기획조사

지역기업 사이버보안 실태 및 대응 방안 조사

2023. 6.

부산상공회의소

〈조사 개요〉

1. 조사 목적

○ **지역기업의 사이버보안 침해 현황 및 대응 실태 파악**

- 최근 클라우드 도입, 원격근무 확대 등 기업의 디지털 전환이 가속화됨에 따라 사이버보안 침해 위협이 크게 증가하고 있음
- 이에 지역기업의 사이버보안 인식과 대응 실태를 파악하여 보안대책 수립 방안을 모색하고, 기업의 보안강화를 위해 필요한 지원책 도출

2. 조사 내용

○ **사이버보안 침해 실태**

- 침해사고 발생 경험 및 유형
- 사이버보안 침해가 증가하는 이유

○ **사이버보안 대응 실태**

- 사이버보안 중요성 인식 현황
- 보안대비 수준 및 투자 계획

○ **사이버보안 강화를 위해 필요한 지원책**

- 기업의 보안강화를 위해 필요한 지원책
- 안전한 사이버보안 환경 구축을 위한 정책요구

3. 조사 대상

○ **부산지역 매출액 상위 500개 기업(응답 250개체)**

〈응답 기업 업종 현황〉

업종	기업수(개)	비중(%)
제조업	93	37.2
도소매업	69	27.6
건설업	37	14.8
서비스업	26	10.4
운수업	25	10.0
전 체	250	100.0

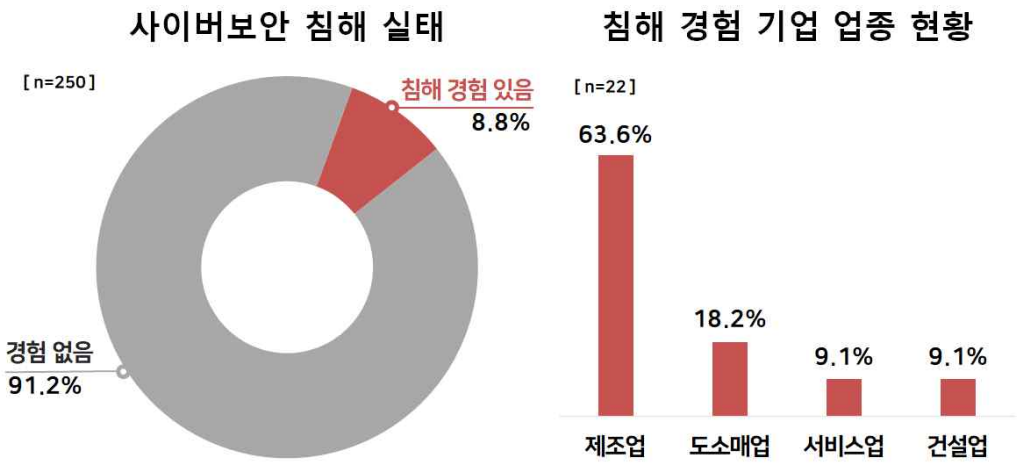
1. 지역기업의 사이버보안 침해 실태

가. 사이버보안 침해 경험

▢ 조사기업의 8.8%는 사이버보안 침해를 경험한적 있다고 응답

○ **업종별로는 제조업이 전체의 63.6%로 가장 많았으며, 도소매업(18.2%), 서비스업 9.1%), 건설업(9.1%) 순**

- 제조업은 최근 디지털 전환 가속화로 디지털 이용률 늘었고, 공정의 스마트화 등으로 인해 사이버 보안위협에 노출되는 기업이 많은 것으로 판단됨
- 한편, 2021년 기준 국내사업체의 1.0%만이 해킹, 악성코드 등의 보안 침해를 경험한 것과 비교해볼 때, 지역기업의 보안침해 경험률 높은 상황(한국정보보호산업협회, 2021년 정보보호실태 조사 결과)

