Strumenti e Strategie per il Monitoraggio e la Prevenzione delle frodi in Azienda

Maggio 2012 – Seminario Clusit Milano

Andrea Zapparoli Manzoni

Tipologie di Insider e rischi correlati

Da un lato (in particolare in Italia e nei paesi latini in genere) il problema crea imbarazzi, è "**tabu**", non se ne parla volentieri…

Dall'altro le tradizionali difese tecnologiche e organizzative sono poco efficaci e molto parziali contro gli Insiders…

Peculiarità dell'Insider Informatico: **tre diverse** classi di Insider

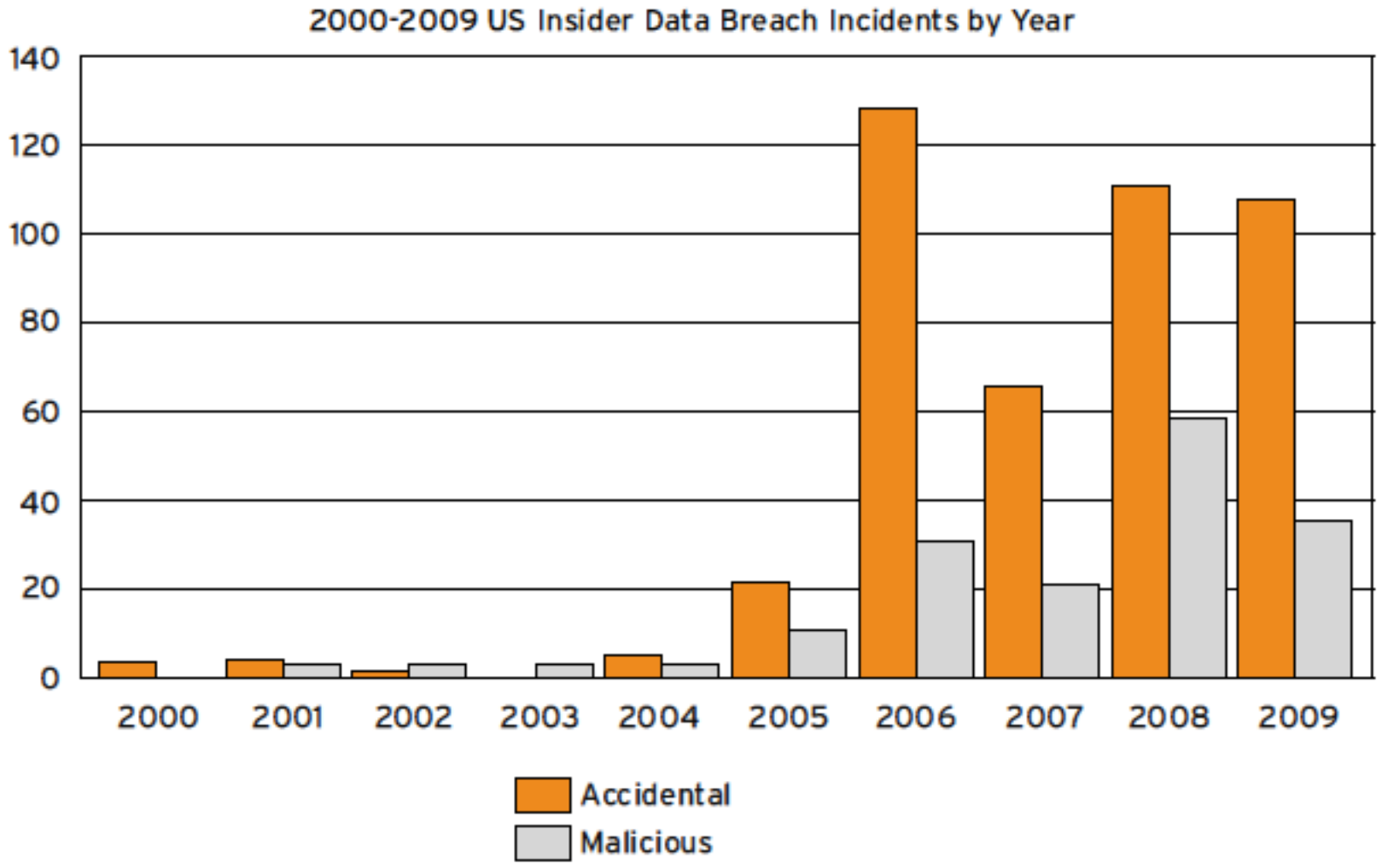
Unaware Insider, Low Profile, High Profile

Psicologia dell'Insider: soggetto a **Distorsioni cognitive** che abbassano la deterrenza e aumentano la propensione al crimine → …sono invulnerabile e intoccabile…

La **Propensione al crimine** negli Insider consapevoli **è indipendente** dal livello: maggiori responsabilità = aumento esponenziale del danno potenziale

