사이버 보험 계약 감사

Jide Olakunle, CISA, CISM, CISSP는 Alfa Vision Insurance의 감사 및 보안 전문가입니다. Olakunle은 Alfa Vision에 입사하기 전에 나이지리아의 3대 신생 은행에서 10년 이상 규정 준수, 감사 및 보안 그룹의 업무를 담당했습니다. 현재 Capella University(미국 미네소타주 미네아폴리스)에서 정보 기술, 보안 및 보증 분야를 연구하는 박사 과정에 있습니다.

조직의 생산성, 수익성 및 프로세스에 대한 정보 기술의 중요도는 급격히 증가하고 있습니다. 제품 설계, 마케팅 및 보고를 활용하고, 정보 관리를 처리하고, 서비스 산출물을 향상시키는 활동에 있어서 IT 인프라에 대한 의존도는 그 어느 때보다도 큽니다. IT 시스템에 대한 의존도가 높아짐에 따라 관련된 위험도 커집니다.

최근 수 년간, 시스템 상호 연결이 증가한 결과로 종이 문서 보관에서 전자 데이터 보관으로 전환하는 정부 및 사설 기관이 온라인 거래 플랫폼의 트래픽을 강화하고 기술 제품(예를 들어, 클라우드 서비스)을 개선함에 따라, 사이버 사고는 IT 보안 위반으로 가장 많이 보고되는 유형 중 하나가 되었습니다. 사이버 사고의 영향, 빈도 및 강도는 계속 높은 추세이어서 사이버 사고에 대비한 사업 연속성 계획에서는 이러한 사고에 대한 개념이 만약이라는 관점에서 언제라는 관점으로 바뀌었습니다. 2013년 1사분기에 미국의 5대 은행이 서비스 거부(DoS) 공격을 받았으며 Twitter, Facebook, Microsoft 및 Apple 시스템이 해킹되었습니다. 대한민국에서는 금융 기관과 언론사 시스템이 해커에 의해 마비되었습니다.

해킹 공격과 관련하여 지불해야 하는 유형 및 무형의 댓가는 실로 큽니다. 조직은 사이버 공격을 지연하고, 방지하고, 퇴치하고, 문서화하기 위한 위험 관리 전략을 구현해야 합니다. 위험 관리의 목적은 자산을 보호하고, 자원을 보전하고, 의사 결정의 질을 높이는 것입니다. 위험 관리 전략에는 위험 수용(위험에 대처하고 예상되는 손실에 대한 예산 편성), 위험 완화(위험과 그 영향을 억제하는 전략 구현), 위험 회피(위험을 유발하는 프로세스, 이벤트 또는 행동을 금지함으로서 위험 예방), 그리고 위험 이전(위험에서 발생하는 책임을 제3자에게 전가) 등이 포함됩니다.

사이버 보험은 사이버 활동에서 발생하는 위험을 전가하기 위해 개발된 상품입니다. 2012년 미국에서 사이버 보험의 보험료는 8억 달러에서 10억 달러 이상의 규모로 성장했습니다.[1] 이 시장은 향후 5년 내에 25퍼센트 추가로 성장할 것으로 예상됩니다. 시장이 성장함에 따라 사이버 노출을 식별하고, 예방 기술을 준비하며, 보안 공백을 확인하는 일에 있어서 정보 시스템(IS) 전문가의 역할이 더욱 중요해질 전망입니다. 수많은 조직이 위험을 전가하는 전략으로 사이버 보험을 도입함에 따라 IS 감사인이 파악하고 검토해야 할 또 다른 영역이 생겼습니다. 사이버 보험의 적절성, 완전성 및 타당성을 효과적이고 효율적으로 감사하기 위해 IS 감사인은 사이버 보험의 복잡한 내용을 이해할 필요가 생겼습니다.