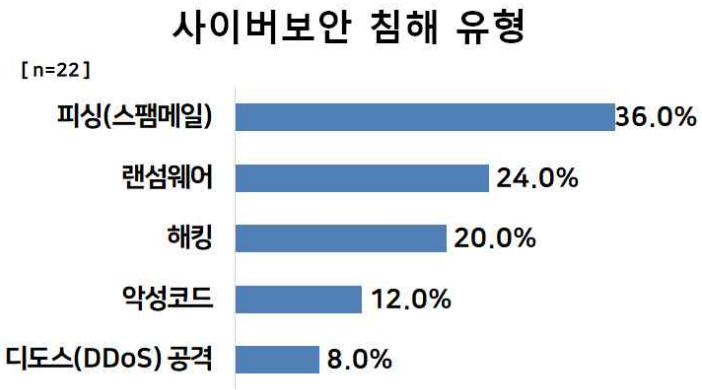


나. 보안침해 유형

▢ 지역기업이 가장 많이 경험한 보안침해 유형은 '피싱, 스팸메일'

○ **응답별 비중을 보면 '피싱(스팸메일)'이 36.0%로 가장 많았으며, 랜섬웨어(24.0%), 해킹(20.0%), 악성코드(12.0%), 디도스 공격(8.0%) 순**

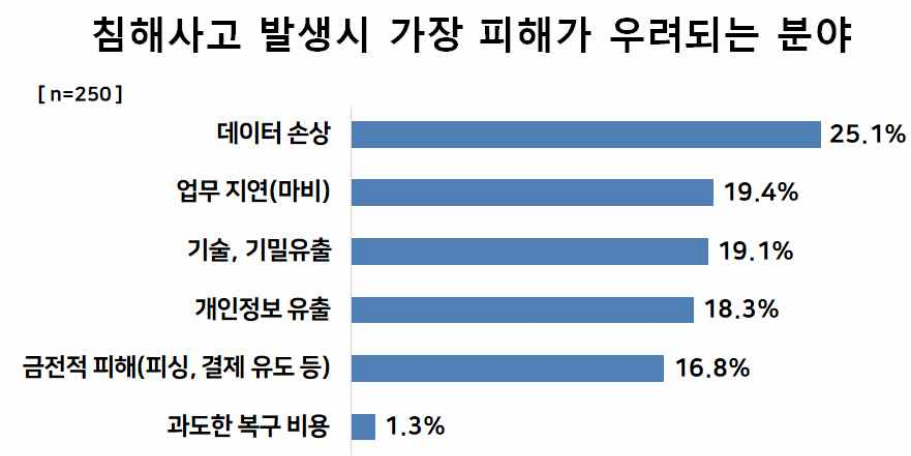
- 기업은 각종 스팸메일, 정보탈취를 목적으로 발송되는 피싱메일 등의 보안위협을 가장 많이 경험하였으며, 특히 침해사고 발생시 정보유출이나 데이터 손상 등의 심각한 피해가 발생하는 랜섬웨어, 해킹 등의 피해를 경험한 기업도 상당수 확인되었음



다. 가장 피해가 우려되는 분야

▢ 지역기업은 보안침해 발생시 '데이터 손상'(25.1%)으로 인한 피해를 가장 우려하는 것으로 나타남

○ 이어 네트워크 공격으로 인한 업무 지연(19.4%), 기술 및 기밀 유출(19.1%), 개인정보 유출(18.3%), 금전적 피해(16.8%), 과도한 복구 비용(1.3%) 순



