대•중소기업 상생을 위한 시큐리티 윈윈 전략

서울과학종합대학원 산업보안MBA
교수 조병철

중소기업 기술유출 심각 …

바른언론 빠른뉴스
연합뉴스

인쇄 | 닫기

中企 기술유출 심각…`인력 빼가기' 피해 급증

(서울=연합뉴스) 강종훈 신재우 기자 = 중소기업의 기술유출 피해액이 해마다 증가하는 것으로 나타났다. 기술 유출의 40% 이상은 대기업 등의 `인력 빼가기'에 의해 이뤄졌다.

22일 중소기업청과 중소기업중앙회 등에 따르면 작년 기술유출을 경험한 중소기업은 12.5%였으며 유출 한 건당 피해액은 평균 15억8천만원이었다.

* 出處: 연합뉴스(2012.10.21) & 내일신문(2012.10.22)

기술유출 사례

우월한 지위(‘甲’)에 의한 기술유출 사례

① 사례 1

전산시스템 구축·관리 분야 대기업인 A社는 증권거래 중개시스템 구축 project를 수주하기 위해 국내 유일의 노하우 보유 기업인 중소기업 B社의 핵심 인력을 스카웃하여 영업비밀을 획득, 프로젝트 수주에 성공

* 出處: **http://www.tpcc.or.kr/portal/ppi/partner.do**

기술유출 사례

열등한 지위(‘乙’)에 의한 기술유출 사례

① 사례 1

대기업 A社는 경쟁사인 대기업 B사가 독자 개발한 이동식 발전설비 PPS 설계도면 등을 B사의 협력업체인 중소기업 C사를 통해 불법 취득

※재판 결과:

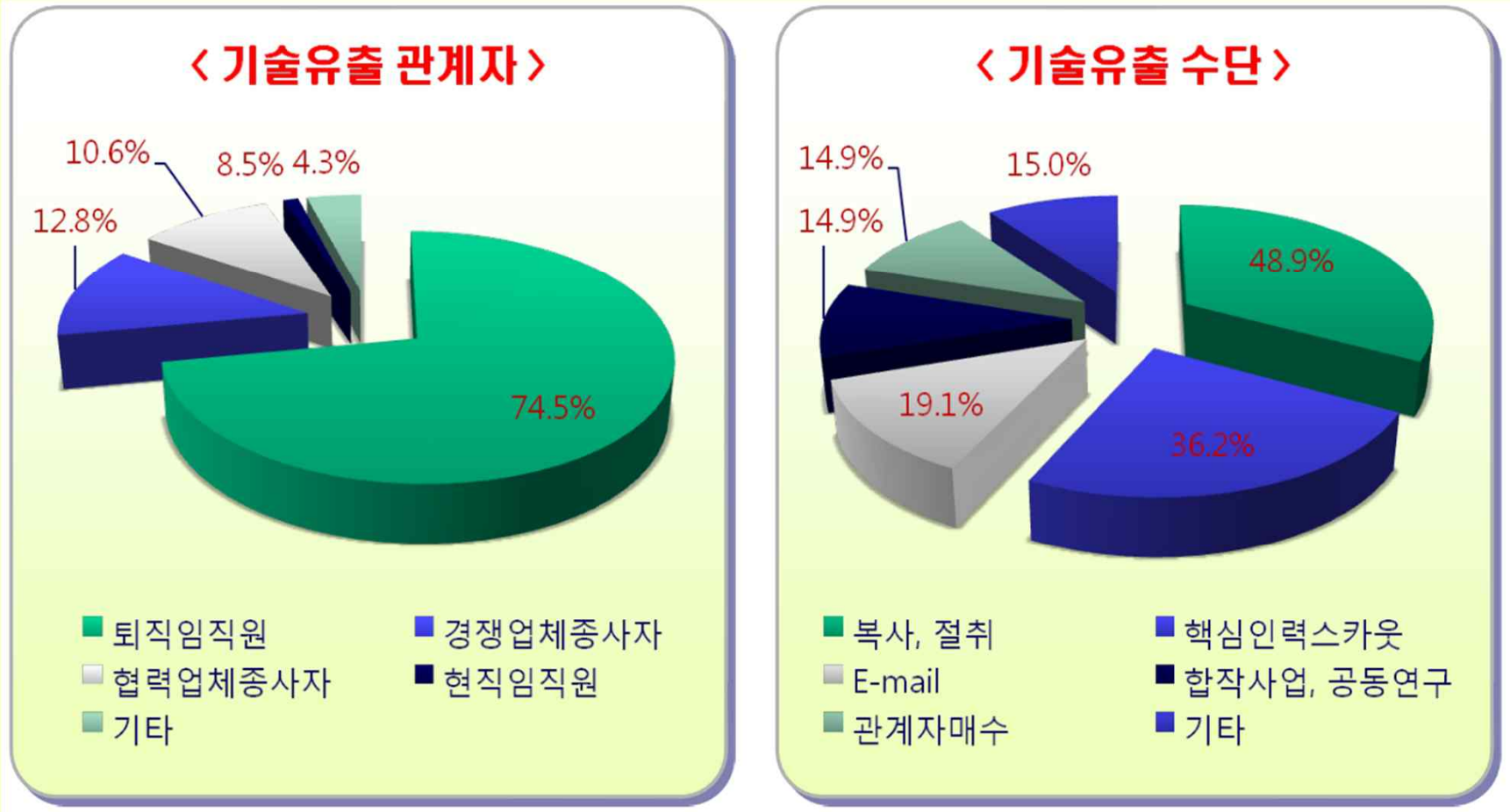
중소기업 C사 직원 3명: 징역 10월

A사 임직원 4명: 징역 (1명1년,3명10월), A사 법인: 20억 벌금

② 사례 2

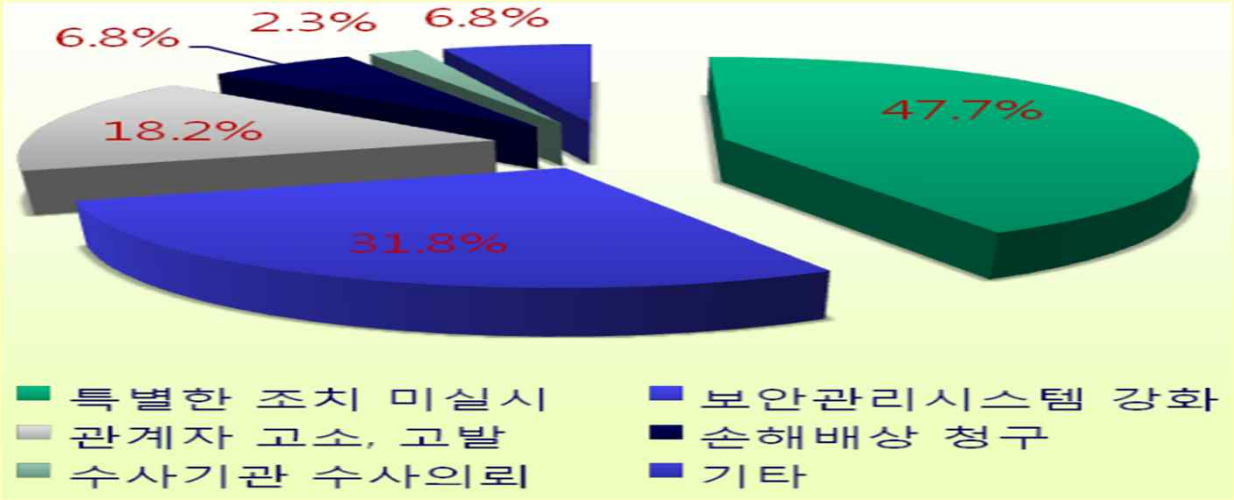
용접기술을 개발하는 A사는 연구원 B를 채용하고 신기술 개발에 참여 시켰으나 기대 만큼의 성과를 내지 못하자, CEO는 B직원의 역량이 부족하다고 판단하여 해고함. 이에 불만을 품은 B직원은 A사의 핵심기술을 몰래 가지고 나가, 취업을 대가로 경쟁업체에 넘김

