CHUBB®

사이버 클레임 시나리오

1) 온라인포털 운영 업체에 대한 사이버 공격

피보험자	온라인포털 운영 업체
사고경위	온라인포털을 통해 회원들에게 데이터베이스 접속 서비스를 제공하는 업체에 대한 사이버 공격이 발생하여 회원들의 가입 정보가 서로 뒤섞여버리는 결과가 초래됨
보상내용	**사이버위험관리보험 기본약관 내 1.2 네트워크배상책임** 등 관련 조항에 따라 아래의 비용 보상 가능 – 사고 원인 파악을 위한 사고대응매니저 및 포렌식 컨설팅 업체 투입에 소요된 사고대응비용

2) 기업 휴지 사고

피보험자	인터넷 구독서비스 제공 업체
사고경위	인터넷 구독서비스 제공 업체에 디도스 공격이 발생하여 해당 업체의 홈페이지에 대한 접속이 22시간 동안 차단되고, 웹사이트를 통해 이루어졌던 구독서비스 판매가 중단되는 등 공격 발생 후 4일 동안 원활한 서비스 제공이 이루어지지 못함
보상내용	**사이버위험관리보험 기본약관 내 1.2 네트워크배상책임, 1.6 기업휴지** 등 관련 조항에 따라 아래의 비용 보상 가능 – 포렌식 컨설팅 비용 및 기업휴지 비용

3) 요양시설에 대한 랜섬웨어 공격

피보험자	요양시설
사고경위	요양시설에 대한 랜섬웨어 공격이 발생하였고, 공격자는 해당 시설에 랜섬비용을 요구함. 고객은 랜섬비용을 지불하는 대신 자체 백업 데이터를 통한 시스템 복구를 선택
보상내용	**사이버위험관리보험 기본약관 내 1.4 사이버갈취, 1.5 데이터 자산 손실** 등 관련 조항에 따라 아래의 비용 보상 가능 – 호출 단추와 보안 시스템, 약물 추적 소프트웨어 등 시설의 핵심적 시스템에 대한 복구 비용 – 사고대응비용 및 포렌식 컨설팅 비용

4) 병원에 대한 랜섬웨어 공격

피보험자	병원
사고경위	병원의 컴퓨터 시스템에 대한 랜섬웨어 공격이 발생. 요구받은 랜섬비용은 크지 않았으나 일시적으로 건강보험회사에 대한 비용 청구 업무 및 급여 지급 업무, MRI와 CT 이미지 처리 업무 등이 불가능해짐
보상내용	**사이버위험관리보험 기본약관 내 1.4 사이버갈취, 1.6 기업휴지** 등 관련 조항에 따라 아래의 비용 보상 가능 – 포렌식 컨설팅 비용, 데이터 복구비용, 기업휴지 비용 및 위기 관리 비용

5) 제휴 업체 및 Supply Chain에 대한 사이버 공격

피보험자	건강정보 보유 업체
사고경위	건강정보 보유 업체의 제휴사 중 한 곳에 랜섬웨어 공격이 발생하였고, 그 결과 업체 고객들의 건강 정보가 유출될 위기에 처함. 사고 대응 매니저가 개입하여 공격 받은 제휴사 시스템에서의 데이터 유출 여부를 확인하였고, 실질적 유출은 없었다는 결론을 내림
보상내용	**사이버위험관리보험 기본약관 내 1.1 개인정보배상책임** 등 관련 조항에 따라 아래의 비용 보상 가능 – 개인정보 유출 여부 확인 과정에서 소요된 사고대응비용

*보상내용은 보험계약조건, 보험금지급관련 조사결과 등에 따라 달라질 수 있습니다.

Chubb. Insured.℠

06/2018