

# Profiling Insider Threats & Pre-detection Model

---

*2012.3.3 FORENSIC INSIGHT*

*Kevin Koo*

*(kevinkoo001@gmail.com)*





- **Case Studies**
- **INSIDERS**
- **Insider Threats**
- **Pre-detection Model for Insider's Information Theft and Manipulation**



SYNTESS®

4 FREE BOOKLETS  
YOUR SOLUTIONS MEMBERSHIP

4 FREE E-BOOKLETS

# Insider Threat

**PROTECTING THE ENTERPRISE FROM SABOTAGE, SPYING, AND THEFT**

**Prevent Employees and Contractors from Stealing Corporate Data**

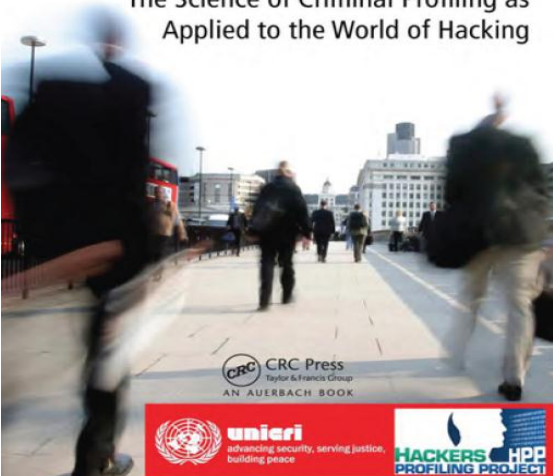
- Learn Why Internal Threats Are Exponentially More Dangerous Than External Threats
- Profile Insider Threats for the Financial, Banking, Commerce, and Government Segments
- Get Expert Perspectives from Authors with Years of Central Intelligence Agency, National Security Agency, and Private Sector Experience

Dr. Eric Cole  
Sandra Ring

RAOUL CHIESA • STEFANIA DUCCI  
SILVIO CIAPPI

# PROFILING HACKERS

The Science of Criminal Profiling as Applied to the World of Hacking




CRC Press  
Taylor & Francis Group  
AN AUERBACH BOOK

unicri  
advancing security, serving justice,  
building peace

HACKERS HDP  
PROFILING PROJECT

ADVANCES IN INFORMATION SECURITY

# Insider Attack and Cyber Security Beyond the Hacker



**Edited by**  
Salvatore J. Stolfo  
Steven M. Bellovin  
Shlomo Hershkop  
Angelos Keromytis  
Sara Sinclair  
Sean W. Smith



## 1. 중소기업 독자개발 기술 유출 사고 (2009)

- 국내 중소기업 J사 독자적으로 개발한 수소저장합금 냉난방 기술
- 내부 직원들이 현금 200억 원과 부회장 등의 직책을 약속 받고 중국으로 유출 (수소저장능력이 큰 금속 등의 합금장치에 수소를 주입하거나 빼내면서 전력소비가 기존 제품에 비해 10% 수준으로 냉난방 기능을 구현하는 기술)

## 2. 내부자 악성코드 고의 유포 시도 (2008)

- FannieMae사: 미연방정부로부터 자금을 받아 미국 내 주택문제와 주택담보 대출시장의 유동성과 안전성을 제공하기 위해 설립된 금융회사
- 마크와나(Babubhai Makwana): 소프트웨어 엔지니어로 4,000여대 전체서버 접속권한
- 처우에 불만을 품고 2009년 1월 31일 오전 9시 이후에 자동으로 전 서버의 데이터를 삭제하는 일종의 논리 폭탄을 제작하여 유포한 혐의

## 3. 전직 인텔 직원의 기밀 유출 사고 (2008)

- 경쟁사인 AMD로 이직하면서 수십억 달러에 달하는 기밀문서를 불법 다운
- 수사결과 용의자는 100여 쪽에 달하는 기밀문서와 미래 프로세서 칩 도면 19개 소유
- 양사에서 동시에 근무하는 것을 수상하게 여긴 인텔 직원의 신고로 드러남



### 4. 무선 및 광대역 인터넷 기술 유출 시도 (2007)

- 미국으로 와이브로 기술을 유출하려 한 혐의로 한국 검찰에 의해 기소  
(WiBro는 무선 광대역 기술로 빠른 데이터 전송이 가능하며 2006년에 이미 상용화)
- 철강회사 포스코의 정보기술업체인 포스데이터의 전직 직원, 현직 연구원
- 포스데이터가 900억원을 들여 개발한 기술을 미국에 1억 8천만원에 인수할 계획

### 5. FBI 직원 지인들에게 기밀 유출 사고 (1997)

- 퍼지(Jeffrey.D.Fudge): 1988년부터 FBI에서 조사 분석을 맡은 직원
- 영장 발부, 전화기록 분석, FBI 기밀 데이터베이스 검색 수행 등 범죄 수사 협업 담당
- 1997년 10월 7일~2003년 4월 25일  
공식적인 업무 외 사건에 대해 무단 검색  
지인들의 부탁으로 수사 중인 사건에 대해 알려주기 위해 비공식적인 검색
- 10개 혐의로 기소되어 유죄판결, FBI로부터 해고



## ○ 범위(Scope)

- 전직 직원 (former employees)
- 현직 직원 (current employees): IT/주요정보 담당자, Spy 직원
  
- 제휴업체 (associates)
- 계약자 (contractors)
- 협력업체 (business partners): 공급자 (suppliers), Helpdesk 직원
  
