

Deloitte.



사이버 사고 대응, 기업 생존을 지키는 실전 전략

사고 발생 시, 기업 연속성을 확보하는 실질적 대응 방안

한국 딜로이트 그룹

One Cyber & Resilience 전문팀

리더 메시지



백철호 파트너

One Cyber & Resilience 전문팀

최근 사이버 보안 사고는 기업의 신뢰와 비즈니스 연속성을 위협하는 중대한 리스크로 떠오르고 있습니다. 사고 초기 대응의 실패는 정보 유출뿐 아니라 고객 이탈, 과징금, 소송 등 치명적인 2차 피해로 이어질 수 있습니다.

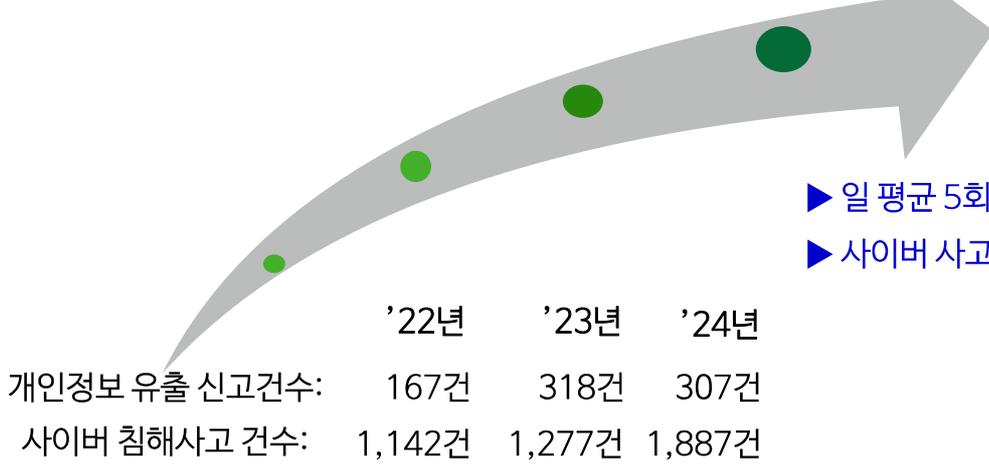
초기 대응의 속도와 정밀도는 피해 최소화의 핵심이며, 이를 위해서는 전문성과 체계를 갖춘 컨트롤 타워를 중심으로 신속하고 일관된 대응이 필요합니다.

결국 사이버 보안 사고 대응 전략은 단순한 위험 관리를 넘어 고객의 신뢰를 확보하고 기업의 경쟁력을 강화하는 중요한 기반이 될 것입니다.

지속적으로 증가하는 사이버 사고 위협

사이버 사고 발생 시 초기 대응이 중요하지만 신속한 대응은 쉽지 않습니다.

'23년 1월 A 통신사 29만 건 유출 과징금 68억 원	'23년 3월 B 플랫폼사 6.5만 건 유출 과징금 151억 원	'23년 11월 C 게임사 221만 건 유출 과징금 75억 원	'24년 8월 D 유통사 158만 건 유출 (조사중)
-------------------------------------------	----------------------------------------------	---------------------------------------------	----------------------------------------



- ▶ 일 평균 5회 이상의 사고 발생
- ▶ 사이버 사고 평균 피해액: 67억

✓ 사이버 보안 사고 발생시 기업의 고려사항

- 1 피해 확산은 현재도 진행 중인 것은 아닌가?
- 2 사고의 원인과 피해 규모는 어떻게 분석할 수 있는가?
- 3 경찰, 한국인터넷진흥원 등 관계기관에 신고는 어떤 절차로 진행해야 하는가?
- 4 외부 전문가 도움이 필요한가?
- 5 향후 기업 비즈니스에 미치는 영향은 어디까지일까?
- 6 언론 및 대외 커뮤니케이션은 어떻게 대응해야 하는가?