중소기업 기술유출 관계자 및 수단



* 出處: 중기청, "중소기업 기술유출 실태 및 기술보호 정책", 2012. 1

기술유출 후, 중소기업의 조치



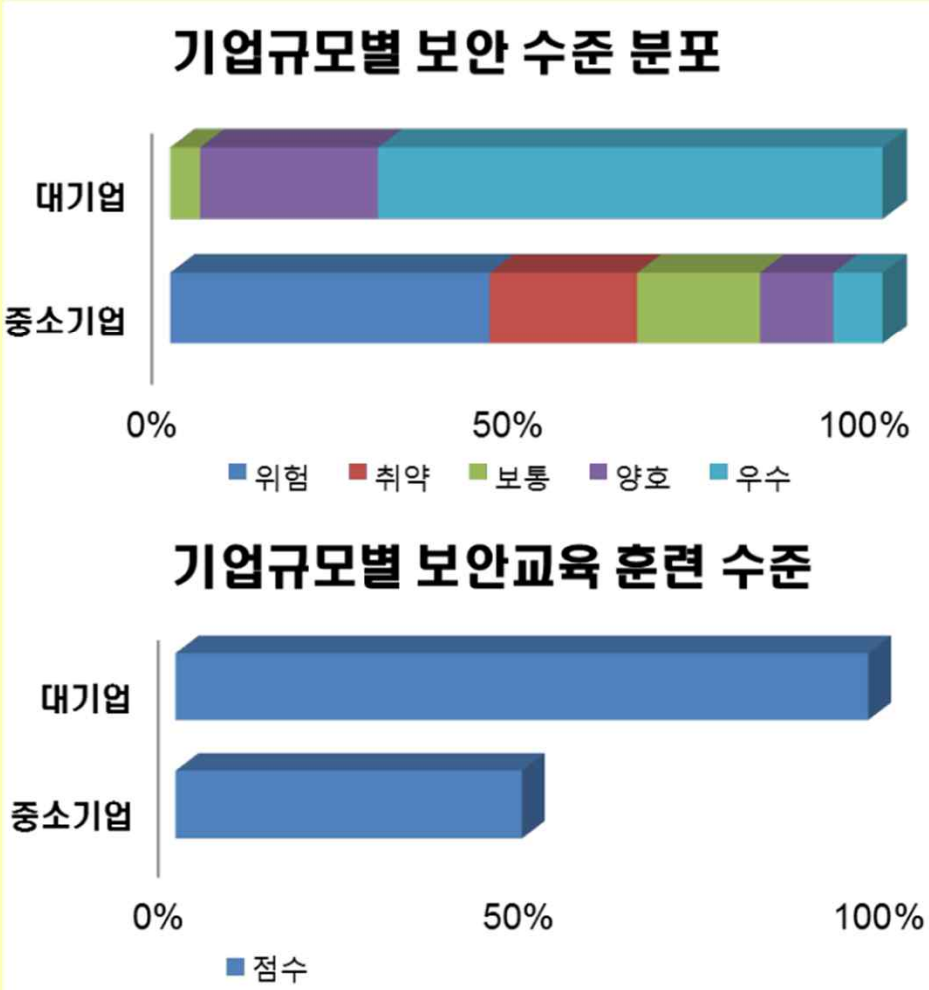
정부의 대책안 …

1. 기술유출 분쟁조정기구 설치
   - ➢ 중재 보다는 징벌적 손해 배상제 같은 강력한 제재 조치 요구

2. '트레이드 머니'(이적료) 지급 : 중소기업 인력을 스카우트할 경우
   - ➢ "기술인력 유출을 정당화하고 합법화하는 조치"라며 반대

3. 피해액의 최대 10배 배상: 중소기업 기술탈취 적발 시 (인수위)

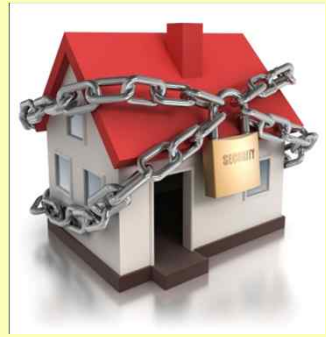
대•중소기업 보안실태



구 분	대기업	중소기업
보안업무조직과 전담자 존재	87.5%	34.5%
보안관리규정보유 및 주기적 갱신	87.5%	27.6%
보안관리규정 공지	75.0%	24.5%
위험평가 실시	87.6%	3.5%
자산분류기준 존재 및 분류 기준 준수	91.6%	44.8%
출력물/전자문서 관련 권한 설정	87.5%	55.1%
보안 서약서 작성 보관	87.5%	58.6%
보안요원 배치 및 보안상황실 운영	95.8%	24.1%
외부 송신 e-mail 통제	75.0%	27.6%
저장매체 사용 통제	95.8%	37.9%