- 일반 방문자 (guests)
- 컴퓨터 유지보수업자 (IT maintenance technicians)



## ○ 내부자 위협 (공격)

- 조직 내 컴퓨터 시스템이나 네트워크에 접근할 수 있도록 인가를 받은 직원이 조직의 보안 정책을 의도적으로 위반하고 오용하는 행위

## ○ Motives (동기)

- 개인적인 욕심(individual greed)
- 금전(financial benefit)
- 복수심(revenge)
- 일반적인 악의 (general malice)
- 정치적인 이해, 권력 (political benefit)

※ 범죄의 3요소: 기회, 동기, 계기



## ○ Fields (분야)

- (1) 금융 부문 - 은행, 증권, 보험 등
- (2) 공공 부문 - 공익사업 (에너지[수도/전기/가스], 통신, 교통) 등
- (3) 국방 부문 - 군사기밀, 정보전 등
- (4) 산업 부문 - 핵심기술, 영업 비밀, 기업 기밀자료, 지적 재산권 등

## ○ Digital Forensic on insiders so far?

- Don't care or Do nothing
- Digital Forensic have focused on methodologies, technologies and techniques
- Post-investigation
  - Pre-detection capturing precursors





- 공통적인 특성과 성향 (Predisposition)
- 행동관점(Behavioral Perspective):  
의심스러운 행위, 주변환경 [비가시적 → 가시적]
- 기술관점(Technical Perspective):  
정보 유출/조작 경로
  
- Putting them all together → MODEL



## ○ 공통적인 특성과 성향

부문별 공통특성	정보통신기술		은행 및 금융		주요기반시설		정부기관		전체	
조사사건수	52		23		49		36		160	
답변	Y	N	Y	N	Y	N	Y	N	Y	N
[근무이력] 전·현직 직원인가?	94%	6%	100%	0%	100%	0%	90%	10%	96%	4%
[범죄경력] 기소된 적이 있는가?	38%	62%	27%	73%	30%	70%	31%	69%	32%	68%
[결혼유무] 기혼인가?	43%	57%	31%	69%	49%	51%	48%	52%	43%	57%
[성별] 남성인가?	91%	9%	58%	42%	96%	4%	50%	50%	74%	26%
[직군특성] 정보기술직군에 종사하는가?	63%	37%	23%	77%	86%	14%	26%	74%	50%	50%

(출처) Insider Threat Study, CERT® Program Software Engineering Institute, Carnegie Mellon University and National Threat Assessment Center, United States Secret Service, 2004-2008 연구자료 기반임



## ○ 행동관점(Behavioral Perspective)

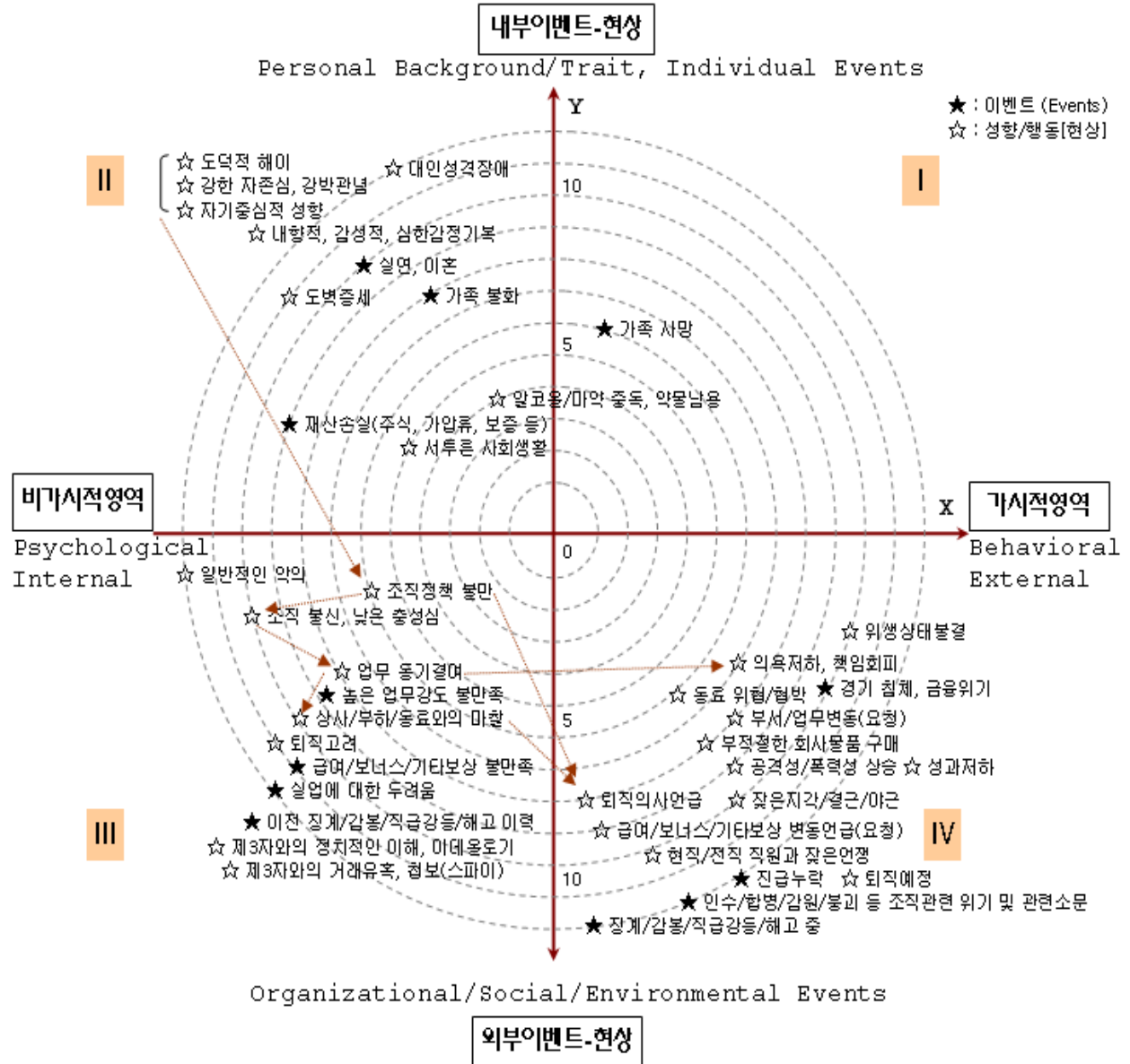
- (1) 비가시 영역 → 가시 영역(징후)
- (2) 내부요소: 심리적 요인
- (3) 외부요소: 사회적/조직적 요인
- (4) 개인성향/특성
- (5) 스트레스성 이벤트