✓ 기업의 사고 대응 지연에 따른 사례

신고 지연 →
추가 과징금 부과

악성코드 차단 지연 →
감염 기기 12대에서
3,000대로 확산

퇴사 후 6개월간 설계
도면 외부 반출 지속

고객 대응 미흡 →
고객 이탈률 2배 증가

사이버 사고에 대한 전사적인 대응의 필요성

보안 사고 대응 시, 전사적 협력으로 피해를 최소화해야 합니다.

#1

객관적이고 정확한 사고 원인과 규모 파악

- 사고 유형 별 최적의 전문가로 조사 팀 구성 필요
- 발생원인 및 규모에 대한 조사의 독립성 확보 → 객관성 확보
- 설계 / 운영 / 모니터링 등의 미비 사항 검증

#2

감독, 조사 기관에 대한 효과적인 대응

- 사고 원인, 규모에 대한 정확한 자료 작성 및 제출
- 유관기관과의 원활한 커뮤니케이션 체계 구축
- 불필요한 정보제공으로 발생 가능한 추가 위험 요소 사전 검토 필수

#3

재발 방지를 위한 전사적인 업무 혁신

- 재발 방지를 위한 혁신 업무 선정 및 진행 관리
- IT와 정보보호 업무 뿐만이 아닌 전사적인 비즈니스 및 프로세스 개선
- 신규 기술과 솔루션 도입에 따른 효율적 투자

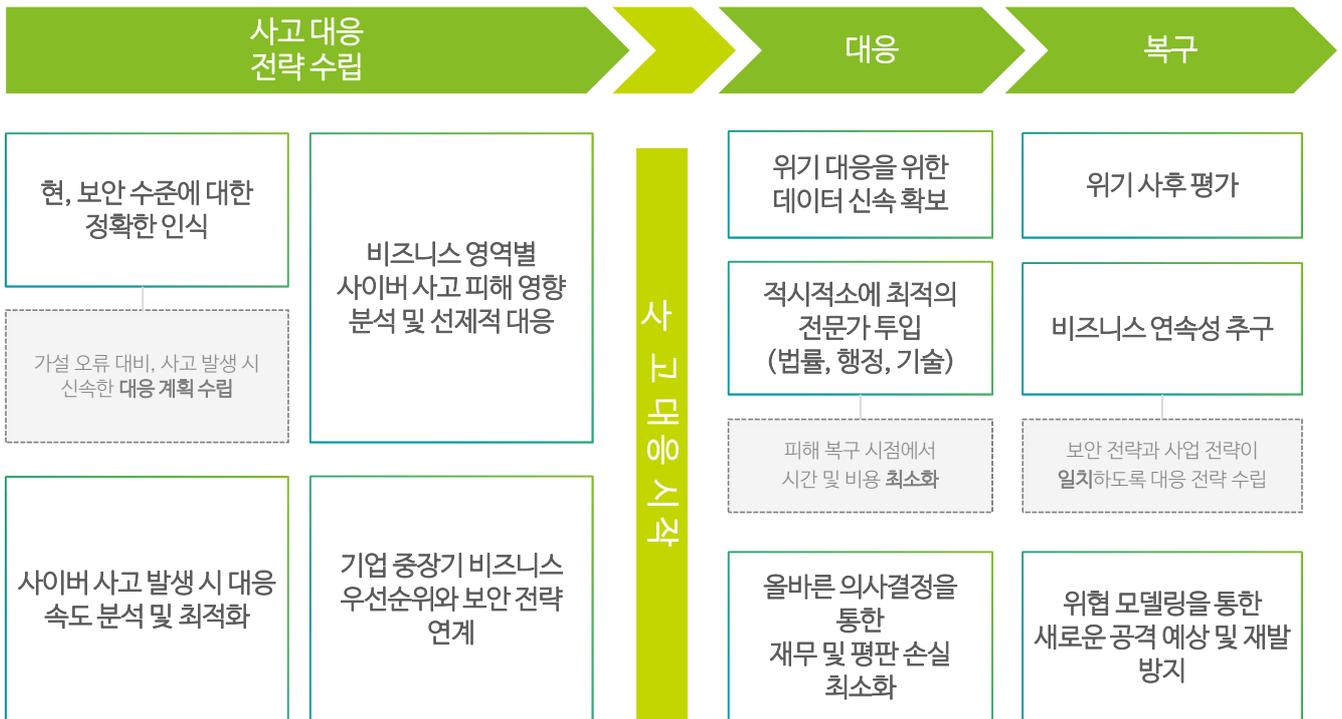
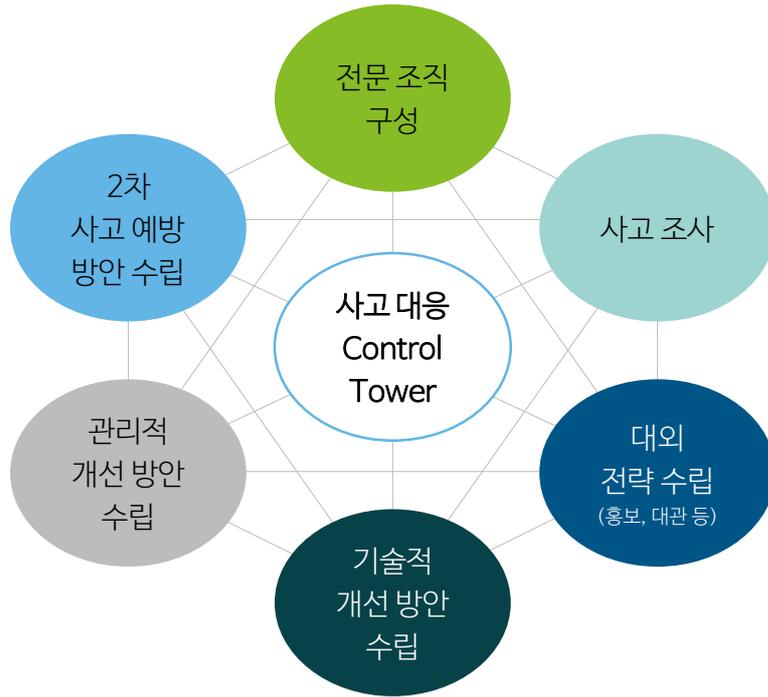
#4

