Looking into Malicious Insiders

JPCERT/CC
Koichiro Sparky Komiyama

First Conference, Vienna

Agenda

- Background
  - Previous work
  - Information leakage by malicious insider
- Our Research
- How to prevent

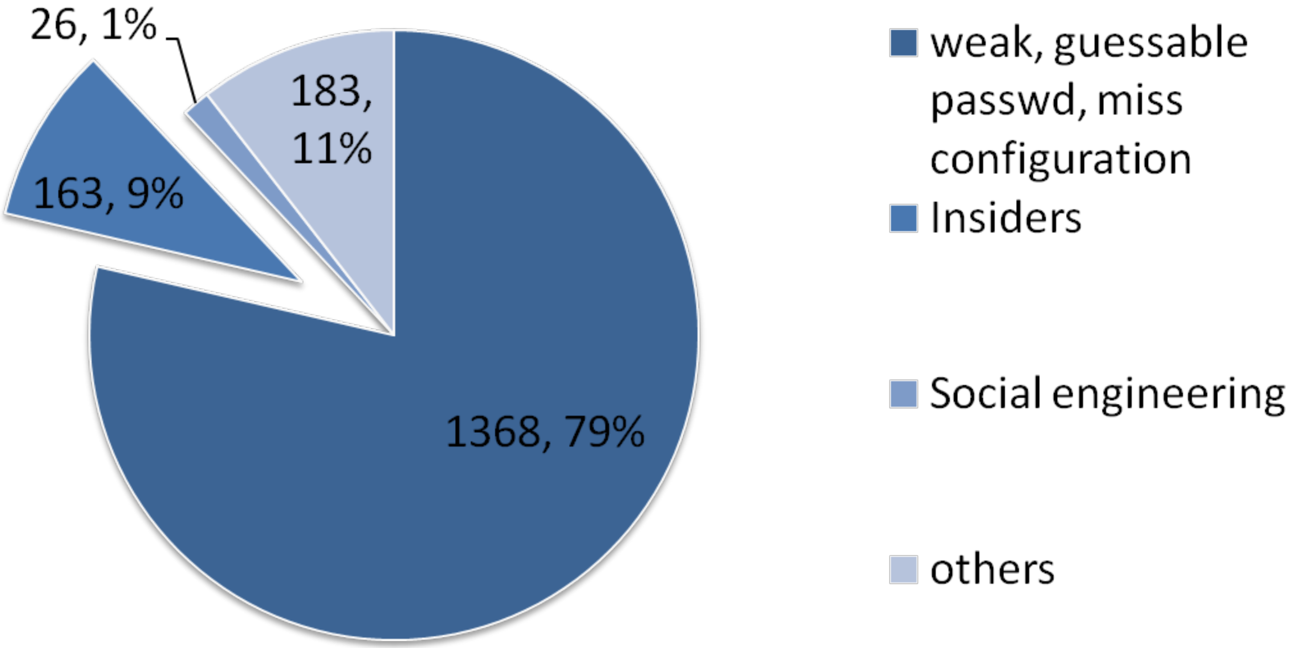
Insider Threat

- Definition by CERT/CC insider threat study
  - A current or former employee, contractor , or business partner who
    - Has or had authorized access to an organization’s network, system, or data and
    - Intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems

WHY INSIDER THREAT?