(내부요소)	개인성향 및 특성	내적 스트레스성 이벤트
개인적 심리적 요인	<input type="checkbox"/> 자기중심적 성향 <input type="checkbox"/> 강한 <u>자만적</u> 성향 <input type="checkbox"/> 내적인 성향 <input type="checkbox"/> 감정적으로 불안한 성향 <input type="checkbox"/> 성격 장애 <input type="checkbox"/> <u>도벽증</u> <input type="checkbox"/> 고집이 센 성향 <input type="checkbox"/> 알코올/마약 중독	<input type="checkbox"/> 가족과의 불화 <input type="checkbox"/> 애인, 지인과의 관계악화 <input type="checkbox"/> 부부생활 불화 <input type="checkbox"/> 이혼, 별거 <input type="checkbox"/> 가족/친척/친구의 사망 <input type="checkbox"/> 심각한 자산 손해 <input type="checkbox"/> 갑작스런 질병이나 상해 <input type="checkbox"/> 만성질병/고질병
↑		
비가시 영역	<input type="checkbox"/> 조직 정책에 대한 불만 <input type="checkbox"/> 퇴직/장기휴직 고려 <input type="checkbox"/> 불신감과 증오심 <input type="checkbox"/> 낮은 충성도와 동기부여 <input type="checkbox"/> 경기침체 및 재정위기 <input type="checkbox"/> 인수합병과 구조조정(소문) (M&A, Downsizing) <input type="checkbox"/> 내부철폐활동 (정치적, 금전적 목적)	<input type="checkbox"/> 해고에 대한 불안감 <input type="checkbox"/> 급여 및 보너스 불만족 <input type="checkbox"/> 강등(demotion) 이력 <input type="checkbox"/> 감봉(pay cut) 이력 <input type="checkbox"/> 견책(reprimand) 이력 <input type="checkbox"/> 해고(fired) 이력 <input type="checkbox"/> 강제휴업(layoff) 이력 <input type="checkbox"/> 승진(promotion) 누락이력 <input type="checkbox"/> 상사 및 동료와의 갈등
↓		
사회적 조직적 요인 (외부요소)	환경적 요인	외적 스트레스성 이벤트
가시적 영역 (징후)	<input type="checkbox"/> 비위생적 상태 <input type="checkbox"/> 언행에 대한 책임감 회피 <input type="checkbox"/> 상사 및 동료와의 잦은 언쟁, 위협 <input type="checkbox"/> 부서 이동 요구/요청 <input type="checkbox"/> 사내에서 부적절한公款 사용 (물품 매입 등) <input type="checkbox"/> 공격적이거나 폭력적인 태도 <input type="checkbox"/> 낮은 성과 <input type="checkbox"/> 잦은 지각, 무단결근, 휴가 <input type="checkbox"/> 퇴직 의사 표명 <input type="checkbox"/> 급여와 보너스에 대한 논쟁/불만 표명 <input type="checkbox"/> 퇴직 절차를 밟고 있는 구성원 <input type="checkbox"/> 징계 중인 구성원 (강등, 감봉, 견책, 강제휴업 등)	



## ○ 행동관점

- Events
- Behaviors





## ○ 기술관점(Technical Perspective): 내부정보 유출과 조작 경로

- (1) 내부자가 합법적인 접근권한을 가진 인가된 시스템 및 어플리케이션 핵심정보나 기술이 담긴 정보의 과도한 다운로드와 위변조 및 외부유출시도, 과도한 로컬 계정 로그인 시도...
- (2) 내부자가 활용할 수 있는 오프라인에서 인가된 기술적 / 비기술적 행위 IEEE1394, CD/DVD, 플로피 디스크, USB 등 백업용 또는 휴대용 대용량 저장장치를 이용한 데이터 전송...
- (3) 내부자가 접근권한을 가진 인가된 네트워크 공유디렉터리, 메신저, FTP, P2P, 웹하드, 이메일 첨부, 인터넷상 외부 게시판 등 네트워크를 통한 주요 데이터의 전송, 외부 프락시를 통한 접속...
- (4) 의심하지 않을 법한 인가된 행동이나 방식 어깨 너머 훑쳐보기, 쓰레기통 뒤지기, 패스워드 물어보기와 같은 사회공학, 불법 소프트웨어 설치, 비업무 웹사이트의 잦은 접속, 업무용 노트북 반출입...
- (5) 내부자에게 허용되지 않은 비인가 시스템, 네트워크 접근이나 기술적 / 비기술적 행위