사이버 보험의 이유

조직이 구현한 예방, 적발 및 교정 통제 방법으로는 사이버 사고를 완전히 막을 수 없습니다. 사이버 보험은 잔존 위험을 관리하는 한 가지 방법입니다. 이것은 인터넷 기반의 위험뿐만 아니라 기타 관련 IT 활동, 도구 및 프로세스로 인해 발생하는 위험으로부터 조직을 보호하기 위해 사용되는 보험입니다. 사이버 공격을 받은 조직이 정보를 숨기던 시대는 지나갔습니다. 이제는 산업 규제 기관과 언론 매체가 기업의 투명성을 압박하고 있습니다. 미국증권거래위원회의 기업재무공개안내(CF Disclosure Guidance)에 따르면 기업은 특정 데이터 누출 또는 기타 사이버 사고와 관련된 중대한 위험을 보고하고, 재정적 비용, 법적 비용, 향후 재발을 방지하기 위해 시행되는 문서 관리 등을 의무적으로 공개하도록 명시하고 있습니다.[2] 해커는 점점 대담해져서 YouTube, Twitter 및 기타 소셜 미디어를 통해 자신들의 대담한 행동과 해킹한 데이터를 공개하고 있습니다. 24시간 케이블 네트워크를 통한 뉴스 경쟁도 모든 뉴스가 알려지도록 부추기고 있습니다.

정부 및 다양한 산업 규제 기관도 위반 행위에 대한 과징금을 부여함으로써 기업이 개인 데이터를 보호하도록 압박을 가하고 있습니다. 미국의 46개 주는 기업이 데이터 침해 행위를 고객에게 통보하도록 의무화하는 법안을 발의했습니다. 금융정보보호법(Graham-Leach-Bliley Act) 및 건강정보 이전과 책임에 관한법(HIPAA)과 같은 미국 연방법, 유럽 정보 보호 지침(2003), 일본 개인 식별 정보법(2005), 그리고 기타 국제 개인정보 보호법 등은 조직이 고객 데이터 위반에 대한 책임을 지도록 하고 있습니다.

2011년 PricewaterhouseCoopers Global State of Information Security Survey의 질문 중에 "소속 조직이 전자 데이터, 소비자 기록 등의 절도 또는 악용으로부터 보호하는 보험 계약을 가지고 있습니까?"라는 것이 있었습니다. 전세계

1만 2,840명의 응답자 중 46퍼센트가 "예"라고 답했습니다.[3] 이것은 위험 이전 전략으로 사이버 보험 계약에 대한 의존도가 증가했을 뿐만 아니라 조직의 보험 상품 수용이 증가했음을 보여줍니다.

사이버 보험의 유형

가장 일반적인 유형의 사이버 보험은 당사자 위험 노출 및 제3자 위험 노출입니다. 당사자 보장 보험은 사이버 침해 및 사이버 공격에 대한 대응으로 가입 기관에 의해 직접적으로 발생된 비용과 가입 기관의 피해에 대해 보장합니다. **그림 1**은 당사자 보험에 의해 보장되는 노출 유형을 설명합니다.

그림 1—당사자 보험 위험 노출

위험 노출	설명	공격 벡터
IT 자산의 손실 또는 손해	이것은 IT 인프라에 대한 손해, 피해 소프트웨어 또는 데이터 손실을 보장합니다. 자산을 복원하거나 교체하기 위해 발생한 비용을 보장합니다.	바이러스 공격, 인젝션 공격, 멀웨어 공격, 웹사이트 변조, 네트워크 하드웨어 파괴
사업 중단/거부	특정 기간 동안 네트워크 자원의 사용 중단 또는 거부로 인한 소득 손실을 보장합니다.	DoS, URL 접근 제한, IP 또는 상표의 절도, 사이버 공격
인지도 하락	이것은 지적 재산의 손실, 고객 손실 또는 조직의 인지도 하락으로 인한 재산 손실을 보상합니다.	이메일 피싱, 웹사이트 해킹
전자 절도	사이버 세계에서 직접적인 금전 손실을 보상합니다.	사이트 간 스크립팅, 트로이 목마
사이버 갈취	네트워크를 파괴하거나 개인 정보를 유출한다는 협박과 관련된 금액 지불을 보상합니다.	사이버 따돌림

제3자 보상은 보험에 가입된 기업에 대해 사이버 공격 및 사이버 침해와 관련하여 제3자가 제기한 주장의 책임, 손해, 변호사 수임료, 비용 등을 보상합니다. **그림 2**는 제3자 보험에 의해 보장되는 노출 유형을 보여줍니다.