* 出處: 신현구, “대-중소기업의 산업기술보호 정책 추진방향”, 2012. 5

보안의 중요성



1. 기업의 競爭力은 물론 生死를 결정

2. 사업기회 상실: 협력업체도 보안수준 인증 요구

3. 기업의 신뢰성, 이미지 추락

4. 법규 위반에 따른 민형사상의 책임
   산업기술유출방지법, 영업비밀보호법, 개인정보보호법 관리미흡으로 유출될 경우 → 민•형사상의 책임

5. 기업경영의 기밀성, 무결성, 가용성 상실

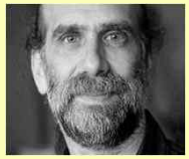
보안은 사슬이다.

Security expert,
Bruce Schneier

Security is a chain; it is only as secure as the weakest link.
보안은 사슬과 같아서, 가장 약한 고리만큼만 안전하다.

☞ 大企業이 아무리 막강한 보안을 구축해도, 보안수준은 協力業體 (중소기업) 의 보안역량에 의해 결정된다.
즉, 협력업체를 통해 정보가 유출되면 말짱 도루묵!

보안은 프로세스다.



Security expert,
Bruce Schneier

Security is a process, not a product. 보안은 제품이 아니라, 프로세스다.

☞ 기업보안은 독자 구축한 보안제품만으로는 안되고, 위협에 대응할 수 있는 체계를 구성원(기업內 or 기업間)들이 함께 만드는 것이다.

생존戰略과 保安(Security)