More insiders are arrested

- How unauthorized access happens? How do attackers obtain credentials? (N=1740)

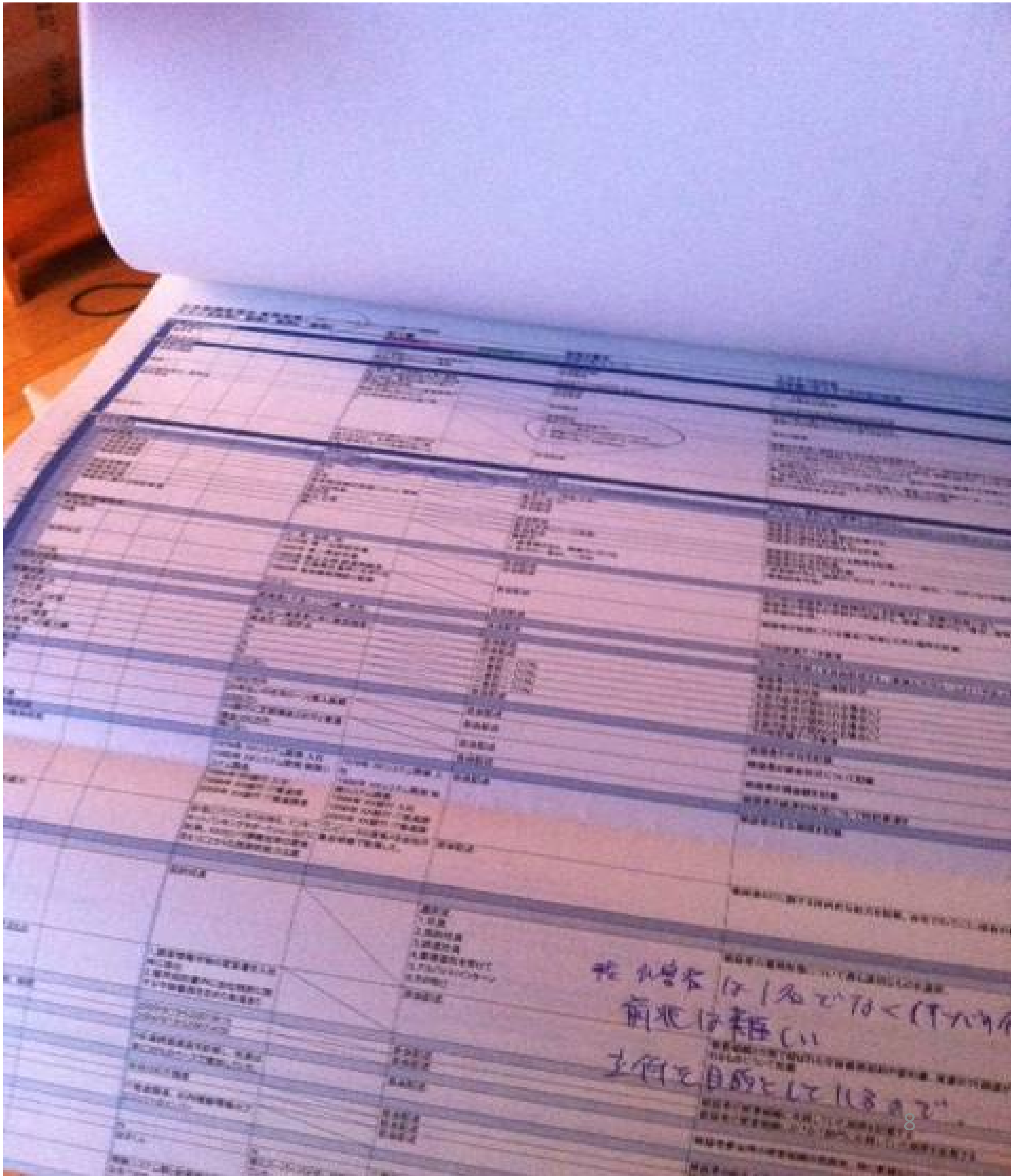


NPA, FY2008, Act on the Prohibition of Unauthorized Computer Access

OUR RESEARCH

- Motivation
- Project members
  - National Police Agency (NPA, prefectural police department)
  - Department of Criminology and Behavioral Science, National Research Institute of Police Science
  - JPCERT/CC
- Survey 30 cases/criminals who
  1. Fit the malicious Insider definition by CERT/CC
  2. Were arrested and prosecuted for Cybercrime related law from 2007 to Jun, 2009