-> Identificare gli High-Profile Insiders è una priorità per le Aziende

Distribuzione delle frodi per tipo di Insider



Il modello SKRAM di descrizione degli Insider

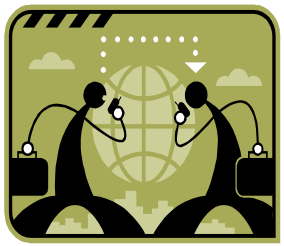
Modello FBI - SKRAM: combinazione di cinque attributi base

Skill, Knowledge, Resources, Access, Motive

Skill

Possiede massima Capacità tecnica sui possibili obiettivi di un attacco

Elevata intelligenza e capacità di pianificare



Knowledge

Possiede la conoscenza dell'ambiente e degli interlocutori, dei loro ruoli, etc.

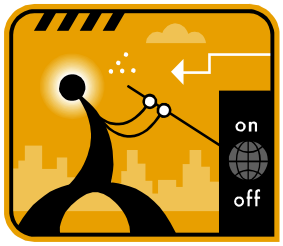
Conoscenza profonda delle difese in essere e delle procedure di controllo

Resources

Dispone di tempo e mezzi per costruire l'effrazione

Può "spegnere" i sistemi di difesa ed agire indisturbato,

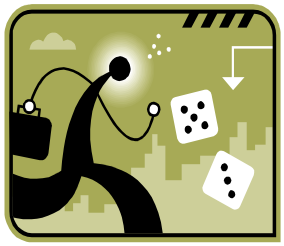
Può operare in più riprese



Access

Ha i Privilegi di accesso "logico" al massimo grado

Spesso autorizzato anche alla vicinanza "fisica"



Motive

Può essere attratto dallla possibile "impunità" eliminando le tracce

Potrebbe e saprebbe nascondere "errori" o incidenti

Quali sono le frodi interne più diffuse?

- falsi pagamenti
- accesso fraudolento a conti per ottenere/alterare dati
- fughe di informazioni / spionaggio industriale
- accesso sospetto a conti (es. Conti VIP)
- manipolazione di polizze e richieste di risarcimento
- furti di identita‘
- violazioni di norme / compliance
- sabotaggio IT
- hacktivism
- complicità con cybercriminali esterni

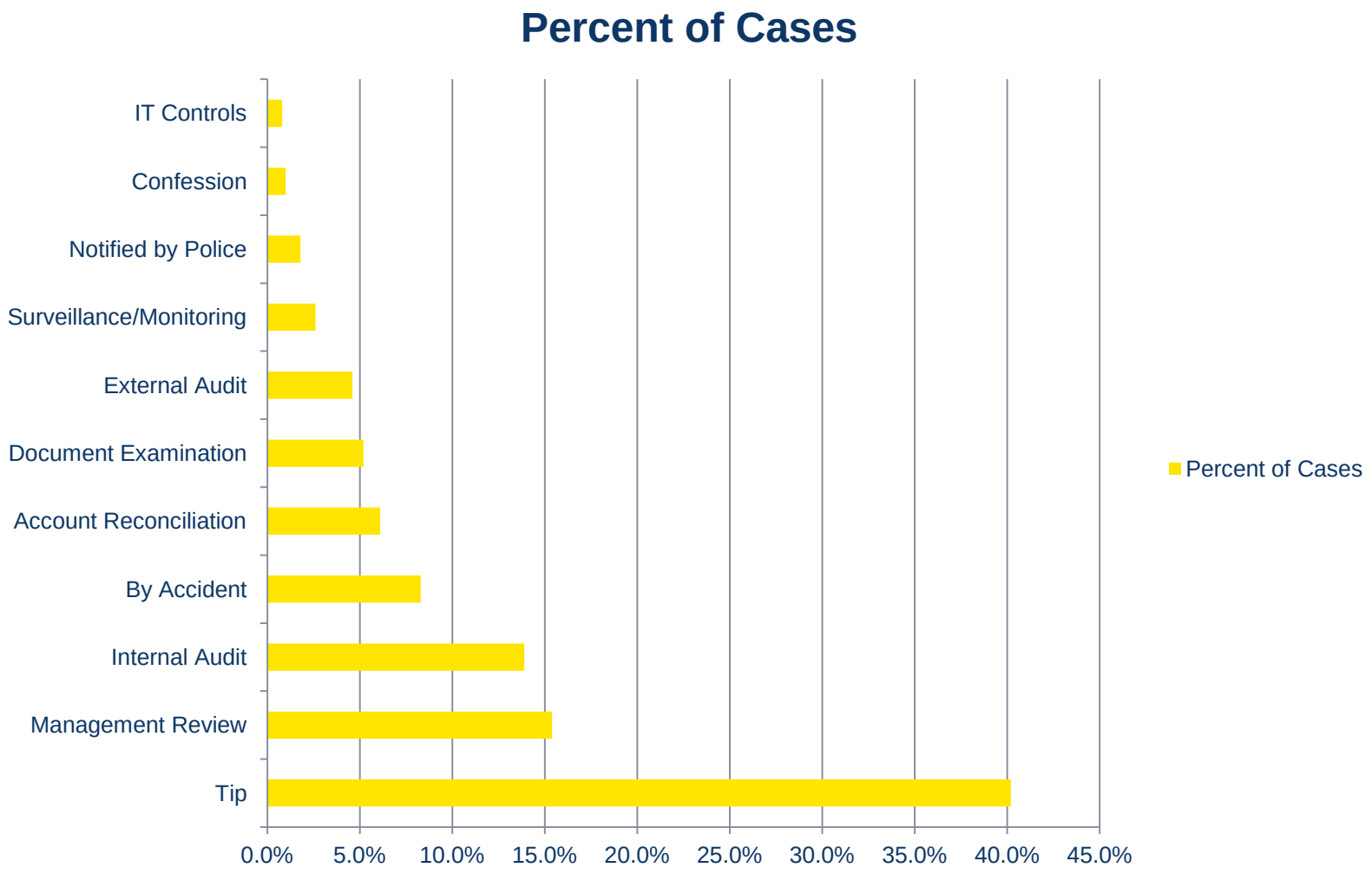
Come vengono scoperte le frodi interne?