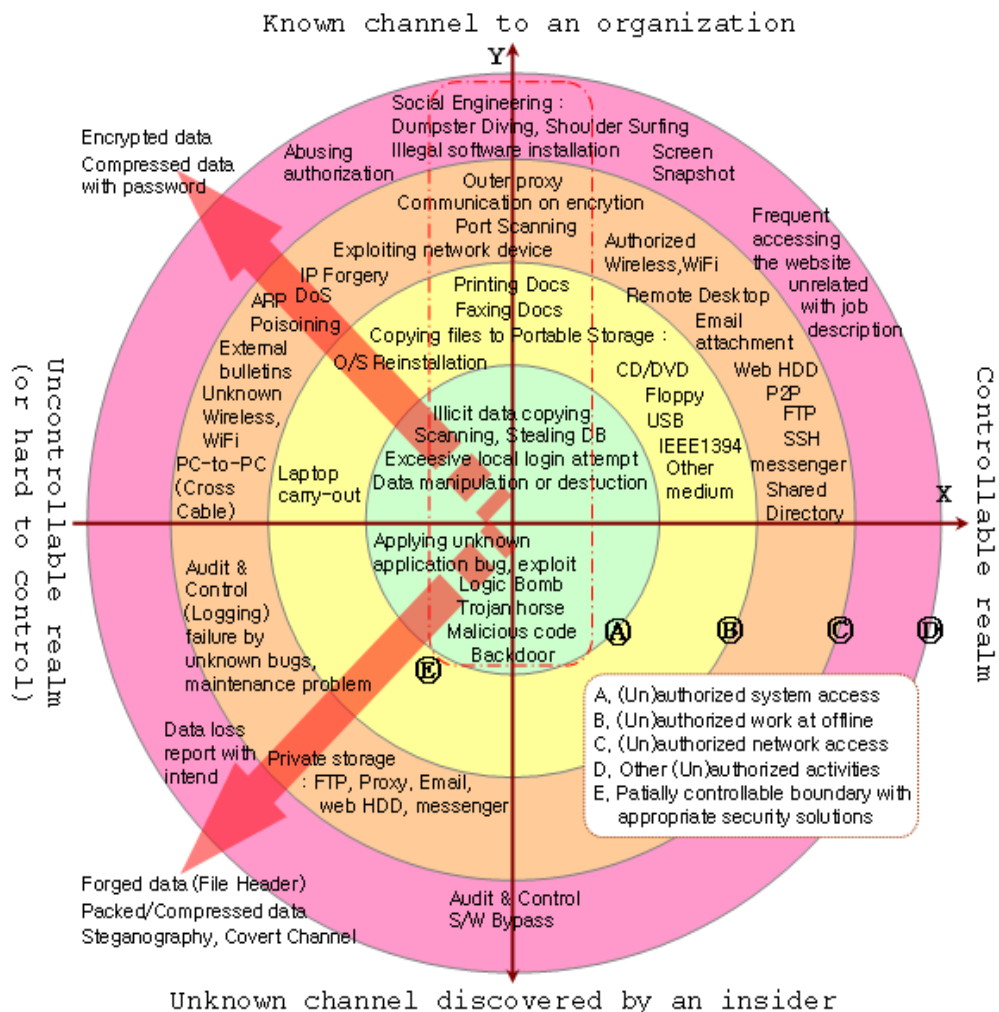
## 기술관점: 내부정보 유출과 조작 경로

(1) Channel

(Known) VS  
(Unknown)

(2) Realm

(Controllable) VS  
(Uncontrollable)





- 가정사항(Assumption)

- (1) 행동특성은 치우치지 않은 공정한 판단을 기반으로 한다.
- (2) 기술적인 경로로부터 탐지된 데이터는 무결성을 보장한다.
- (3) 자체적으로 수립하여 적용한 보안 정책을 가지고 있다.
- (4) 주요내부자산을 정의하고 접근통제를 실시하고 있다.



## ○ 용어정의(Terms)

(1) 사전확률(PP, Prior Probability): 기존 사고사례에서 Profiling 기반 확률

(2) 징후요인(PF, Precursor Factor): 위협 징후를 결정하는 요소

- P (P, Predisposition) 개별성향 및 특성요인

- B (B, Behavioral Factors): 가시적인 비정상 행동요인

- T (T, Technical Factors): 내부정보 유출 및 조작경로

(3) 기존관측치/현재관측치

- 관측값(O, Observation):

현재관측치가 YES일 때에는 1, 그 외에는 0

-  $O_p/O_c$ : Prior/Current Observation

- Domain: {YES, NO, DON'T KNOW}

(4) 가중치(Weight)

- 기본 가중치( $W_b$ , Basic Weight):

사전확률에 기반하여 1.2~3.0까지 할당

- 변화 가중치( $W_c$ , Change Weight):

행동에 변화가 있을 때 위협지수를 2배 증가

사전확률(PP)	가중치(Weight)
0% ~ 50%	1.0
50% ~ 55%	1.2
55% ~ 60%	1.4
60% ~ 65%	1.6
65% ~ 70%	1.8
70% ~ 75%	2.0
75% ~ 80%	2.2
80% ~ 85%	2.4
85% ~ 90%	2.6
90% ~ 95%	2.8
95% ~ 100%	3.0