1, visit local police office
2, fill in survey form with reffering police investigative report
3, Sanitize to secure anonymity
4, Correlation analysis by 24 variables

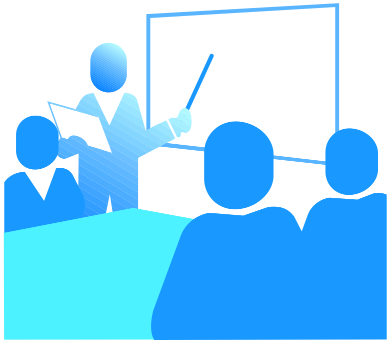


※ 加害者は1名でなく(すべり[illegible]
前兆は難しい
上司を目的としている[illegible]まで

24 variables: Case

- The case is
  - □By a repeat offender
  - □caused financial damage
  - □computer which company provided was used
  - □access from outside
  - □Delete/modify logs of activity
  - □use his/her own account to login

24 variables: Surrounding



- Company/Organization
  - □ Has insecure account management (like easily guessable user name)
  - □ Does not have any physical monitoring (video monitor, guards)

24 variables: Criminals

- Criminal is
  - □Is a lone criminal
  - □Has no job at the time
  - □Is in dire financial circumstances
  - □Is under strong pressure

24 variables: Relationship

- Criminal is
  - □ a former employee of the company/organization
  - □Has been terminated in the past
  - □caused any trouble in the past
  - □Is in charge of system management
  - □Is a web admin
  - □Is in charge of accounting or finance

24 variables: Motives

- Criminals motivation is
  - □To make money
  - □To get information , then to make money by selling those
  - □Sabotage
  - □Personal satisfaction