라. 사이버보안 침해위협 증가 이유

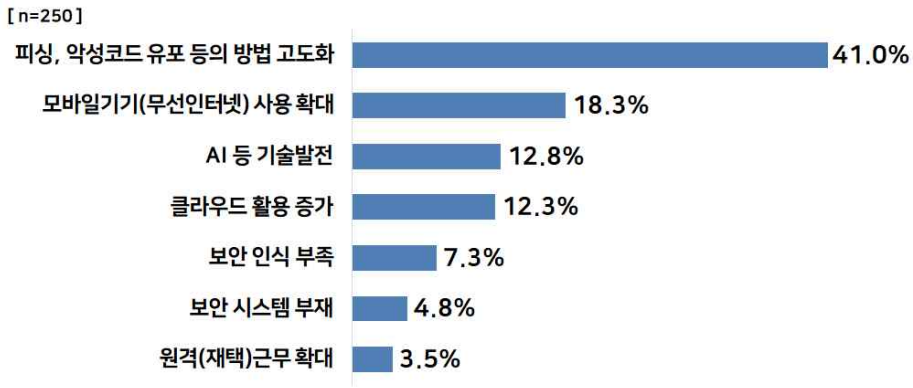
▢ 최근 지역기업 대상 사이버보안 위협이 증가하는 가장 큰 이유는 '피싱, 악성코드 유포 등 침해 방법 고도화' 때문

○ 이어, 모바일기기 사용 확대(18.3%), AI 등 기술 발전(12.8%), 클라우드 활용 증가(12.3%), 보안 인식 부족(7.3%), 보안 시스템 부재(4.8%), 원격(재

택)근무 확대(3.5%) 등으로 나타남

- 기업의 사이버보안 대비 수준을 높이는 것도 중요하지만, 진화하는 보안 위협에 대응하기 위한 기술적·제도적 예방책 마련이 필요

사이버보안 침해 위협 증가 원인



2. 지역기업의 사이버보안 대응 실태

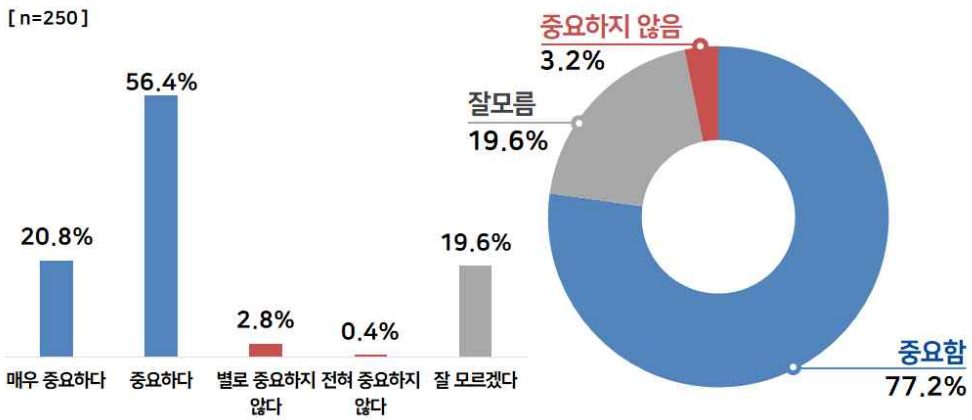
가. 사이버보안 인식 현황

▢ 조사기업의 대다수(77.2%)는 사이버보안이 중요하다고 인식하고 있었음

○ **응답별로는 매우 중요하다(20.8%), 중요하다(56.4%), 잘모르겠다(19.6%), 중요하지 않다(3.2%) 등으로 나타남**

- 사이버보안 침해는 데이터 손상, 업무 지연 등의 심각한 피해를 초래하는 만큼, 지역기업은 사이버보안의 중요성에 대해 충분히 인지하고 있는 것으로 나타남

사이버보안 중요성 인식 현황



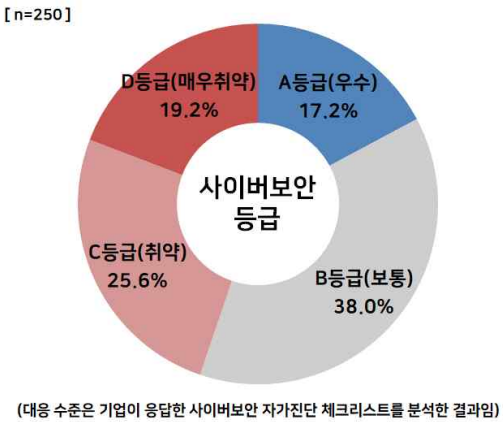
나. 보안대비 수준

▢ 지역기업의 사이버보안 대비 수준 44.8%가 취약(C+D등급)