## ○ 용어정의(Terms)

(5) 내부자 위협증거 벡터 (ITE vector):  $E(P,B,T)$

(6) 내부자 위협증거 지수 (ITE index):  $E_{insider} = |E(P,B,T)|$

$$P = \sum_{l=1}^i W_{bl} \times p_l, \quad B = \sum_{l=1}^j W_{bl} \times W_{cl} \times b_l, \quad T = \sum_{l=1}^k W_{bl} \times W_{cl} \times t_l \quad 5)$$

where  $P = \{ P_1, \dots, P_i \}$ ,  $B = \{ B_1, \dots, B_j \}$ ,  $T = \{ T_1, \dots, T_k \}$

$$E_{insider} = |E| = \sqrt{P^2 + B^2 + T^2}$$

[정규화]

$$P_z = \frac{P_i - \mu_p}{\sigma_p / \sqrt{n}}, \quad B_z = \frac{B_j - \mu_b}{\sigma_b / \sqrt{n}}, \quad T_z = \frac{T_k - \mu_t}{\sigma_t / \sqrt{n}} \quad \text{where}$$

$$\mu_p = \frac{1}{n} \sum_l^i P_l, \quad \mu_b = \frac{1}{n} \sum_l^j B_l, \quad \mu_t = \frac{1}{n} \sum_l^k T_l$$

$$\sigma_p = \sqrt{\frac{1}{n} \sum_l^i (P_l - \mu_p)^2}, \quad \sigma_b = \sqrt{\frac{1}{n} \sum_l^j (B_l - \mu_b)^2}, \quad \sigma_t = \sqrt{\frac{1}{n} \sum_l^k (T_l - \mu_t)^2}$$

$$E_z = E(P_z, B_z, T_z) = \sqrt{P_z^2 + B_z^2 + T_z^2}$$



## ○ 잠재적인 내부자 위협 징후요인(PFs)

개별성향 및 특성요인 (P <sub>i</sub> )	p <sub>1</sub>	전·현직 직원이다.	내부정보 유출 및 조작경로 (T <sub>k</sub> )	t <sub>1</sub>	대용량 메일을 이용하여 자주 내부 자료를 전송한다.
	p <sub>2</sub>	미혼이다.		t <sub>2</sub>	<b>업무용 장비에 조직 내에서 필수적으로 적용하는 보안 소프트웨어를 미사용 중이다.</b>
	p <sub>3</sub>	기존에 범죄를 저지른 혐의가 있다.		t <sub>3</sub>	대량의 데이터를 휴대용 저장장치로 전송한다.
가시적인 비정상 행동요인 (B <sub>j</sub> )	p <sub>4</sub>	기술적인 업무를 한다.		t <sub>4</sub>	<b>채용 사이트에 자주 접속하고 재직증명서를 발급한다.</b>
	b <sub>1</sub>	평소 불평을 자주 하는 편이다.		t <sub>5</sub>	<b>권한이 없는 내부 시스템에 접근을 시도한다.</b>
	b <sub>2</sub>	연봉과 보너스에 불만스러운 편이다.		t <sub>6</sub>	<b>비정상적인 데이터베이스 쿼리를 사용한다.</b>
	b <sub>3</sub>	퇴직의사를 밝힌 적이 있다.		t <sub>7</sub>	특정 네트워크 또는 시스템을 스캔한다.
	b <sub>4</sub>	감봉, 강등, 견책 등 징계경력이 있다.		t <sub>8</sub>	퇴직 후 VPN에 접속하고 사내시스템에 접근한다.
	b <sub>5</sub>	언행에 대해 책임을 지지 않는 편이다.		t <sub>9</sub>	업무에 무관한 문서 출력이나 팩스 전송을 자주 한다.
	b <sub>6</sub>	직무 수행에 대한 성과가 매우 낮다.			
	b <sub>7</sub>	출퇴근 시간이 너무 이르거나 늦다.			
b <sub>8</sub>	상사나 동료와 잦은 분쟁이 있다.				



## ○ 내부자 위협 증거 지표( $E_{insider}$ ) 계산표

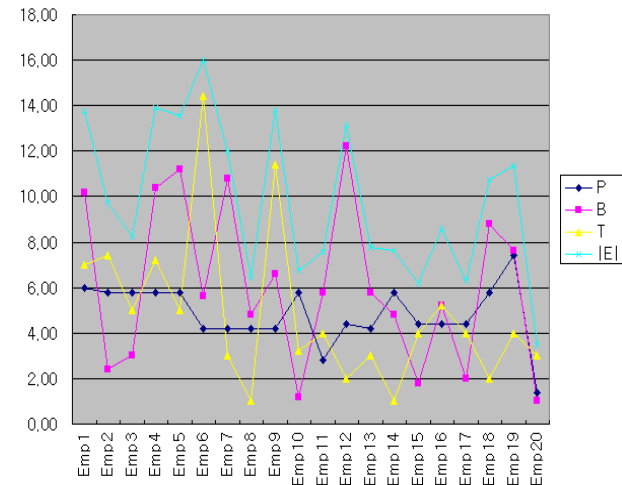
$$P = \sum p_i = 6.0 \quad B = \sum b_i = 10.2 \quad T = \sum t_i = 7.0 \quad \rightarrow \quad |E(P,B,T)| = \sqrt{P^2 + B^2 + T^2} = 3.75$$

