증가하는 사이버 사고...
비즈니스 연속성 계획의 중요성

비즈니스 연속성 계획(BCP)을 통해 대응하는 사이버 사고

BCI Horizon Scan Report 에 따르면 사이버 범죄는 미래 위험 요소 중 상위에 꾸준히 위치하고 있으며, 2022 년에도 미래의 위험 요소에서 1 위를 차지했다. 기업은 사이버 공격에 대한 Resilience 을 유지하기 위해 기술 개발에 많은 투자를 하고, 새로운 제어 기능을 도입하고 있지만, 공격 빈도는 꾸준히 증가하고 있으며 공격 벡터[1]는 더 복잡해지고 탐지하기 어려워졌다. Check Point Research 는 2021 년과 2022 년 사이에 사이버 공격 수가 38% 증가하였다고 보고하였으며, ChatGPT 등 AI 기술의 발전으로 사이버 공격의 횟수가 2023 이후에도 증가할 것으로 예측하고 있다.

사이버 공격으로 인한 영향은 단순히 시스템을 침해하는 것을 넘어, 기업 평판이 하락하고 판매량이 감소하며 주가가 폭락하는 데 영향을 미칠 수 있다. 따라서 기업의

[1] Attack Vector: 사이버 공격자가 네트워크 또는 시스템에 침입하는 방법

경영진은 사이버 위협에 대해 더욱 탄력적으로 대처하는 것이 매우 중요하다. 일부 조직은 IT 또는 사이버 부서가 비즈니스 연속성 부서와 별도로 작동하고 있지만, 이러한 조직 구성은 공격을 유발할 가능성이 더 높다. IT 부서와 비즈니스 연속성 부서가 협력해야 하는 필요성에 대한 인식이 나타나는 것이다. 실제로 사이버 위험에 대한 대응을 통합하는 것이 더 성공적인 기업 전략으로서 채택되고 있다.

사이버 **Resilience** 란 무엇인가?

사이버 Resilience 란 비즈니스 운영의 연속성을 보장하면서 사이버 공격을 식별, 보호, 탐지, 대응 및 복구하는 조직의 능력이다. 즉, 사이버 Resilience 는 공격을 방지하는 것뿐만 아니라 이를 견디고 신속하게 복구할 수 있는 능력과 연관되어 있다. 최근에는 인적 자원, 프로세스 및 기술을 포함하는 종합적이고 교차 기능적인 사이버 Resilience 와 비즈니스 연속성(Business Continuity)가 상호 연계된 접근방식의 중요성이 강조되고 있다 [1)].

사이버 Resilience 를 확보하는 것은 재정 손실을 최소화하기 위한 모든 조직의 중대한 전략이 되었다. 사이버 보안 및 IT 팀이 사이버 Resilience 에 대한 주요 책임을 지니지만, 비즈니스 연속성 및 리스크 관리팀과 같은 다른 조직도 정기적으로 협업하여 위험을 최소화해야 한다. 특히 각 기능마다 명확한 책임자가 작성되어 있는 문서화된 전략이 필요하다. 또한, 경영진의 리더십은 강력한 사이버 Resilience 전략을 수립하는 데 중요한 역할을 하며, 전략이 수립된 이후에도 이를 실제로 실행하기 위해 필요한 자원과 투자를 지원해야 한다. 특히, BCI Cyber Resilience Report 2023 에서는 IT 부서와 비즈니스 연속성 관련 부서가 훨씬 더 긴말하게 협력해야 한다고 강조한다. 뿐만 아니라, 대응 계획을 통합하여 임직원의 인식을 제고하기 위한 노력이 필요하고, 모든 임직원은 교육, 검증 활동 및 내부 정책이 중요한 역할을 수행함을 인정할 수 있어야 한다.

1) BCI Cyber Resilience Report 2023 의 설문 응답자 중 43%는 사이버 보안 부서가 BC(Business Continuity)조직과 별도로 구성돼 있다고 하더라도, BC 는 사이버 Resilience 를 구현하는데 핵심적인 역할을 수행한다고 응답하였다.