나 살고, 너 죽고 (弱肉强食 형)		
	살고	죽고
나	●	
너		★

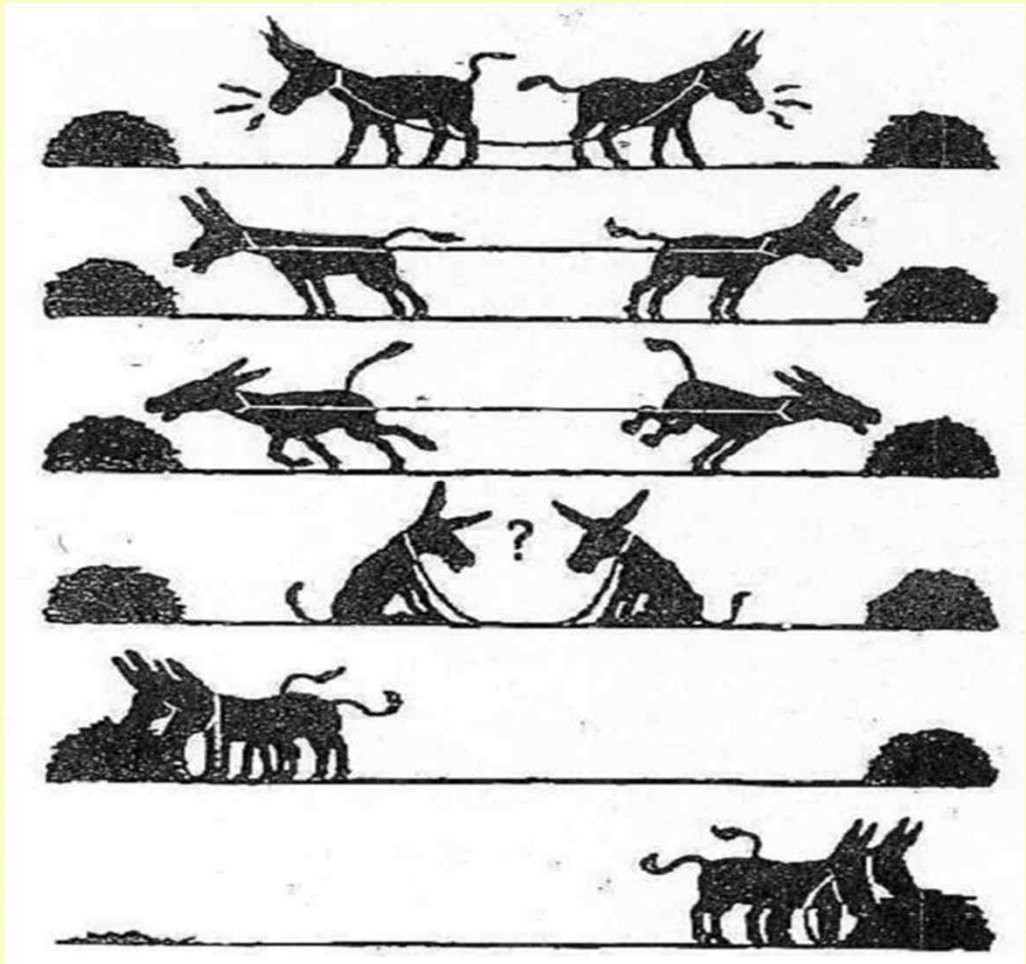
나 죽고, 너 죽고 (자살테러 형)		
	살고	죽고
나		★
너		★

나 죽고, 너 살고 (예수그리스도 형)		
	살고	죽고
나		★
너	●	

나 살고, 너 살고 (상생협력 형)		
	살고	죽고
나	●	
너	●	

출처: 윤석철, 삶의 정도, 2006

상생협력의 필요성



출처: **http://www.edecision4u.com/Partner_program.html**

대•중소기업, 보안분야 상생협력 전략

글로벌 동반성장을 위한
공동보안체계 구축

- 중소기업 보안수준 평가 후, **보안인증 및 인센티브 부여**
- 중소기업 보안시스템 도입을 위한 **예산 및 기술 지원**
- 개별 중소기업 여건에 맞는 **맞춤형 보안 컨설팅**
- 중소기업 보안관리체계 구축을 위한 **진단 및 지도**
- 보안의 중요성에 대한 **인식 공유 및 확산**(공동세미나 개최 등)

중소기업 기술보호, 相生협력으로 해결

1. 중소기업 기술보호 선포식
   정부와 대기업이 협력해 중소기업 기술을 보호하고, 건실한 相生발전을 도모

2. 선언문
   △기술보호를 위한 동반자적 협력 지속 △기술보호 인프라 구축을 위한 인력·기술 지원
   △기술유출 방지를 위한 공정한 거래 관행 유지 △기술보호 중요성에 대한 인식 확산

3. 참여 대기업: 현대차, 포스코, 삼성전자, LG전자, SK텔레콤, 호남석유화학 등 12개

출처:http://news.smba.go.kr/news/board.do?method=execView&sc.newsId=16157&sc.sectionId=24

保安분야, 相生協力 사례 (현대•기아차)

- 보안 진단 및 지도: 연2회, 170개 이상의 1~2차 부품 협력업체 대상
  - 관리적, 물리적, 기술적 보안 全 영역에 걸쳐 점검
  - 현대차 제공 기술자료 미 삭제• 복구가능 상태로 방치 등 지적
- 보안 인증제 실시: 가이드라인 제시 후, 평가해 협력업체 보안수준을 보증
- 협력업체마다 서로 다른 보안수준을 上向 平準化하고, 완성車와 부품社간 글로벌 동반성장을 위한 보안 강화
- 현대•기아차: 기술유출 등 발생 가능한 보안 사고를 예방하고
- 중소기업(협력업체): 대기업의 도움으로 보안 시스템을 구축

保安분야, 相生協力 사례 (포스코)

- 협력업체의 보안수준은 15%로 포스코의 85%와 비교해 매우 열악
  - 상당수 협력사가 '보안규정', '보안서약서' 부재 등 관리적, 물리적, 기술적 보안 全 영역에서 매우 미흡
- 맞춤형 보안컨설팅 실시
  - 협력업체 여건을 고려, '즉시실천', '단기개선' , '중장기 개선' 과제로 구분하여 제안하고, 협력업체는 적극 호응
- 모기업과 협력업체(중소기업)의 상생협력을 통한 보안관리체제 구축