일원화 되고 효율적인 대외 활동

- 사고 원인, 피해 규모 등 민감한 정보에 대한 외부 공개 여부 결정
- 추측성, 악성 기사에 대한 대응
- 고객 피해로 인한 비즈니스 피해 최소화

사이버 사고 대응 전사 컨트롤 타워의 역할

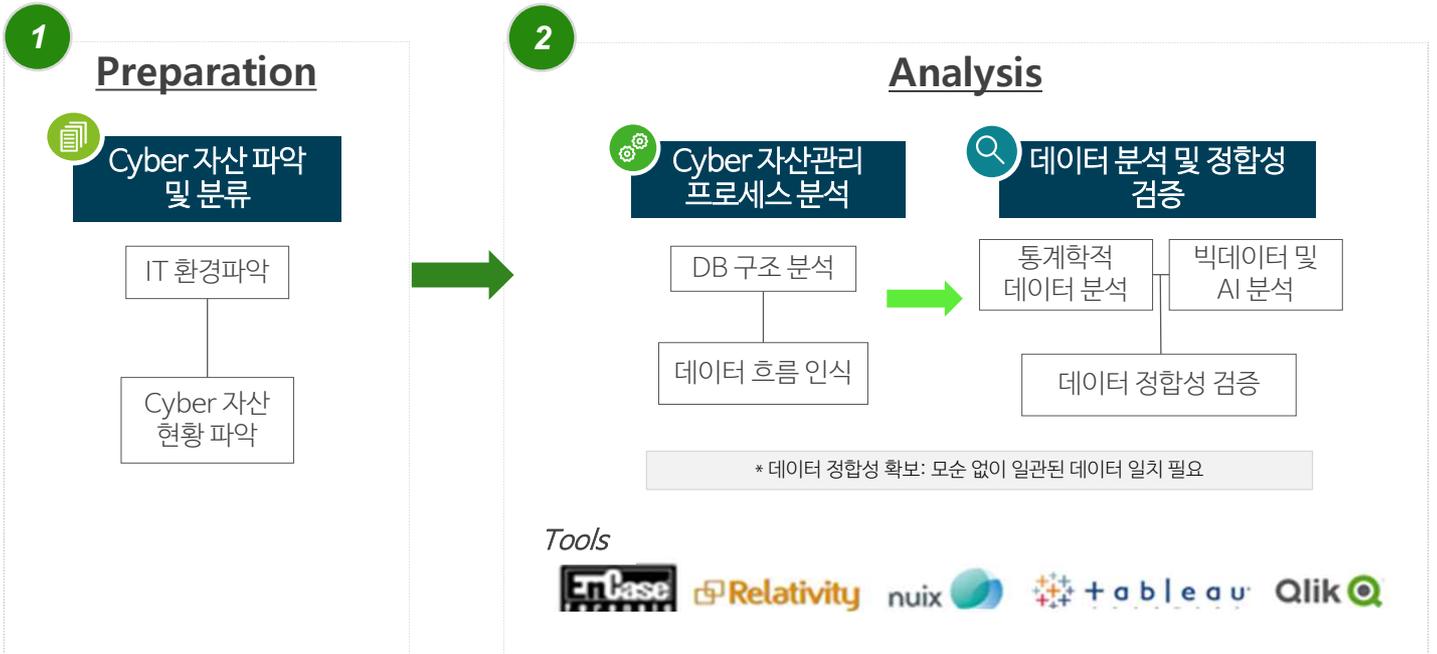
보안 사고 대응 시 컨트롤 타워의 역할이 피해를 경감시킬 수 있습니다.