사이버 **Resilience** 확보를 위한 기업의 움직임

BCI Cyber Resilience Report 의 응답자 대부분(87.0%)은 자신의 조직이 사이버 사고를 처리하기 위한 비즈니스 연속성 계획(Business Continuity Planning)을 마련해 놓았다고 보고하였다. 실무자 중 가장 많은 비율(39.2%)이 사이버 사고 대응 또는 복구를 위한 내부 자원을 활용하고, 32.0%는 사이버 보험 정책에 사이버 사고 대응 또는 복구를 위한 지원이 포함되어 있다고 답하였다. 15.7%는 사이버 복구를 위한 제 3 자와의 계약을 체결하였다. BCI Cyber Resilience Report 는 과거부터 비즈니스 연속성이 사이버 사고 대응 조치를 취하는 데 중요한 역할을 한다는 것을 강조해왔으며, 올해의 조사 결과를 통해서도 비즈니스 연속성 계획(BCP)의 중요성을 느낄 수 있었다. 이는 사이버 Resilience 을 구축하거나 개선하려는 전문가들이 참고할 수 있는 중요한 기준 분석 자료로 활용될 수 있다.

귀사에는 사이버 사고로 인한 중단을 처리할 수 있는 계획이 있습니까?	비율

예, 사이버 사건 대응 및/또는 사이버 복구에 사용할 수 있는 내부 자원이 있다.	39.2%
예, 자사 사이버 보험 정책에는 사이버 사건 대응 및/또는 사이버 복구 지원이 포함되어 있다.	32.0%
예, 신뢰할 수 있는 제 3 자와 사이버 사건 대응 및/또는 사이버 복구 전용 계약을 체결하였다.	15.7%
아니오	3.9%
기타	3.9%
모르겠음	5.2%

사이버 Resilience 을 강화하는 비즈니스 연속성 계획(BCP)

아래 표는 비즈니스 연속성 계획(BCP)이 사이버 Resilience 을 지원하는 방법을 보여준다. 주요 지원 방안으로는 빠른 복구를 보장(81.3%), 재정적 손실을 줄일 수 있음(51.4%), 사고 대응을 위한 전문 자원을 제공함(50.7%) 등이 선택되었다. 이는 비즈니스 연속성 전문가들이 현재의 문제에 대응하면서도, 중요한 역할로서 인정받은 BCP 의 품질을 꾸준히 유지하고 있다는 것을 보여준다. 인터뷰 대상자는 사이버 사고가 비즈니스에 영향을 미칠 때 비즈니스 연속성 계획이 명확한 역할을 하며, 사고 발생 시 비즈니스 연속성 계획의 주요 역할은 대처 방안과 대체 공급업체를 확보하는 것이라고 설명했다.

귀사의 비즈니스연속성계획(BCP)은 사이버 사고 대응에 어떤 도움이 되나요?	비율
더 빠른 복구를 보장함	81.3%
재정 손실을 완화함	51.4%
사고에 대응하기 위한 전문 인력을 제공함	50.7%
조기 단계에서 공격을 감지하는 데 도움을 줌	47.2%
평판 손실을 완화하기 위한 일관된 PR 전략을 보장	44.4%
조직에 영향을 미치기 전에 공격을 저지함	37.5%
사고와 관련한 법률 자문 제공	35.4%
인적 실수 가능성을 감소시킴	35.4%
효과적이지 않음	3.5%

기타	**1.4%**
모르겠음	**5.6%**

또한, 응답자 중 일부는 "비즈니스 연속성(Business Continuity)은 시스템 및 인프라 개선을 통해 점차적으로 강화되는 만큼 IT 와 BC 사이에 강력한 연계가 유지되고 있다."고 언급하며 "기술 Resilience, 비즈니스 Resilience, 사이버 Resilience 의 통합은 비즈니스 전체에 대한 공동 및 포괄적인 보호를 제공한다."고 설명했다. 가까운 미래를 전망할 때, 많은 사람들이 비즈니스 연속성과 사이버, IT 및 정보 보안 분야 간의 연계가 더욱 강화될 것으로 예상한다는 것이다. 두 영역 간의 연계는 매우 중요하며, IT 및 HR 계획 구현에 BCP 요구사항이 더욱 긴밀히 통합되어야 한다.