그림 2—제3자 보험 위험 노출

위험 노출	설명	사고 유형
위기 서비스 비용	여기에는 조사, 통지, 신용도 모니터링 및 관련 평판 피해 등과 관련된 비용이 포함됩니다.	멀웨어 공격, 신용카드 데이터 훼손, 데이터 침해
법적 손해 비용	여기에는 변호 비용, 채무 완결 및 민사 책임이 포함됩니다.	규정 위반
벌금	보안 또는 개인정보 보호 책임과 관련된 규제 기관의 조사 또는 시행으로 발생되는 지급액 또는 벌금이 포함됩니다.	고객 의료 기록의 노출로 인한 데이터 침해
제3자 재산 손실	제3자 재산의 손실이나 손상, 또는 데이터 손실에 대한 책임이 포함됩니다.	멀웨어, 보험 가입 기업을 시작 플랫폼으로 사용하는 바이러스 공격, 봇네트

사이버 보험 계약 감사 목적

감사를 효과적이고 효율적으로 실시하기 위해, 감사인은 수행 목적을 이해해야 합니다. 사이버 보험 감사의 목적에는 다음 사항이 포함됩니다:

- 위험 관리 프로세스의 효과성 확인
- 위험을 식별하고 분석하기 위한 적절한 절차가 개발되어서 노출을 줄이는 프로세스를 구현하고 진행 상태를 모니터링하고 있는지 확인
- 식별된 위험에 대해 사이버 보험이 적절한 보상을 하는지 확인
- 사이버 보험 계약이 모든 중요 IT 인프라를 보상하는지 확인
- 사고를 보고하고 클레임을 제기하기 위한 절차의 존재 및 적절성 확인

사이버 보험의 감사를 위한 방법

사이버 보험 계약의 감사는 2개의 주요 요소로 구분될 수 있습니다.

1. 사이버 보험 계약에 대한 선행 조건
2. 사이버 보험 계약의 동시 조건

IS 감사인은 사이버 보안 계약을 적절히 감사하기 위해 사업, 중요 자산 및 IT 인프라를 이해해야 합니다. 감사인은 이러한 기본 지식을 토대로 사이버 보험 계약의 가입이 필요하게 된 조건을 검토해야 합니다. 다음은 IS 감사인이 고려해야 할 사항입니다.

- **네트워크 다이어그램과 업무 처리 플로우 차트를 검토합니다.** 네트워크 다이어그램은 IT 인프라를 그림으로 묘사해서 보호해야 할 중요 프로세스를 식별하는 단계적인 순서도를 보여줍니다. 네트워크 다이어그램은 정기적으로 업데이트되어야 합니다.
- **조직의 위험 관리 프레임워크가 사업에 대한 중요도에 따라 모든 IT 자산을 식별하고 분류하고 있는지 확인합니다.** 모든 자산은 중요도에 따라 등급이 구별되어야 합니다. IS 감사인은 자산 관리 문서의 완전성을 확인해서 모든 중요 자산이 문서화되고, 등급이 지정되고, 프로세스 변경에 따라 지속적으로 검토되고 있는지 확인해야 합니다.
- **위험 관리 전략이 정기적으로 업데이트되고 현행 사업 및 IT 인프라를 반영하고 있는지 확인합니다.** 오늘날과 같은 제로데이 악용(Zero-day exploits)의 시대에서는 방어 메커니즘을 매일 검토해야 합니다.
- **IT 보안 전략의 적절성을 평가합니다.** IS 감사인은 IT 보안, 도구 및 프로세스의 적절성을 검토해야 합니다. 보안 시스템에 대한 첫 번째 단계는 예방적인 통제입니다.
- **특정 기간 내의 IS 사고 보고서를 검토합니다.** IS 감사인은 사고 보고서를 통해 공격의 경향, 대상 시스템, 그리고 공격 채널을 이해할 수 있게 됩니다.

IS 감사인은 사이버 보험의 목적이 이러한 사이버 활동으로 야기되는 재정적인 손실로부터 보험 가입자의 재정적인 부담을 완화하는 것임을 이해해야 합니다. IS 감사인은 사이버 보험 증권을 입수하는 동시에 아래의 절차들을 취해야 합니다:

- **조직이 보험사에 제출한 제안서 샘플을 받아서 그 안에 기재된 데이터의 완전성 및 진실성을 평가합니다.** 제안서에는 네트워크의 성격, 크기 및 복잡도, 데이터 구조, 현재 시스템 보안, 그리고 전체 IT 인프라에 대한 사항이 명시되어 있습니다. 보험사는 제안서에 있는 정보를 사용해서 보험료를 책정하고 기타 보험 관련 의사결정을 내립니다. 보험료 지급청구가 발생했을 때, 조직이 설문 내용에 중요 정보를 고의적으로 또는 실수로 누락한 사실이 발견되는 경우에는 계약이 무효화될 수 있습니다. IS 감사인은 제안서의 세부 사항에 대해 진실성을 확인해야 하며, 부정확한 답변이 발견되는 경우에는 경영진에게 통보해야 합니다.
- **보험 증권 사본을 입수해서 보장 범위를 검토하고 모든 중요 영역이 계약에 포함되어 있음을 확인합니다.** 조직의 과거 보안 사고 또는 업계 동향에 따라 사고에 노출될 경향이 높은 모든 필수 시스템을 보장하지 못하는 경우, 감사인은 이러한 영향을 분석해서 경영진에 통보해야 합니다. 예를 들어 고객의 중요 신용 카드 데이터를 제3자 클라우드 스토리지에 보관하지만 사이버 보험 계약에서 이러한 자산을 보장하지 못한 온라인 소매점이 있을 수 있습니다. 소매점은 클라우드 운영의 보안에 관해 통제할 수 있는 사항이 제한되어 있지만, 고객 데이터의 보안에 대한 전체적인 책임을 지게 됩니다.
- **시행 중인 보안 대책을 검증합니다.** 보험 증권을 발행하기 전에 조직은 제안서에 보안 현황을 제출해야 합니다. IS 감사인은 기존 통제가 적절한지 테스트해야 합니다. 보안 공백에 대해 즉시 경영진에게 통보해야 합니다.
- **사고 보고의 문서화를 점검합니다.** IS 감사인은 사고의 보고 내용의 적절성이 사이버 보험 계약과 조화를 이루는지 확인해야 합니다.
- **사이버 보험 계약 및 절차가 해당 직원에게 통보되었는지 확인할 수 있도록 IT 직원과 인터뷰합니다.** 직원은 사이버 보험 계약, 보고해야 하는 사고, 그리고 보험 적용 사고 발생시 취해야 할 단계에 대해 적절히 숙지하고 있어야 합니다. 보험 가입된 사고 발생시 수 분 내에 취한 행동에 따라 성공적인 지급청구가 이루어질 수 있습니다.
- **IT 인프라의 중대한 변경 사항이 보험사에 어떻게 전달되는지 확인하고, 보험 계약에서 보상되는 물리적 자산의 사본을 입수해서 현재 자산과 비교합니다.** 제외된 사항은 알려서 조치를 취하도록 해야 합니다.
- **과거에 보상 받은 사고 또는 지급청구의 샘플을 수집해서 사고 위험을 줄이기 위해 구현할 수 있는 시정 조치가 있는지 확인합니다.** 사고 증가가 보고된 내용은 조사를 해야 하며 자원을 적절히 전환해야 합니다.

기사가 흥미롭습니까?

- 지식 센터에서 감사 도구 및 기술과 사이버 보안에 대해 토의한 후 협업하는 방법에 대해 알아보십시오.

www.isaca.org/knowledgecenter

결론

사이버 공격과 이에 따른 보안 침해는 현재 조직에 있어서 급격히 확산되고 있는 보안 위협입니다. 보안 사고의 빈도, 성격 및 비용은 우려할 수준으로 증가 추세입니다. IS 감사인은 조직이 적절한 자체적인 보호 기능을 제공하고 중요 데이터에 대한 보안을 지키도록 해야 합니다. IS 감사인은 위험 관리 검토 또는 독립적인 검토의 일환으로 사이버 보험 계약 감사를 계획해야 합니다. 사이버 보험은 의무적인 요건은 아니지만, 점점 더 많은 조직이 위험 전가를 위해 이러한 전략을 취하고 있기 때문에, IS 감사인은 그 프로세스를 이해하고 완전성, 적절성 및 무결성에 대해 보험 계약을 테스트해야 합니다.

미주

[1] Airmic, "Airmic Review of Recent Developments in the Cyber Insurance Market," 8 June 2012, *www.airmic.com/sites/default/files/Airmic%20Review%20of%20Recent%20Developments%20in%20the%20Cyber.pdf*

[2] Division of Corporation Finance, Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2, "Cybersecurity," 13 October 2011, *www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm*

[3] PricewaterhouseCoopers, "Global State of Information Security Survey 2011," *www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml*