되고 대량생산되기 때문에 개인정보에 대한 위협이 증가할 것은 자명한 사실이다. 앞으로 Web 3.0 시대가 안전하게 자리를 잡기 위해서는 사이버 보안은 필수적인 인프라다.

랜섬웨어 공격 피해 규모



자료: Cyber Security Ventures

미국 인프라 법안중 사이버 보안 예정 지출 + 추가 잠재 지출



자료: Gartner

2021년 주요 사이버 공격 사례

날짜	사건	비고
2020.12~2021년 1월	Solarwinds 해킹 피해	IT 모니터링 및 관리 소프트웨어에 트로이 목마를 통해 해킹했으며, 전 세계 컨설팅, 기술, 통신, 미국 정부기관(국방부, 재무부, 상무부) 등이 피해
2021년 3월	Microsoft Exchange 해킹	상당수 중소기업과 지방정부를 포함 미국 전역의 최소 3만 개 조직이 해킹 피해
3월	Acer	에이서의 재무제표, 은행 현금 잔고 등의 자료 공개 협박 후 5천만 달러 요구
5월	Colonial Pipeline 랜섬웨어 피해	미국 남동부에 위치한 미국 송유관 회사인 컬로니얼 파이프라인이 해킹으로 6일간 업무를 중단했으며, 해커는 440만 달러의 대가를 요구
5월	JBS 랜섬웨어 피해	미국과 호주 내 육류 공급의 약 1/5을 담당하고 있는 JBS의 내부 주요 파일을 암호화하면서 시스템 마비, 대가로 1,100만 달러 요구
7월	Kaseya 소프트웨어 해킹	다양한 기업이 컴퓨터 시스템을 원격으로 관리하는 데 사용하는 원격 모니터링 및 관리 솔루션을 해킹하면서 데이터 복구 조건으로 7천만 달러 요구
10월	Tesco 홈페이지 해킹	주간 약 130만 건의 주문을 받는 테스코 시스템이 해킹당하면서 테스코는 불가피하게 홈페이지 업그레이드 실시
12월	Log4j	프로그램 방문자의 접속기록이나 개발과정을 기록하는 오픈소스에 대한 취약점 발견

주요 기업들의 사이버 보안 투자 계획

기업	투자 내용
Apple	9천 개 이상의 부품 협력사를 위한 새로운 보안 프로그램 개발
Microsoft	5년간 200억 달러를 투자해 사이버 보안을 강화하고 보안 훈련 파트너십 확장
JP Morgan	사이버 보안 비용으로 매년 6억 달러를 투자할 예정이며 IT인력을 3천 명 이상 배치
Google	5년간 100억 달러를 사이버 보안에 투자하며 IT 지원 및 데이터 분석 분야의 전문가 10만 명에 사이버 보안 훈련 실시
Toyota	Nissan, Panasonic 등 90개 기업이 협업하여 사이버 공격 침입점을 공유하고 공동으로 대응

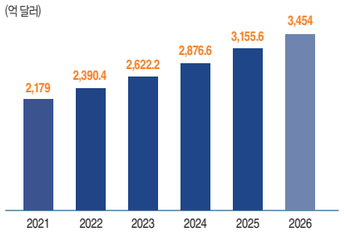
정부 및 기업의 사이버 보안 정책 강화

사이버 범죄가 지속됨에 따라서 정부와 기업의 사이버 보안에 대한 정책과 투자가 꾸준하게 늘어나고 있다.

2021년 5월, 바이든 대통령은 연방 사이버 보안 역량을 현대화하고 사이버 공격에 대한 대응 전략을 표준화하며 정부 계약업체에 대한 정보 공유 요건을 강화하려는 목적의 행정명령에 서명했다. 그 후 7월, 바이든 대통령은 전력, 용수 및 교통과 같은 중요 인프라에 대한 사이버 공격을 막기 위한 국가 보안 각서에 서명했다. 이러한 조치는 인프라 투자 및 일자리 법에서 실제 지출로 반영되었다. 이 법은 국가의 사이버 보안을 개선하기 위해 17억 달러의 전용 지출 및 약 70억 달러의 예비지출을 포함한다. 또한 지난해, 상원은 백악관의 첫 국가 사이버 국장 임명을 만장일치로 인준했다.

의회는 2021년 국가방위수권법의 일환으로 이 자리를 신설하였는데, 이는 앞으로 행정부 내에서 사이버 보안에 더욱 중점을 두겠다는 신호이다.

글로벌 사이버 보안시장 예상규모



자료: Statista

기업들 역시 사이버 보안에 대한 투자를 강화하고 있다. IT컨설팅 및 리서치 회사인 가트너(Gartner)가 3천 명 이상의 임원을 대상으로 실시한 최근의 설문조사에 의하면 응답자의 69%가 2022년 사이버 보안 지출이 늘어날 것으로 예상했다. 이 회사에 따르면 데이터 보호 및 리스크 관리에 대한 지출이 2021년부터 11% 증가하여 2022년에 1억 7,200만 달러에 이를 것이라고 한다.

이러한 사이버 보안에 대한 투자는 IT, 금융, 제조업 등 모든 산업에서 확대되고 있는 상황이다. 개인들도 아직은 적은 수준이지만 사이버 보안에 대한 지출을 조금씩 늘리고 있다. VPN, 이중 인증 절차, ID 도난 방지 서비스와 같은 예방책을 사용하고 있다. 특히 개인에 대한 기업 및 정부차원에서의 교육이 무엇보다도 필요하다.

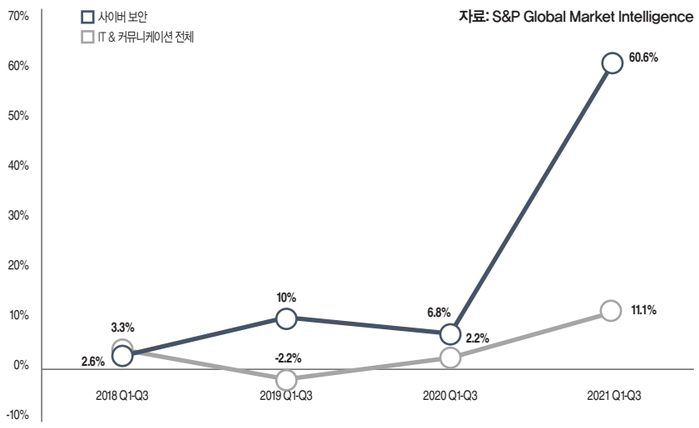
커지는 사이버 보안 시장 규모

사이버 보안 시장 규모는 갈수록 증가하는 추세이다. 2021년 사이버 보안 시장의 규모는 2,179억 달러 수준으로 2026년에는 3,454억 달러로 향후 5년간 약 58% 증가할 것으로 예상된다.

사이버 보안 시장이 관심을 끌고 있는 것은 M&A 건수로도 확인이 가능하다. 2021년 8월 사이버 보안 업체 두 거물이 합병을 해서 화제가 되었다. 노턴이 어베스트(Avast)를 86억 달러에 인수한 것이다.

이를 비롯하여 2021년도 3분기 기준 M&A건수를 보면 사이버 보안업체 부문에서는 건수가 전년 94건에서 151건으로 60.6% 증가했다. 이는 IT & 커뮤니케이션 전체 11.1% 대비 5배가 높은 수준이다. 또한 사이버 보안업체들의 성장성 또한 시장 전체 대비 아주 높은 수준이다.

부문별 M&A 거래 건수



자료: S&P Global Market Intelligence

> 사이버 보안 시장이 관심을 끌고 있는 것은 M&A 건수로도 확인이 가능하다. 2021년 8월 사이버 보안 업체 두 거물이 합병을 해서 화제가 되었다. 노턴이 어베스트(Avast)를 86억 달러에 인수한 것이다.