40,2%	**soffiate**
1%	**confessioni**
0%	**confessioni in Europa**
0,6%	**controlli IT in Europa (*)**

Dati tratti da "Report to the Nations on Occupational Fraud and Abuse" 2010, ACFE 2010 Global Fraud Study

(*) Il dato relativo ai controlli IT complessivo e' pari allo 0.8%

Come vengono scoperte le frodi?



(*) Dati tratti da "Report to the Nations on Occupational Fraud and Abuse" 2010, ACFE 2010 Global Fraud Study

Quanto costano le frodi (e per quanto tempo)?

- Costi tipici sostenuti a cause di frodi interne (*):

  per una normale azienda:
  in media **5%** del fatturato ogni anno

  ¼ delle frodi causa un danno di almeno **$1.000.000**

  la cifra globale e' astronomica: $2.9 trilioni

- Tempo medio trascorso prima che una frode sia scoperta (*): **18 mesi**

(*) Dati tratti da "Report to the Nations on Occupational Fraud and Abuse" 2010, ACFE 2010 Global Fraud Study

Le tendenze sono preoccupanti

UK CIFAS survey 2011

+14,5% Aumento casi di frode nel 2011 (vs 2010)

+41% Aumento azioni di insider "consapevoli" (vs 2010)

+7,5% Aumento di account oggetto di frodi (vs 2010)

Dati tratti da "CIFAS Staff Fraud Trends" 2011 , CIFAS www.cifas.org.uk

I Problemi dell'Antifrode - #1 Attribution

Senza la certezza dell'attribuzione
le attività Antifrode sono sostanzialmente vanificate

- **l'endpoint non è trusted by design**

- **accesso non esclusivo / l'autenticazione non è forte**

- **furto di credenziali**

- **RATs**

- **Dossieraggio a tappeto durante attività "lecite"**

I Problemi dell'Antifrode - #2 Data Leakage Prevention

L'esfiltrazione dei dati può avvenire per canali non presidiati, anche in tempi diversi dalla consultazione

- **trashing**
- **stampanti (e manutentori)**
- **smartphones (BYOD?)**
- **rogue wifi**
- **microcamere / mal-hardware**
- **steganografia**
- **social networks**

I Problemi dell'Antifrode - #3 Separation of Duty

Per vari motivi, le organizzazioni non sono in grado e/o vogliono implementare efficacemente la SoD

- **"cui custodiet ipse custodies"**
- **AdS**
- **… e Developers**
- **Need to Know ed enforcement**
- **Complotto di insiders**
- **IDM, IAM & Role Engineering**

I Problemi dell'Antifrode - #4 Non Repudiation

1° mantra: Non Si Fa Security Con i Log di Sistemi non Trusted
2° mantra: L'Antifrode serve per Tutelare i Responsabili Legali Aziendali e per Vincere le Cause

- i log dei sistemi non sono validi a fini security

- la rete non è trusted

- catena di custodia invalida

-forensics impossibile

- le evidenze raccolte non sono opponibili a terzi

Strategie di contrasto alle frodi interne

- Monitoring and Investigative Processes
  - Monitoring & Logging
  - Forensics & Investigations
  - Threat Analysis & Assessment
- Risk and Vulnerability Management Processes
  - Risk Management
  - Vulnerability Management
  - Secure Development Life Cycle
- Response and Continuity Processes
  - Business Continuity Planning
  - Crisis Management
  - Incident Response

Awareness, responsabilizzazione, organizzazione, policies e tecnologie funzionano solo se applicati **insieme**.

Grazie!

Andrea Zapparoli Manzoni

a.zmanzoni@idialoghi.com