그러나 기업 내 고립된 조직 문화에서는 여전히 여러 가지 문제점이 존재한다. 예를 들어, 한 응답자는 BCP 가 그들의 역할에 주요 부분을 차지하고 있지만, 현지 IT 팀이 사이버 위험에 대해 거의 소통하지 않는다고 답하였다. 다른 응답자는 "비즈니스 연속성이 사이버 사고 대응에 도움이 되지만, 경영진이 항상 이러한 연계를 보는 것은 아니다"라고 답하였다. IT 와 비즈니스 연속성 간 요구되는 협업 환경은 고위 경영진에서부터 실행되어야 하는 것이다. 경영진과 이사회가 두 영역의 긴밀한 관계를 구축해야 하며, 이는 여전히 많은 조직에서 해결해야 할 문제이다.

비즈니스 연속성 계획(BCP)은 사이버 사고가 발생한 때와 그 이후에 조직 평판에 미치는 영향도 지원한다. 평판 영향은 대규모 사고가 공개되어 주주 가치, 고객 이탈 및 수익에 영향을 미치는 경우, 경영진에게 큰 우려가 될 수 있다. 절반에 가까운 응답자들(44.4%)이 비즈니스 연속성이 평판 손실을 완화하기 위한 일관된 PR 전략을 수립하는 데 도움이 된다고 답하였다. 이는 산업 표준 및 지침에서 직접적으로 언급되는 위기 관리 및 위기 커뮤니케이션 구조를 확립하는 것이 비즈니스 연속성 관리(Business Continuity Management) 체계 수립의 필수 요소이기 때문이다.

BCP 를 갖춘 조직에 속한 한 응답자는 조직 내 BCP 의 기여가 매우 효과적이라고 설명하면서 "우리 조직은 사이버 보안 공격 뿐만 아니라 모든 비즈니스 중단 사항에 대한 위기 커뮤니케이션 계획을 수립하였다. 이 프로세스는 수년에 걸쳐 완성되었으며 ISO 표준 인증을 획득했다. 또한 위기 발생 시 의사소통이 가능한 독립적인 도구를 보유하고 있다."고 설명했다. 이는 사이버 사고에 대한 대응이 매우 중요하며, 초기 사이버 공격 자체보다 잘못된 외부 커뮤니케이션을 통해 더 큰 피해를 야기할 수 있음을 시사한다.

결론

현재 대부분의 사람들은 기업이 언젠가 사이버 공격을 당하고, 시스템이 중단되는 것이 일어날 수 있는 일임을 예상한다. 어느 누구도 기업이 사이버 공격을 당하지 않을 수 있는 완벽한 능력을 가졌다고 예상하지 않기 때문이다. 따라서 중요한 것은 사이버 공격에 대응하는 방식이다. 기업은 사이버 공격에 대해 어떻게 대응하고 있는가? 그들은 잘 소통하고 있는가? 그들은 합리적인 결정을 내리고 있는가? 그들은 나를 위해 무엇을 하고 있는가? 그들은 나의 정보를 어떻게 보호하고 있는가? 사고가 발생한 후 적절한

국가기관에 연락을 하였는가? 기업은 이러한 모든 의문에 답을 제공할 수 있어야 한다. 다시 말해, 사람들에게 전달해야 할 정보를 파악하고, 이 정보를 명확하게 전달하는 것이 기업을 보호하는 것이다.

또한, 비즈니스 연속성 계획(BCP)을 통해 사이버 사고 대응을 효과적으로 하기 위해서는 서로 다른 부서 간의 관계를 강화하는 것이 중요하다. 조직 내 관행을 구체적으로 파악하고 업무 영향 분석(BIA)[2]에 중점을 두는 것이 중요하며, BIA 를 통해 명확한 역할과 책임을 균형 있게 설정해야 한다. 또 다른 핵심 요소는 다양한 부서의 참여가 필요한 훈련을 실시하여 사고 발생 시나리오를 연습하는 것이다. 기업의 경영진은 통합의 중요성을 강조하며 공동 계획을 수립하고, 시나리오 시뮬레이션 및 훈련에 초점을 맞추는 것이 필요하다.

[2] BIA(Business Impact Analysis): 업무 중단 시 조직에 미치는 정량적·정성적 영향 혹은 손실을 측정하고 위기 발생시에도 우선적으로 수행되어야 할 최소한의 업무를 정의하는 활동을 말하며, 업무별 목표복구시간, 복구우선순위, 복구 필요 자원 및 중요정보 등을 식별한다.

[Reference]

- BCI Cyber Resilience Report 2023, BCI