○ **사이버보안 수준 진단 결과, C등급(취약)과 D등급(매우취약)이 각각 25.6%, 19.2%였으며, 이어 B등급(보통) 38.0%, A등급(우수) 17.2%로 나타남**

- 보안의 중요성을 인식하고 있지만, 그와 별개로 실제 기업의 보안수준은 높지 않은 상황, 대응이 취약한 기업의 보안수준을 강화하는 것 필요

지역기업의 사이버보안 대비 수준



(대응 수준은 기업이 응답한 사이버보안 자가진단 체크리스트를 분석한 결과임)

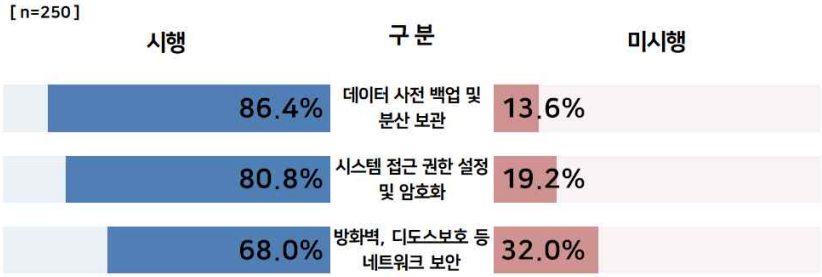
다. 대비책별 시행 실태

▢ 보안위협에 대비하여 '데이터 분산 보관'이나 '시스템 암호화'를 시행 중인 기업 가장 많았음

○ **데이터 사전 백업 및 분산 보관을 실시 중인 기업은 86.4%였으며, 시스템 접근 권한 설정 및 암호화 설정(80.8%), 방화벽, 디도스보호 등 네트워크 보안 실시 중(68.0%) 순**

- 지역기업은 데이터 손상이나 유출로 인한 피해를 가장 우려하는 만큼, 이를 대비하기 위해 데이터 사전 백업 및 분산 보관을 가장 충실히 이행하고 있는 것으로 나타남

지역기업의 사이버보안 대응 현황

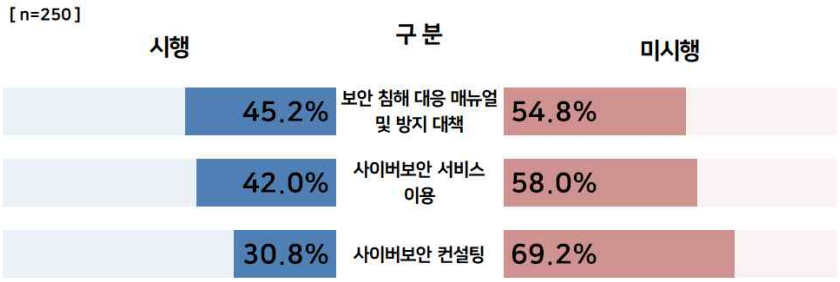


▢ 한편, 사이버보안 컨설팅을 받거나 보안서비스를 이용하는 기업의 비중은 낮았음

○ **사이버보안 컨설팅을 받고 있다고 응답한 기업 30.8%에 불과했으며, 보안서비스 이용(42.0%), 대응 매뉴얼 및 정보유출 방지 대책(45.2%) 등의 대비를 하고 있는 기업은 과반수 이하로 나타남**