징후 요인	내부자 이상 징후를 탐지하기 위한 요인	사전 확률 (PP)	관측치 (Observation)			가중치 (Weight)		PF Value
			Op	Oc	O	Wb	Wc	
p <sub>1</sub>	전·현직 직원이다.	0.94	-	YES	1	2.8	1	2.8
p <sub>2</sub>	미혼이다.	0.57	-	YES	1	1.4	1	1.4
p <sub>3</sub>	기존에 범죄를 저지른 혐의가 있다.	0.62	-	NO	0	1.6	1	0.0
p <sub>4</sub>	기술적인 업무를 한다.	0.63	-	NO	0	1.6	1	0.0
b <sub>1</sub>	평소 불평을 자주 하는 편이다.	0.91	YES	DON'T KNOW	0	2.8	1	0.0
b <sub>2</sub>	연봉과 보너스에 불만스러운 편이다.	0.66	NO	DON'T KNOW	0	1.8	1	0.0
b <sub>3</sub>	퇴직의사를 밝힌 적이 있다.	0.74	YES	YES	1	2	1	2.0
b <sub>4</sub>	감봉, 강등, 견책 등 징계경력이 있다.	0.85	YES	DON'T KNOW	0	2.4	1	0.0
...	...	...	...	...	...	...	...	...
b <sub>8</sub>	상사나 동료와 잦은 분쟁이 있다.	0.50	DON'T KNOW	DON'T KNOW	0	1	1	0.0
t <sub>1</sub>	대용량 메일로 내부 자료를 전송한다.	0.50	NO	YES	1	1	2	2.0
...	...	...	...	...	...	...	...	...
t <sub>3</sub>	휴대용 저장장치로 대량 전송한다.	0.50	YES	YES	1	1	1	1.0
t <sub>4</sub>	채용 사이트에 접속후 재직증명서를 발급한다.	0.50	NO	NO	0	1	1	0.0
...	...	...	...	...	...	...	...	...
t <sub>7</sub>	특정 네트워크/시스템을 스캔한다.	0.50	NO	NO	0	1	1	0.0
t <sub>8</sub>	퇴직 후 VPN에 접속을 시도한다.	0.50	NO	YES	1	1	2	2.0



## ○ 구성원이 20명인 조직에서 E(P,B,T) Simulation 결과치

구성원	P	B	T	E	구성원	P	B	T	E
내부자1	6.00	10.20	7.00	13.75	내부자11	2.80	5.80	4.00	7.58
내부자2	5.80	2.40	7.40	9.70	내부자12	4.40	12.20	2.00	13.12
내부자3	5.80	3.00	5.00	8.22	내부자13	4.20	5.80	3.00	7.76
내부자4	5.80	10.40	7.20	13.92	내부자14	5.80	4.80	1.00	7.59
내부자5	5.80	11.20	5.00	13.57	내부자15	4.40	1.80	4.00	6.21
<b>내부자6</b>	<b>4.20</b>	<b>5.60</b>	<b>14.40</b>	<b>16.01</b>	내부자16	4.40	5.20	5.20	8.57
내부자7	4.20	10.80	3.00	11.97	내부자17	4.40	2.00	4.00	6.27
내부자8	4.20	4.80	1.00	6.46	내부자18	5.80	8.80	2.00	10.73
내부자9	4.20	6.60	11.40	13.83	내부자19	7.40	7.60	4.00	11.34
내부자10	5.80	1.20	3.20	6.73	내부자20	1.40	1.00	3.00	3.46
Avg.	4.84	6.06	4.84	9.84					
Max	7.40	12.20	14.40	16.01					