保安분야, 相生協力 사례 (대우조선해양)

- 협력사(중소기업) 기술자료 임치제도를 도입, 동반성장을 도모
- 협력사 기술자료를 '대중소기업 협력재단'에 임치함으로써
  - 협력업체(중소기업)의 기술유출을 방지하고,
  - 모기업(대우조선해양)의 안정적 사용을 동시에 보장
- 한편, 대우조선해양은 임치비용 전액을 부담함으로써
  - 모기업이 앞장서 협력사 기술을 보호하는 모범적 동반성장 토대 구축

중소기업 자체 보안능력 배양

정부와 대기업이 아무리 지원해도, 중소기업 스스로 변화하지 않으면 無用之物

- 보안에 대한 임직원의 중요성 자각, 경영의 핵심 요소로 통합
- 보안 정책•조직 •교육 • 점검 등 보안관리 체계 구축 및 관리
- 핵심인력 • 퇴직자 등에 대한 보안조치 강화
- 기본적인 보안 예산 투자

깨진 유리창 이론(Broken window theory)

건물의 유리창 하나가 깨진 채로 방치된다면, 유리창을 더 깨도 문제 될게 없다는 신호로 인식되고, 결국은 우범지대로 전락된다.

☞ 경영자가 사소한 보안위해 요소를 방치하면, 직원들의 보안 무관심 (or 무시) 분위기가 확산되며, 결국 보안관리 不能 상태로 귀결된다.

보안실태 자가진단


http://www.tpcc.or.kr/portal/pmy/selfDiagnosis.do - Windows Internet Explorer
http://www.tpcc.or.kr/portal/pmy/selfDiagnosis.do
예상 보안점수
30 점
STEP 1
보안정책
STEP 2
자산관리
STEP 3
인적자원 관리
STEP 4
시설관리
STEP 5
IT 보안 관리
STEP 6
기업 유출 대응
보안규정을 보유하고 있는가?
보유하고 있다
보유하고 있지 않다

보안실태 진단항목

1. 보안 정책 : 기업의 정보보안 정책을 체크 합니다.

2. 자산 관리
   기업 자산에 대한 분류, 보호, 통제 등의 보안 실태를 체크 합니다.