Correlation Map

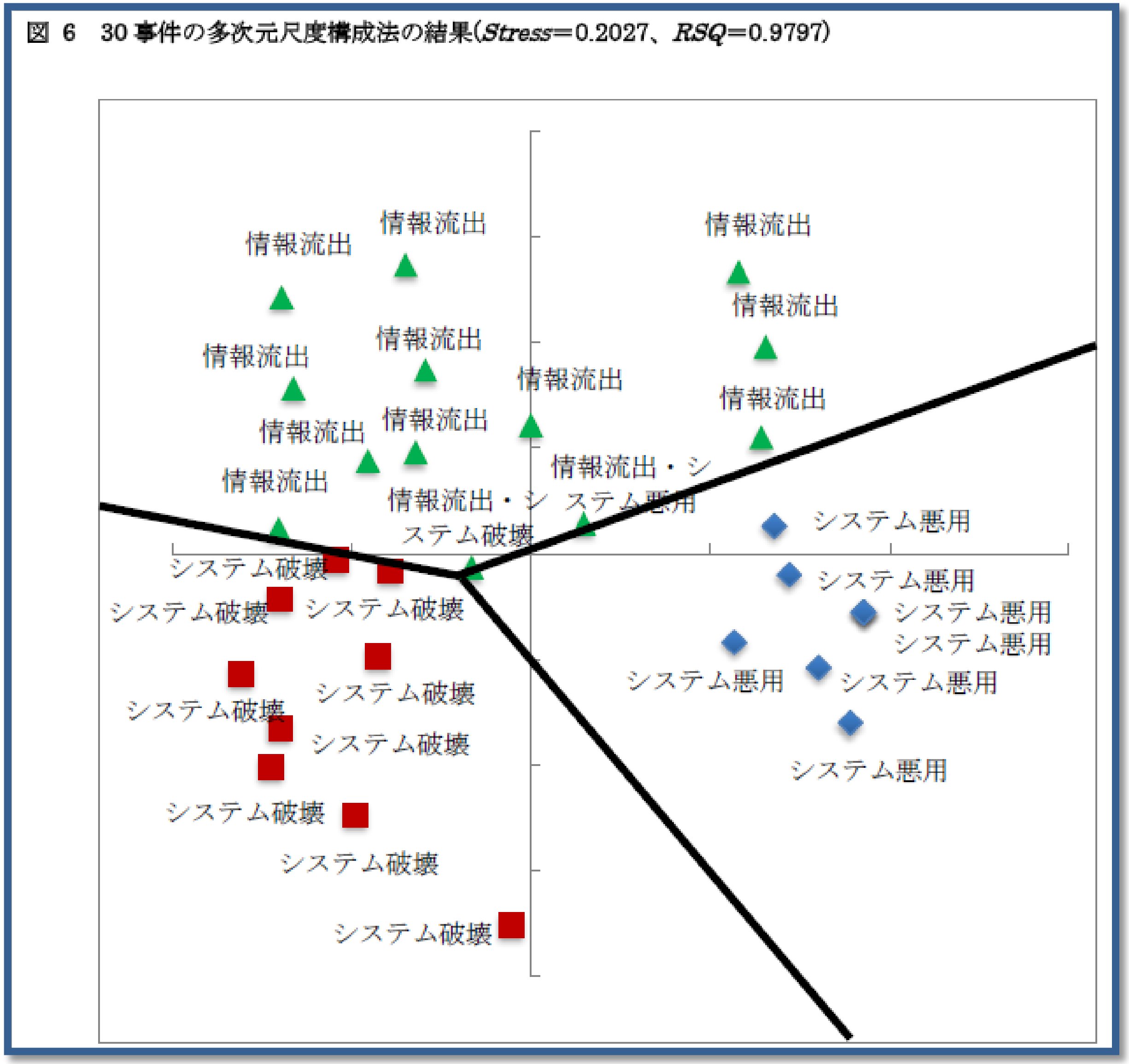