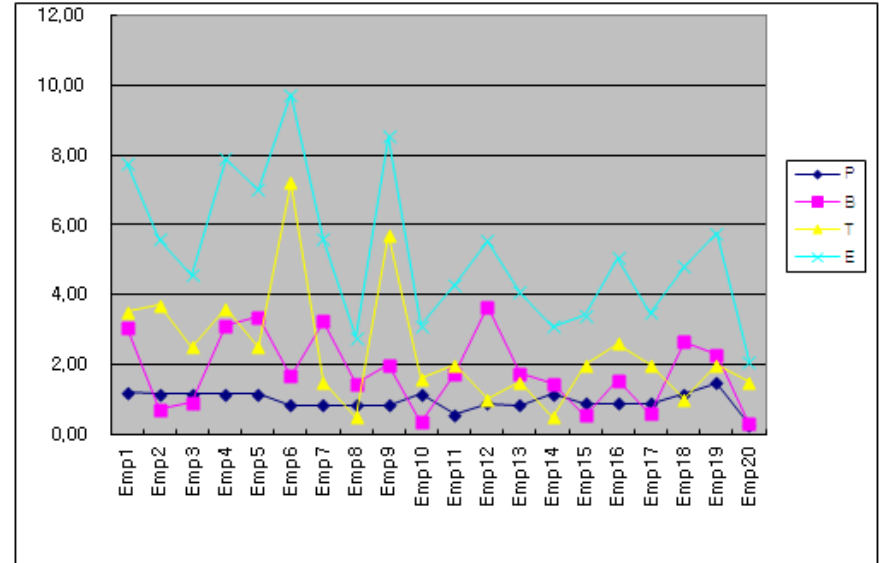




## 정규화 전후

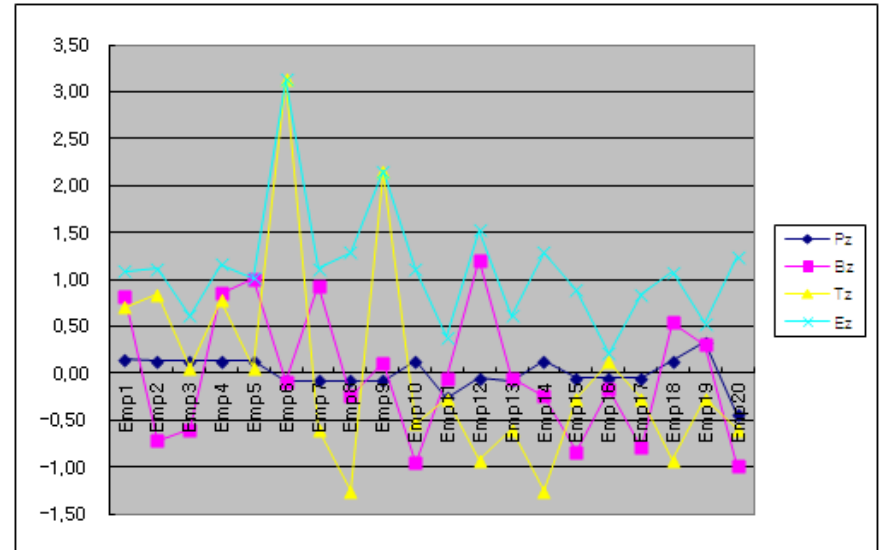
1. 정규화하기 전 값

Original	P	B	T	E
Emp1	1.20	3.06	3.50	7.76
Emp2	1.16	0.72	3.70	5.58
Emp3	1.16	0.90	2.50	4.56
Emp4	1.16	3.12	3.60	7.88
Emp5	1.16	3.36	2.50	7.02
Emp6	0.84	1.68	7.20	9.72
Emp7	0.84	3.24	1.50	5.58
Emp8	0.84	1.44	0.50	2.78
Emp9	0.84	1.98	5.70	8.52
Emp10	1.16	0.36	1.60	3.12
Emp11	0.56	1.74	2.00	4.30
Emp12	0.88	3.66	1.00	5.54
Emp13	0.84	1.74	1.50	4.08
Emp14	1.16	1.44	0.50	3.10
Emp15	0.88	0.54	2.00	3.42
Emp16	0.88	1.56	2.60	5.04
Emp17	0.88	0.60	2.00	3.48
Emp18	1.16	2.64	1.00	4.80
Emp19	1.48	2.28	2.00	5.76
Emp20	0.28	0.30	1.50	2.08
Avg.	0.97	1.82	2.42	5.21
Max	1.48	3.66	7.20	9.72



2. 정규화한 후 값

Scaled	Pz	Bz	Tz	Ez
Emp1	0.15	0.81	0.71	1.09
Emp2	0.13	-0.72	0.84	1.11
Emp3	0.13	-0.60	0.05	0.62
Emp4	0.13	0.85	0.77	1.16
Emp5	0.13	1.01	0.05	1.02
Emp6	-0.08	-0.09	3.13	3.13
Emp7	-0.08	0.93	-0.60	1.11
Emp8	-0.08	-0.25	-1.26	1.28
Emp9	-0.08	0.11	2.15	2.15
Emp10	0.13	-0.95	-0.54	1.10
Emp11	-0.27	-0.05	-0.28	0.39
Emp12	-0.06	1.20	-0.93	1.52
Emp13	-0.08	-0.05	-0.60	0.61
Emp14	0.13	-0.25	-1.26	1.29
Emp15	-0.06	-0.84	-0.28	0.88
Emp16	-0.06	-0.17	0.12	0.21
Emp17	-0.06	-0.80	-0.28	0.84
Emp18	0.13	0.54	-0.93	1.08
Emp19	0.33	0.30	-0.28	0.53
Emp20	-0.45	-0.99	-0.60	1.25
Avg.	0.00	0.00	0.00	1.12
Max	0.33	1.20	3.13	3.13