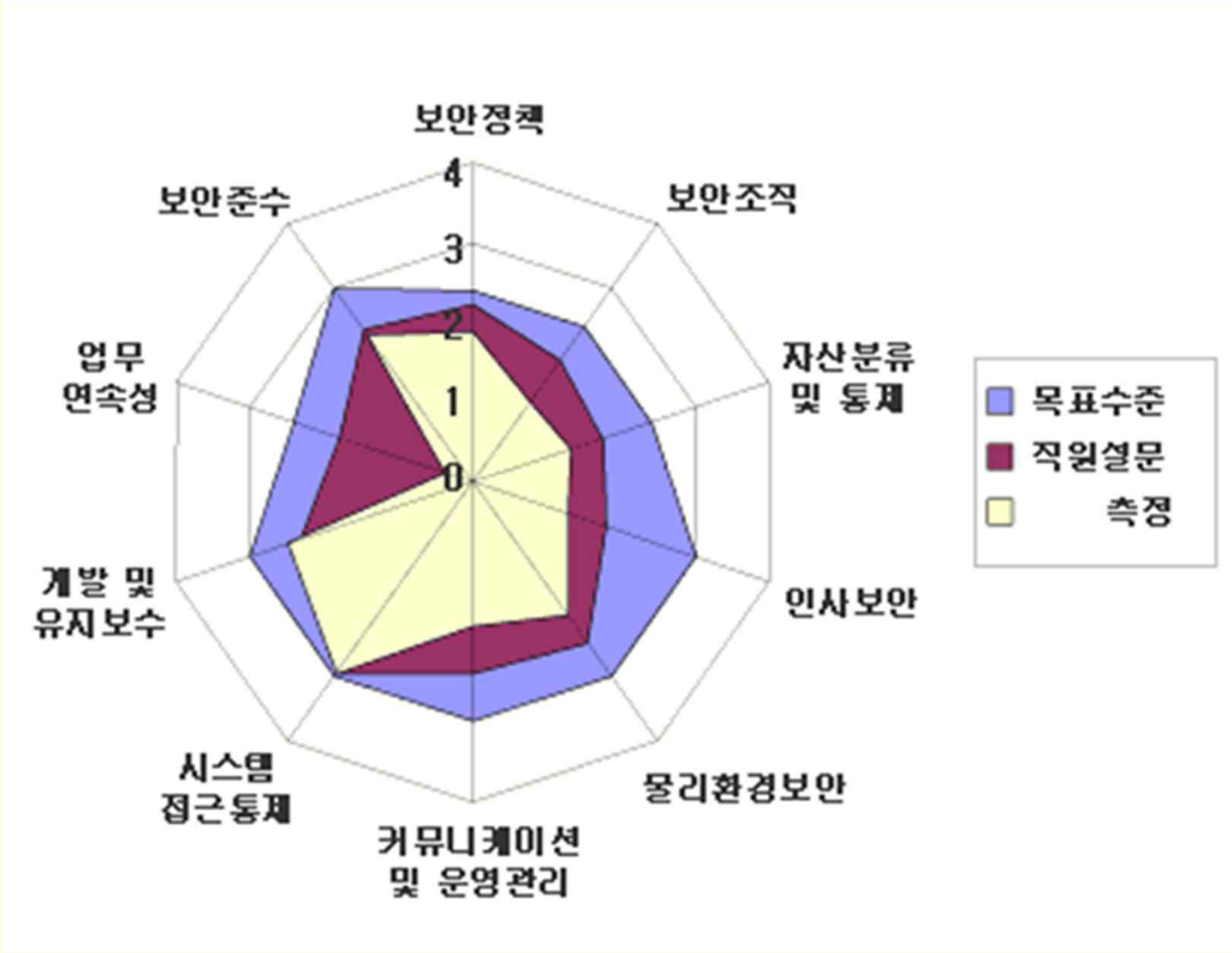
3. 인적 자원 관리
   기업의 인적자원에 대해 채용, 고용 중 그리고 퇴직 시의보안 실태를 체크 합니다.

4. 시설 관리 : 기업의 출입통제 등의 물리적, 환경적 보안 실태를 체크 합니다.

5. IT 보안관리
   기업 IT 자산에 대해 운영절차, 제3자 운영 시의 보안, 시스템 도입 시 고려사항, 악성코드 및 해킹에 대한 대비, 정보 자산의 백업과 매체의 관리, 정보교환 시의 보안, 정보 시스템의 감사, 정보 접근통제 등을 체크 합니다.

6. 유출사고 대응
   기업자산에 대해 보안사고 예방 및 점검, 사고 시 대응책 등을 체크 합니다.