- 보안 컨설팅이나, 보안서비스를 이용하기 위해서는 추가적인 비용이 발생하기 때문에 이를 이용하는 기업의 비중은 낮은 것으로 판단됨

지역기업의 사이버보안 대응 현황

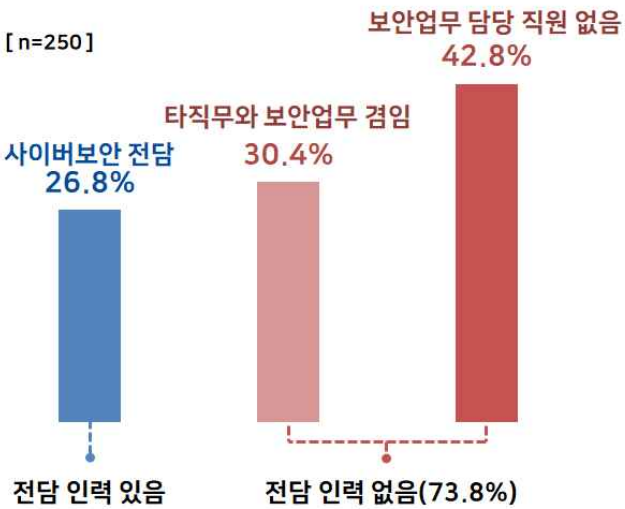


라. 인력 현황

▢ 사이버보안 전담 인력을 보유하고 있는 기업은 26.8%에 불과

○ **조사기업 중 사이버보안 전담직원이 있는 기업의 비중은 26.8%였으며, 이어 보안업무 담당 직원 없음(42.8%), 타 직무와 겸임(30.4%) 등으로 집계**

사이버보안 담당 인력 현황

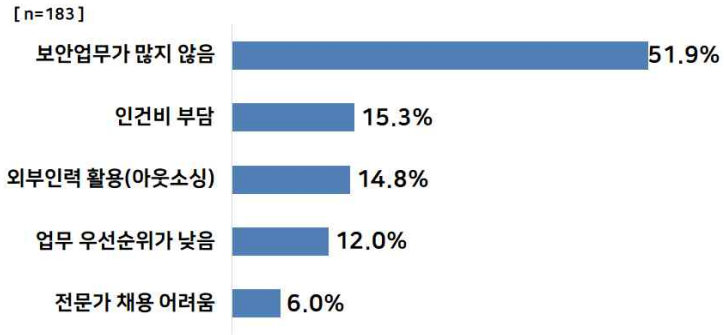


▢ 전담인력을 채용할 만큼 상시보안 업무가 많지 않다고 응답

○ **사이버보안 전담인력이 없는 이유로는 '보안업무가 많지 않음'이 51.9%로 가장 많았으며, 이어 인건비 부담(15.3%), 아웃소싱(14.8%), 업무 우선순위가 낮음(12.0%), 전문가 채용 어려움(6.0%) 순**

- 보안인력이 없을 경우 보안침해 위협에 신속하게 대응할 수 없음, 따라서 이러한 보안공백을 막기 위해 사이버보안 서비스나, 외부보안 업체(인력)를 이용하는 등의 대비가 필요

사이버보안 전담 인력이 없는 이유

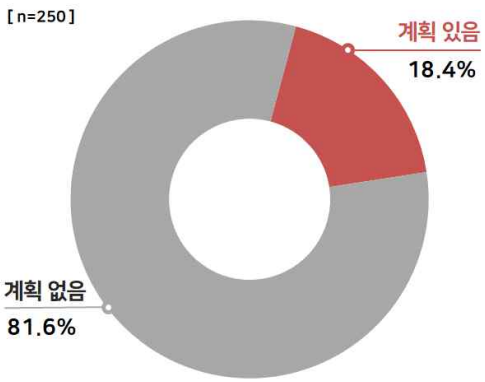


마. 투자 계획

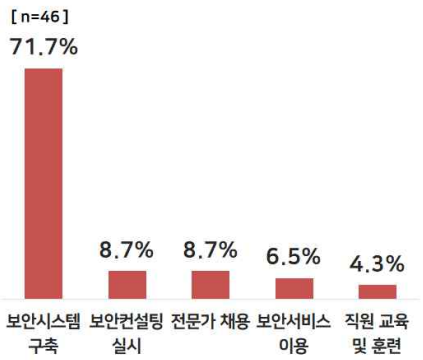
▢ 향후 사이버보안 강화를 위해 투자를 계획 중인 기업은 18.4%였으며, 81.6%는 투자계획이 없다고 응답