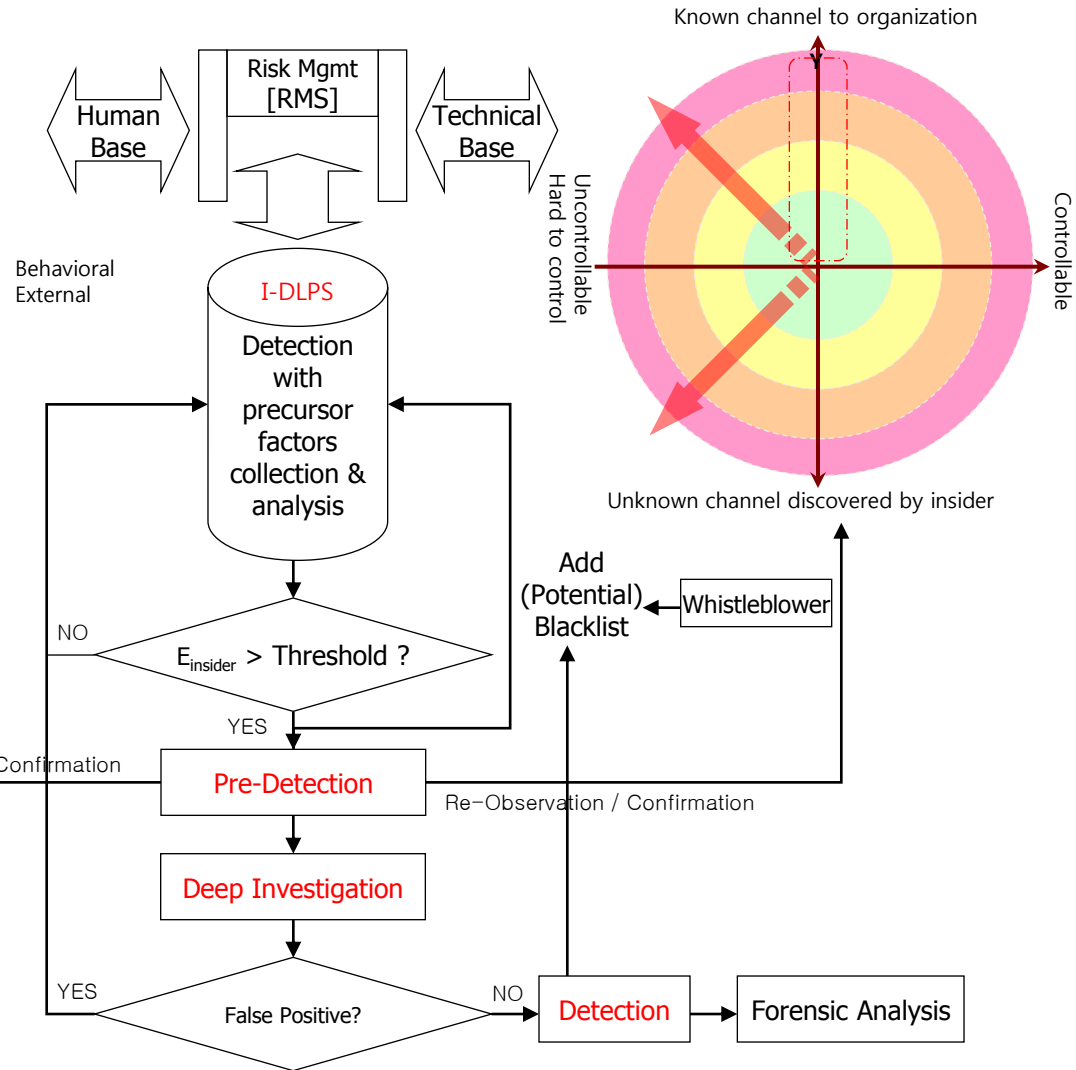


# Pre-Detection Model (8)



Detection Preparation → Identification(Pre-Detection) → Detection → Forensic Request

Individual	<b>Predisposition (Personal Backgrounds)</b>	<b>Stressful Events</b>
	<ul style="list-style-type: none"> <li>☆ Self-Oriented, Stubborn</li> <li>☆ Intensive self-esteem</li> <li>☆ Introspective nature</li> <li>☆ Emotionally unstable</li> <li>☆ Personality conflicts</li> <li>☆ Seizure disorder</li> <li>☆ Panic attack</li> <li>☆ Alcohol/drug addiction</li> </ul>	<ul style="list-style-type: none"> <li>★ Trouble in family</li> <li>★ Trouble in relationship with personal acquaintances</li> <li>★ Divorce, Separation</li> <li>★ Death in the family, friends</li> <li>★ Severe property damage</li> <li>★ Unexpected illness</li> <li>★ Chronic disease</li> </ul>
Social		
	<ul style="list-style-type: none"> <li>☆ Disgruntlement on organizational policy, mgmts</li> <li>☆ Consideration of retirement, long leave</li> <li>☆ Distrust or Hatred</li> <li>☆ Low loyalty, motivation</li> <li>☆ Recession, Financial crisis</li> <li>☆ M&amp;A, downsizing rumors</li> <li>☆ Plan for espionage : theft or modification for financial gain and/or business advantage</li> </ul>	<ul style="list-style-type: none"> <li>★ Fear on losing job</li> <li>★ Inefficient salary</li> <li>★ Inefficient bonus</li> <li>★ Sanction</li> <li>★ Reprimand</li> <li>★ Demotion</li> <li>★ Fired</li> <li>★ Layoff</li> <li>★ Promotion Failure</li> <li>★ Trouble in relationship with supervisor and/or boss</li> </ul>
Visible Realm	<b>Organizational or Environmental Factors</b>	<b>Stressful Events</b>
	<ul style="list-style-type: none"> <li>▷ Poor hygiene</li> <li>▷ Responsibility avoidance in speech and behavior</li> <li>▷ Bullying or intimidation of coworkers</li> <li>▷ Request for alternate work</li> <li>▷ Inappropriate purchases on company</li> <li>▷ Aggressive and/or violent attitude</li> <li>▷ Poor job performance</li> <li>▷ Frequent tardiness, truancy, absence</li> <li>▷ Request for retirement</li> <li>▷ Complaints, disagreements on salary, bonus</li> <li>▷ Frequent disputes, argument with co-workers, boss</li> <li>▷ Retirement scheduled</li> </ul>	





- 인간의 행동을 객관적으로 정확하게 측정할 수 있는 도구
- 정보 유출 및 조작 발견과정
- Monitoring 인력이 조직외부와 연결고리가 있을 경우
- 은폐기법: Packing, Compression, Encryption, Steganography,  
Unknown other covert channels



# QUESTIONS?