2022년 4월 말 기준 사이버 보안 기업들의 향후 12개월 매출 성장률은 26.2%로 S&P 500 평균 7.6% 대비 3배 가량 높은 수준이다.

사이버 보안업체들은 안티바이러스 소프트웨어를 판매하는 것에 그치는 것이 아니라 매번 진화하는 공격 패턴에 따라 주기적인 업데이트 및 기업/개인 서버 등의 관리를 하고 있고 이에 따라 매월 정액제 서비스, 프리미엄 서비스 등을 제공하여 수익을 추구하고 있다.

사이버 보안업체 주요 종목은 오른쪽 표와 같다.

사이버 보안 산업의 장기 성장 기대

Global X 리서치팀은 사이버 보안산업이 인터넷과 다양한 IT기술의 발전을 통해 이미 초기 다수자(Early Majority)단계에 도달했다고 판단한다.

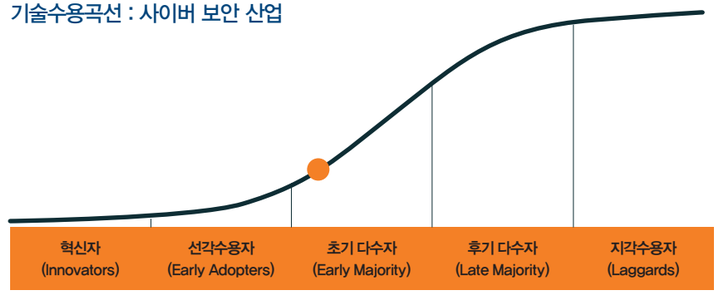
향후 Web 3.0 그리고 앞으로 다가올 다양한 혁신기술의 발전에 따라 데이터 양이 방대해지고 거기에 따라 사이버 위협과 공격이 강해질수록 사이버 보안 산업의 발전과 확장은 지속될 것으로 예상하며 성장성에 있어서 가장 스윗 스팟(sweet spot)인 초기 다수자 단계를 당분간 계속 향유할 것으로 본다.

주요 사이버 보안업체

자료: Bloomberg, 2022년 5월 25일 기준

회사명	시가총액(백만달러)	기업 개요
FORTINET INC.	46,123	네트워크 보안 솔루션 제공업체. 동사는 네트워크 보안 장비, 관련 소프트웨어 및 가입 서비스를 제공. 동사의 시스템은 방화벽, VPN, 바이러스 백신, 침입 방지(IPS), 웹 필터링, 스팸 차단, 트래픽 조절 등 보안기술 업계에서 가장 광범위한 제품군 제공
CHECK POINT SOFTWARE TECH	113,783	다양한 소프트웨어, 하드웨어 상품 및 IT 관련 서비스를 개발, 판매 및 지원하는 업체. 동사는 또한 고객들에게 네트워크, 게이트웨이 보안 솔루션, 데이터 및 엔드포인트 보안 솔루션과 관리 솔루션을 제공
CROWDSTRIKE HOLDINGS INC – A	34,023	기업을 보호하고 엔드 포인트에 대한 공격을 방지하기 위한 사이버 보안 플랫폼을 제공
PALO ALTO NETWORKS INC.	50,367	네트워크 보안 솔루션 제공업체. 동사는 애플리케이션을 식별 및 제어하고, 위협을 방지할 목적으로 콘텐츠를 스캔하며, 데이터 유출을 방지하고, 통합 애플리케이션, 사용자 및 콘텐츠 가시성을 제공하는 방화벽 서비스를 제공
NORTONLIFELOCK INC.	14,252	소비자 사이버 보안 솔루션 제공업체. 동사는 고객의 장비, 온라인 프라이버시, 신원, 가정 네트워크를 보호할 수 있는 솔루션을 제공

기술수용곡선 : 사이버 보안 산업



자료: Global X Research Team