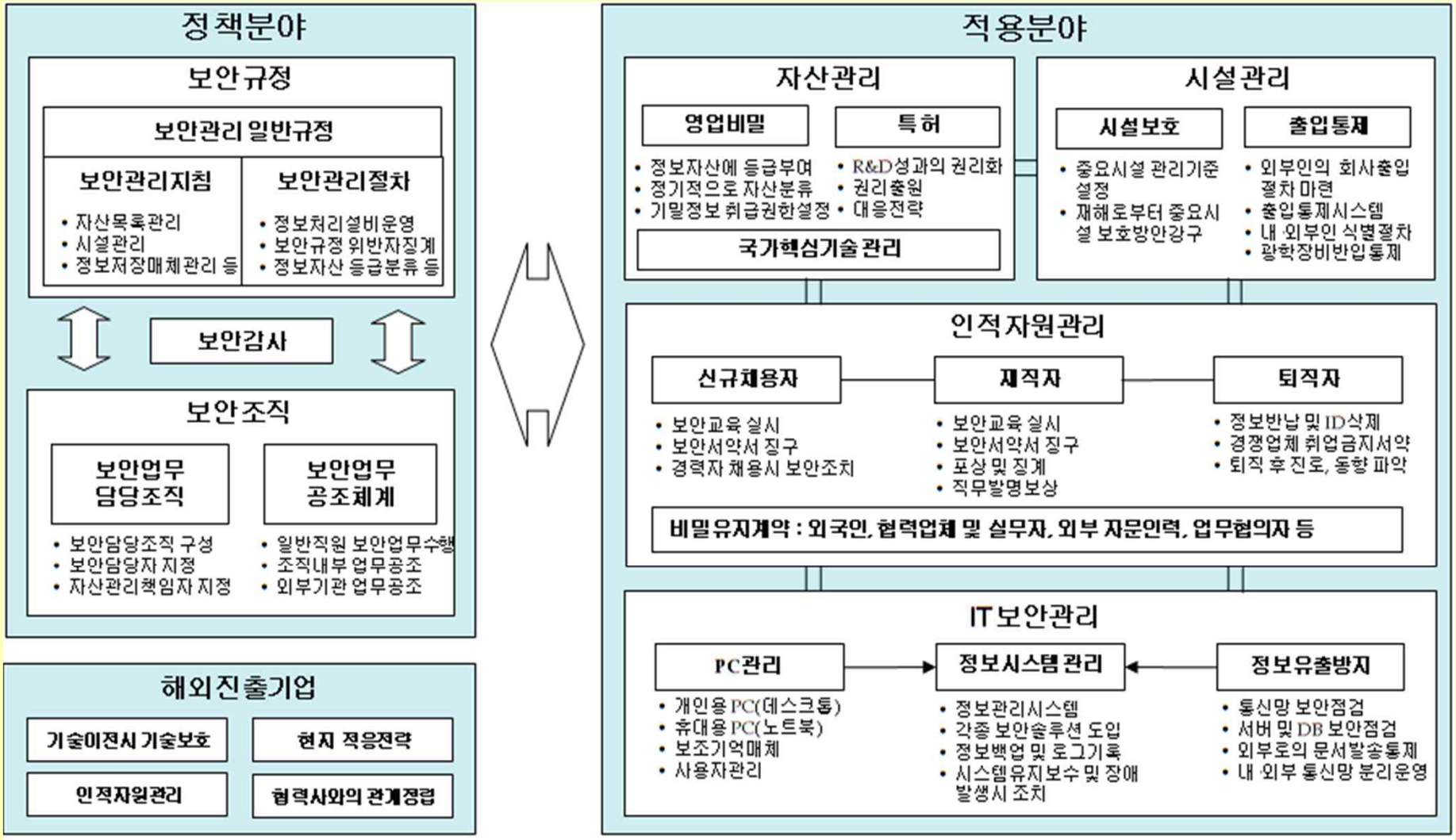
보안수준 평가 및 목표설정



보안관리 체계 개념도

* 出處: **http://www.ahnlab.com/kr/site/product/consultType1.do**

중소기업 보안추진 가이드라인



* 出處: 중기청, 중소기업 기술유출 대응매뉴얼 , 2007.12

주요 참고자료

1. 신현구, “대-중소기업의 산업기술보호 정책 추진방향”, 2012. 5
2. 원병철, “보안 시스템 상생협력으로 기술유출 철통방어”, www.boannews.com/media/view.asp?idx=28915
3. 윤석철, 삶의 정도, 2006
4. 조원동, “중소기업형 스톡 옵션제”, 서울신문 2012.06.23
5. 중기청, “중소기업 기술유출 실태 및 기술보호 정책”, 2012. 17.
6. 중기청, 중소기업 기술유출 대응매뉴얼, 2007.12
7. http://postfiles6.naver.net/20120622_229/g4bnipa_1340349964135lvwPN_JPEG/bgimage_(38).jpg?type=w
8. http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0001806518
9. http://www.tpcc.or.kr/portal/ppi/partner.do
10. http://www.edecision4u.com/Partner_program.html
11. http://news.smba.go.kr/news/board.do?method=execView&sc.newsId=16157&sc.sectionId=24
12. http://www.ahnlab.com/kr/site/product/consultType1.do

감사합니다.

산업보안 MBA / 산업보안연구소
교수, 연구위원, EnCE
공학박사 조 병 철

윤리·지속경영 대학원 평가
'The Global Top 100' 선정

서울과학종합대학원 www.assist.ac.kr
120-808 서울특별시 서대문구 대현동 67-7
Phone. 070 7012 2721 Fax. 02 360 0797 Mobile. 011 247 5178
E-mail. bcho@naver.com, bccho@assist.ac.kr