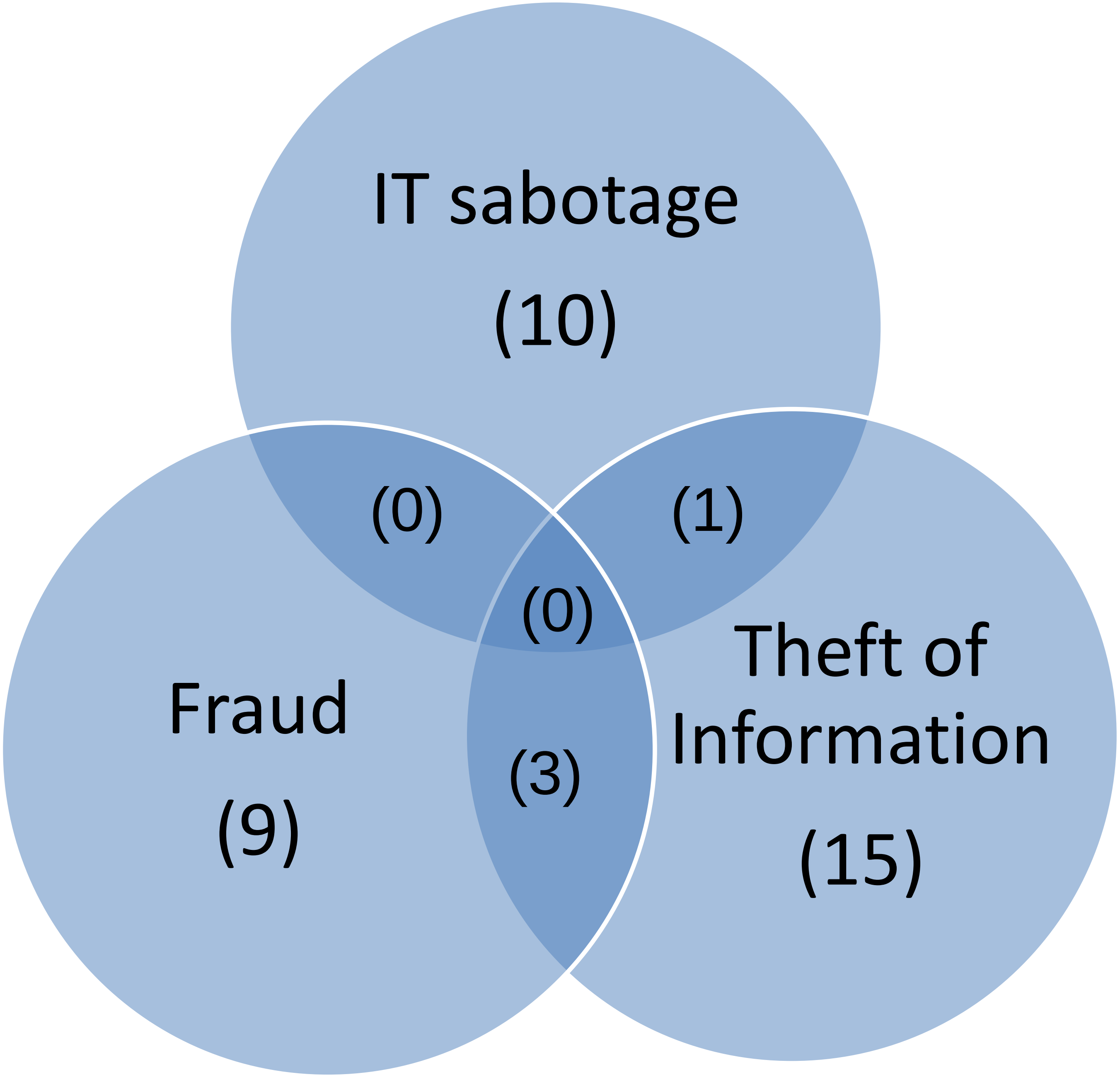