고객 신뢰 확보 및 Resilience 기반 사이버 사고 대응 전략으로 경쟁 우위 확보

데이터 분석 기반의 사이버 위협 이상 진단

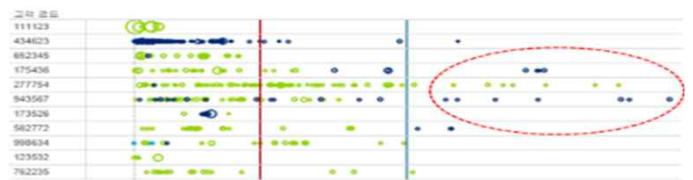
데이터 분석 기반 이상징후 분석 및 사고 식별 프로세스



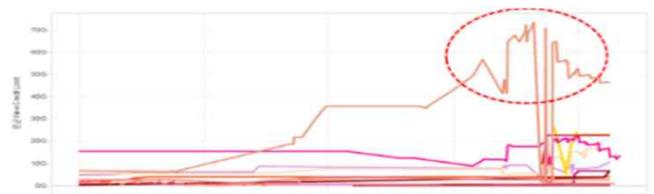
데이터 분석을 통한 이상 진단 예시



특정 업무의 시간대 별 수행 내역



이상 사용자 패턴 확인



대용량 데이터 이동 확인

3 Documentation

Documentation

Cyber 이상 진단



- * Cyber 이상 현황의 근본적 원인
- * As-is Cyber 현황에 대한 To-be 제시

사이버 사고 대응에 필요한 전문성

사이버 사고 대응 컨트롤 타워는 전문 역량을 갖춘 인력들로 구성되어야 합니다.

▶ 신속하고 정확한 사고 대응 전문성

- 사고 유형별 전문가 구성 능력
- 개인정보·통신 관련 법률 대응 역량
- 악성코드·모의해킹 등 기술 분석 전문성
- 디지털 포렌식 등 증거 수집 역량
- 대외홍보, 언론 대응을 위한 전문가 활용 역량

▶ 비즈니스 연속성 확보를 위한 전략

- 기업 비즈니스 이해와 연속성 확보 전문성
- 다양한 산업 분야 경험 및 지식
- 프로세스·위험·내부통제 개선 경험

▶ 경영진 및 기술부서 간 원활한 커뮤니케이션

- 경영진의 빠른 의사결정을 위한 커뮤니케이션 능력
- 기술 부서의 요구사항과 애로사항 이해 및 전달 역량

▶ 장기 프로젝트 관리 및 성과 평가 능력

- 재발 방지를 위한 다양한 프로젝트의 관리 경험
- 재발 방지 효과에 대한 정확한 성과 측정 체계 확보

성공 사례

여러 딜로이트 고객사가 사고 발생 후 종합적이고 효과적인 대응을 통해 피해를 최소화할 수 있었습니다.