○ **투자를 계획 중인 기업은 투자분야로 보안시스템 구축이 71.7%로 가장 높게 나타났으며, 다음으로 보안전문가 채용(8.7%), 보안컨설팅 실시(8.7%), 보안솔루션 이용(6.5%), 직원 교육 및 훈련(4.3%) 순으로 나타남**

사이버보안 투자 계획

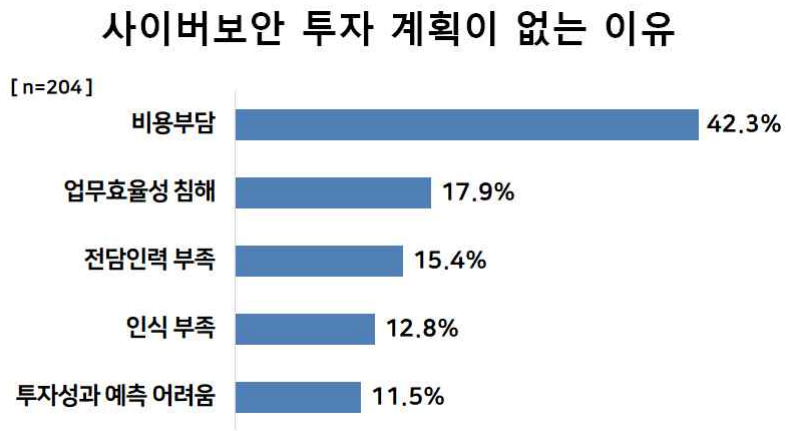


사이버보안 투자 분야



○ **투자계획이 없는 이유는 '비용 부담'이 42.3%로 가장 많았으며, 이어 업무효율성 침해(17.9%), 전담인력 부족(15.4%), 인식 부족(12.8%), 투자성과 예측 어려움(11.5%) 순**

- 보안투자에 취약한 지역기업으로서는 향후 고도화되는 보안침해 위협에 무방비 상태로 노출될 수 밖에 없으므로, 비용부담을 완화할 수 있는 지원책 마련 필요

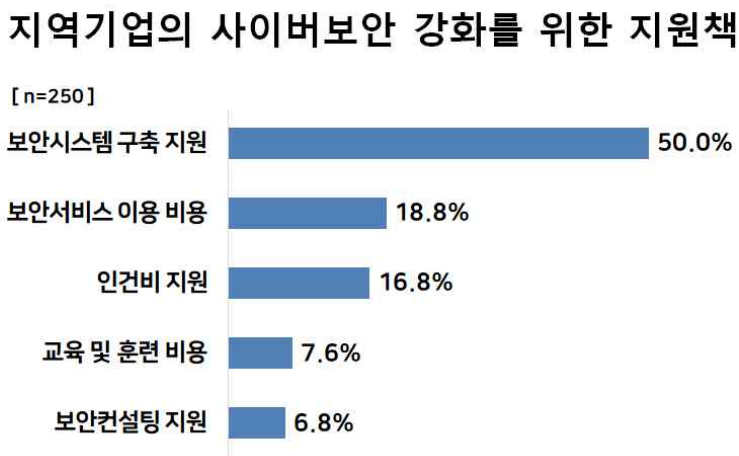


3. 보안강화를 위해 필요한 지원책 및 정책요구

가. 지원책

▢ 지역기업이 가장 필요로 하는 지원책은 '보안시스템 구축 지원'

○ **기업의 사이버보안 강화를 위해 필요한 지원책으로는 보안시스템 구축 지원이 전체의 50.0%로 가장 많았음, 이어 보안서비스 이용 지원(18.8%), 인건비 지원(16.8%), 교육 및 훈련비용 지원(7.6%), 보안컨설팅 지원(6.8%) 순**



나. 정책 요구사항

▢ 안전한 사이버보안 환경을 구축을 위해 필요한 정책으로는 '사이버보안 기술 개발' 지원이 1순위(40.4%)

○ 이어 법제도 강화(22.0%), 보안 인증제도 강화(16.0%), 보안정책 및 가이드라인 제공(16.0%), 보안 전문가 육성(7.2%), 사이버 보안 산업 및 기업 육성(4.0%) 순