図 6　30 事件の多次元尺度構成法の結果(*Stress*=0.2027、*RSQ*=0.9797)

FINDINGS


IT sabotage
(10)
(0)
(1)
(0)
Fraud
(9)
(3)
Theft of Information
(15)

HAVE A LOOK AT 30 INSIDERS

WHO? (Gender, work history)

Type	Fraud(9)	IT Sabotage(10)	Information Theft - Money(7)	Information Theft - Satisfaction (8)
Gender	Male(6) **Female(3)**	Male(9) Female(1)	Male(7)	Male(8)
work history	・hopping part time job ・job change 5times ・job change 3times(2） ・job change 1 time(fired by ex-company） ・job change１times（own his start-up and shut it down） ・no job(3)	**・job change 7 times** ・job change 4 times ・job change 3 times(3) ・job change 2 times(3) ・no job ・unknown	・job change 3times(3) ・job change 2times ・job change 1times(2) ・no job	・job change 4 times ・job change 3times(2) ・job change 2times ・job change 1time(3) ・no job

- Frequent job change can be seen all categories

WHO? (Personality)

Fraud(9)	IT Sabotage(10)	Information Theft - Money(7)	Information Theft - Satisfaction (8)
▪Humble, sociable ▪wear torn jeans, not like a business man ▪patient and quiet. ▪always exhibitionistic. ▪unknown	▪clumsy at office, can not communicate with others **▪very active for any business and solid person** ▪quiet ▪not very good at communication ▪habitually lying	▪good guy, a bit of a scatterbrain **▪polite, perfect young gentleman** ▪stiff and proper, can't refuse when someone asks ▪act in a childish manner ▪unknown	▪easily offended, hold by his own idea ▪Sociable, sometimes acts paranoid for minor problem ▪very childish **▪popular among project team members**

- Less conversation, less communication

WHO? (Criminal record, Education)

Type	Fraud(9)	IT Sabotage(10)	Information Theft - Money(7)	Information Theft - Satisfaction (8)
Criminal record	**▪No(5)** ▪professional embezzlement and stealing ▪stealing ▪assault ▪trademark law violation	**▪No(6)** ▪twice for theft of lost or mislaid property ▪once for theft of lost or mislaid property ▪shoplifting, stealing	**▪No(6)** ▪assault	**▪No(6)** ▪twice for theft of lost or mislaid property ▪assault
False entry in resume	▪False entry (2)	▪False entry (3)		▪False entry (1)

•Over 80 percent are first-time criminals

･some lie on a resume, especially their educational background

When? and Where?