개인정보 유출 피해 최소화 (해외 대응)



- ✓ 외부 전문가를 활용한 조사 분석 팀 구성
- ✓ 전사적 지원으로 정확한 사고 분석
- ✓ 해외 가입자 다수 발견
- ✓ GDPR(유럽), CCPA(미국 캘리포니아) 등 선제적 법률·행정 대응 성공

기밀 정보 유출로 발생한 소송 및 피해 보상 성공



- ✓ 유출 징후 확인 후 신속한 컨트롤 타워 구성
- ✓ 유출된 자료 전수 확보
- ✓ 비즈니스 피해 규모 산정
- ✓ 국내·해외 빠른 소송으로 피해 최소화

장기적인 사이버 업무 혁신의 성과 확보



- ✓ 개인정보 유출 후, 재발 방지 및 혁신을 위한 별도 조직 구성
- ✓ 전사적 프로세스 혁신
- ✓ 확대 예산 확보 및 활용
- ✓ 국제 기준 보안성 평가 점수 대폭 상승 견인
- ✓ 지속적 모니터링 및 재발 방지 체계 확립

정확한 커뮤니케이션으로 비즈니스 영향 최소화



- ✓ 악의적 데이터 조작으로 인한 협력사 비용 산정 사고 발생
- ✓ 사고 원인 분석과 재발 방지 대책 수립
- ✓ 협력사와의 정확한 사고 원인, 규모, 재발 방지 대책 커뮤니케이션
- ✓ 지속적인 관계 유지 체계 구축

One Cyber & Resilience

한국 딜로이트 그룹은 정보보호·보안과 리스크 관리에 대한 차별화된 방법론과 전문인력을 보유하고 있습니다. 딜로이트 One Cyber & Resilience팀은 고객의 비즈니스 환경과 산업특성에 따른 정보보호·보안 리스크를 식별하여 선제적 대응방안을 마련하고 사고발생시 체계적인 대응전략 수립을 지원합니다.

Professionals



백철호 파트너

One Cyber & Resilience

Tel: cbaek@deloitte.com

Mail: 02-6676-2250



서영수 파트너

One Cyber & Resilience

Tel: youngseo@deloitte.com

Mail: 02-6676-1929



유선희 파트너

One Cyber & Resilience

Tel: sunhyou@deloitte.com

Mail: 02-6676-2956



문범석 파트너

One Cyber & Resilience

Tel: bsmoon@deloitte.com

Mail: 02-6676-2949



이창성 파트너

One Cyber & Resilience

Tel: changsulee@deloitte.com

Mail: 02-6099-4888



앱스토어, 구글플레이/카카오톡에서 '딜로이트 인사이트' 를 검색해보세요.
더욱 다양한 소식을 만나보실 수 있습니다.

Deloitte. Insights

성장전략부문 대표

손재호 Partner

jaehoson@deloitte.com

딜로이트 인사이트 리더

정동섭 Partner

dongjeong@deloitte.com

인사이트 편집장

박경은 Director

kyungepark@deloitte.com

연구원

신인식 Manager

insshin@deloitte.com

Contact us

krinsightsend@deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other.

DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more. Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.

DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

본 보고서는 저작권법에 따라 보호받는 저작물로서 저작권은 딜로이트 안진회계법인("저작권자")에 있습니다.

본 보고서의 내용은 비영리 목적으로만 이용이 가능하고, 내용의 전부 또는 일부에 대한 상업적 활용 기타 영리목적 이용시 저작권자의 사전 허락이 필요합니다. 또한 본 보고서의 이용 시, 출처를 저작권자로 명시해야 하고 저작권자의 사전 허락없이 그 내용을 변경할 수 없습니다.