- When
  - Fraud: during business hours
  - IT sabotage: one to six month after resignation/termination, most of those failed to get a new job. Night Time
  - Insiders start with trivial activities, then escalate
- Where
  - Fraud, Information Theft: in office
  - IT sabotage: from home

WHY? (direct motivation)

Fraud(9)	IT Sabotage(10)	Information Theft - Money(7)	Information Theft - Satisfaction (8)
・get money to pay off debts (3) ・frustration at long hours, aim to get back at management ・feel less secure since spouse doesn’t work ・get money to pay off debts ・feels it’s such a waste letting points to expire	・betrayed the expectations of being a full time worker ・want to harass(5) ・get fired despite of his outstanding performance **・company contact him as a last resort.**	・can not find new job and want to make money, even if only a little ・want to make money by selling personal information (2) ・ get info in order to please his boss	・sudden random thought while drinking **・want to understand the situation he used to work in** ・he has pending lawsuit with the company. And he checks if there are any other trouble

- Money , ★恨み, 人間関係、ストレス
- More likely to occur when they failed to get new job.

How they get into the system?

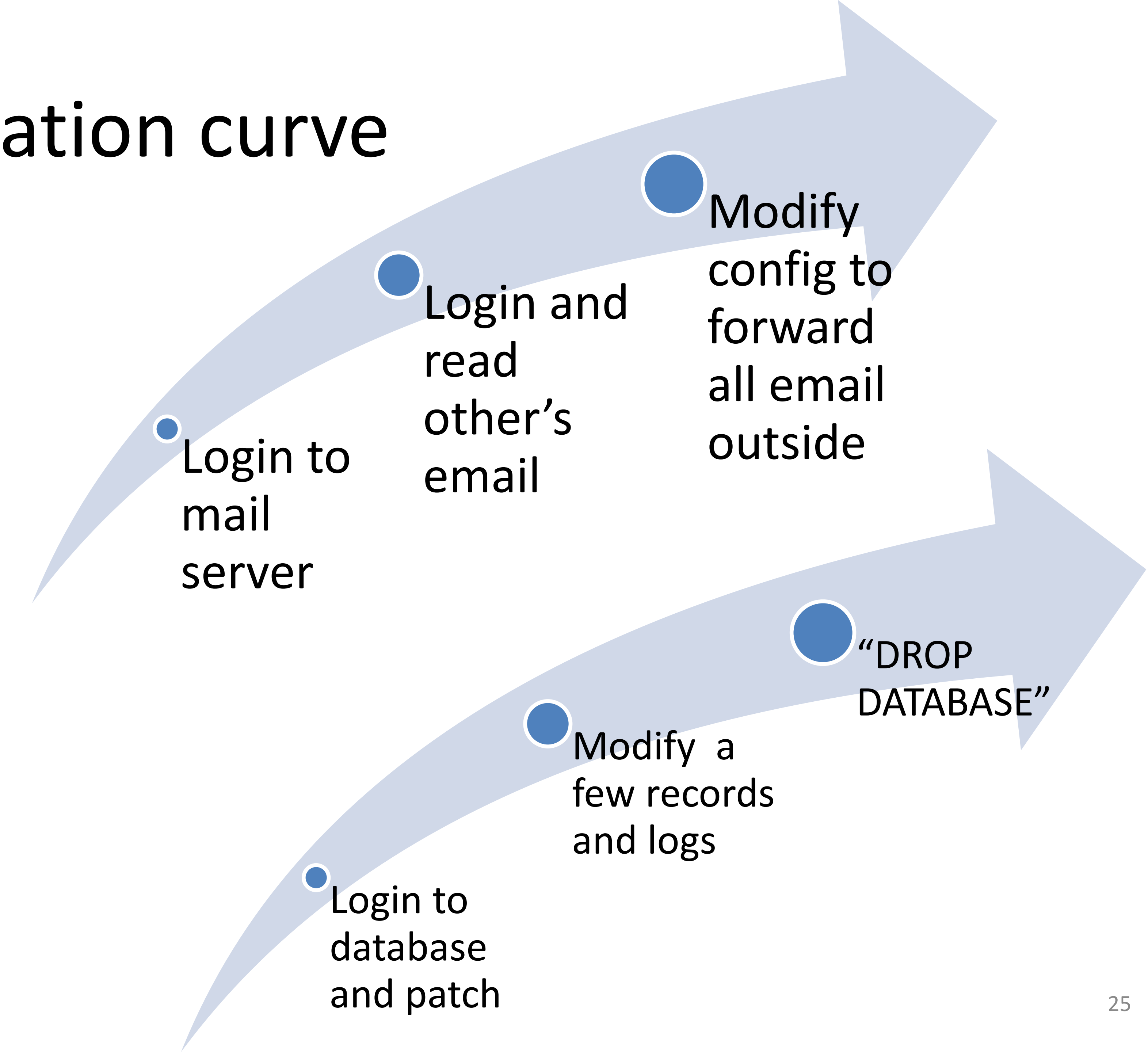
Fraud(9)	IT Sabotage(10)	Information Theft - Money(7)	Information Theft - Satisfaction (8)
・during his/her regular duty (4) ・studying similar abstraction cases reported in a newspaper. ・start it as a trial with curiosity ・stole password using key logger. Someone taught him how to use it	・login to Web server with ex-coworker’s account （2） ・login to Web server with one’s own superuser account (2) ・login to other server with one’s own superuser account (2) ・login PC with one’s own account ・login to server with co-worker’s account (using guessing)	・Modify mail server settings to forward all e-mail to his private account. Even after his termination. ・He/She is the admin for a server that contain sensitive personal information(2) **・there’s politics among staff. Then he installs key logger to PC’s of his opposition.**	・make secret back door on a server that enables him to connect from home. ・Modify mail server settings to forward all e-mail to his home. ・login to mail server with his boss’s ID. Successfully guess password.

More than half of 30 cases are preventable by disabling user account(s) right after termination.

Victims

- We could not find elements that victims have in common
- IT Sabotage: Small company, one single system administrator, selfish owner
- Pay less or no attention to security

Escalation curve



Login to mail server

Login and read other’s email

Modify config to forward all email outside

Login to database and patch

Modify a few records and logs

“DROP DATABASE”

HOW TO PREVENT

Considerations

- Pre-employment period
  - Check resume for certain points (job hopper? degree certificate)
  - Sign NDA
- During employment
  - Closer communication (company news letter, baseball tournament, other social events)
  - Check for visible sign (how they dress, work attitude)
  - Periodical audits, transfer as necessary
  - Try not to create too much dependency on one individual
    - Pair programming
- Upon termination
  - Suspend account immediately
  - Change passwords as necessary

Challenges for the future

- Technical details were not be clear from police investigative reports
- Need more case studies
  - No politically motivated cases
- Signs of insider threat, preventive measure could be different by country, culture and IT skill.
  - Global companies need measures for each area

Special Thanks To:

- SYAKAI ANZEN KENKYU ZAIDAN
  - http://www.syaanken.or.jp/02_goannai/08_cyber/cyber_f.htm (JAPANESE)
- National Police Agency

Thank you.