

SERVIZIO POLIZIA POSTALE E DELLE COMUNICAZIONI

**U.A.C.I.**

Unità di Analisi sul Crimine Informatico  
Computer Crime Analysis Unit



**insiders**

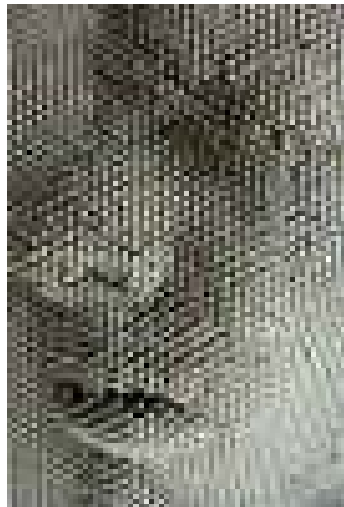
di Marco Strano

2004



## Rischi e costi degli attacchi inside

- Gli attacchi inside provocano i danni economici maggiori
- Gli attacchi esterni gravi vedono sempre la complicità di un inside





## L'origine dei comportamenti inside illegali in azienda

- Azioni deliberate per voglia di appropriazione o vendetta
- Azioni dovute a scarsa conoscenza delle norme
- Azioni dovute a scarsa valutazione dei danni provocabili
- Azioni dovute a bassa stima di essere scoperto



## Reati classici ad opera di insiders

- Uso dei sistemi informatici aziendali per scopi personali (peer-to-peer, email, web, scrittura, videogames ecc.)
- Piccole frodi ai danni dell'azienda (es. aggiunta giorni di ferie)
- Grandi frodi ai danni dell'azienda (agevolare un soggetto esterno nel ricevere un servizio)
- Piccoli sabotaggi (es. cancellazione di email e file vari di capi ufficio e colleghi per dispetto)
- Acquisizione di informazioni aziendali riservate per vantaggi personali interni all'azienda;
- Grandi sabotaggi (distruzione di dati importanti, danneggiamenti hardware per vendetta);
- Violazione della privacy di clienti dell'azienda;
- Acquisizione di informazioni aziendali riservate per favorire la concorrenza (spionaggio industriale).





## I criminali informatici “insiders”

1. Sono spesso dipendenti scontenti o consulenti informatici in contrasto con l'azienda;
2. Il movente più comune è la vendetta o la bramosia di guadagno;
3. Molti insiders dimostrano una bassa percezione del crimine;
4. Molti insiders spesso sono soggetti “non-criminali”.



Si allarga la base dei  
potenziali autori di reato



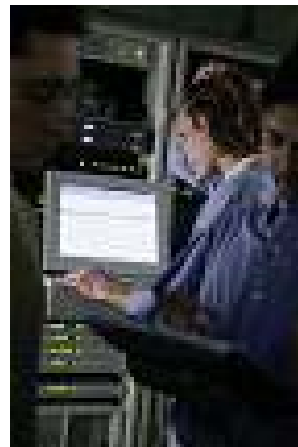
Aumentano i comportamenti illegali da parte di  
persone avulse al mondo del crimine

## La tecnologia informatica facilita alcuni crimini: lo spionaggio industriale



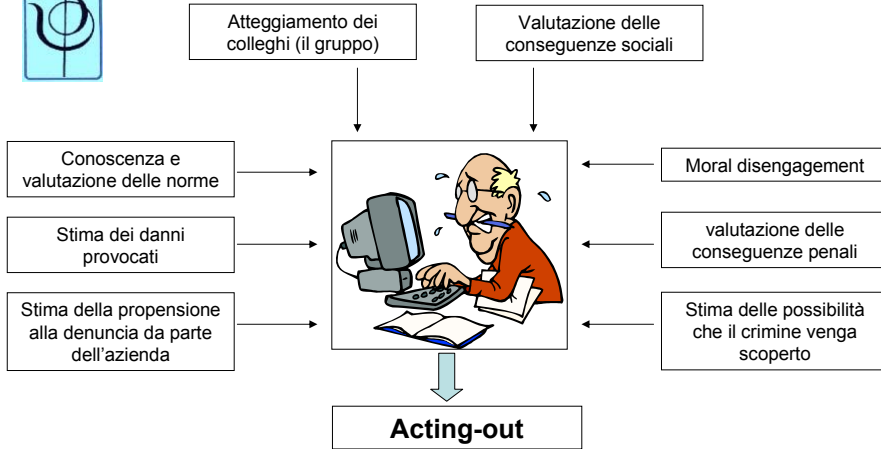
## Motivazioni degli insiders

- Psicopatologica
- Vandalica
- Appropriativa
- Vantaggi personali
- Danneggiare l'azienda
- Danneggiare un superiore gerarchico
- Danneggiare un parigrado/subordinato
- Sfida nei confronti del sistema





Il criminal decision making process: gli insiders prima di commettere un illecito, valutano i pro, i contro e le conseguenze.



## Alcuni processi percettivi modificati dal computer

- Percezione dell'illegalità del comportamento
- Stima dei rischi di essere scoperto
- Stima dei rischi di essere denunciato
- Percezione del danno procurato alla vittima
- Paura della sanzione sociale
- Paura della sanzione legale





## L'ORIGINE PSICOLOGICA DEL RISCHIO "CRIMINE" ALL'INTERNO DELLE AZIENDE

- LA PERCEZIONE DEL CRIMINE PUO' CONTEMPLARE ERRORI O DISTORSIONI COGNITIVE DOVUTI A SCARSA INFORMAZIONE.
- LA SCELTA CRIMINE/NON CRIMINE PUO' BASARSI QUINDI SU CONVINZIONI ERRATE



## Alcune tipiche distorsioni cognitive dei dipendenti di una azienda (informazioni non vere ma diffuse)

- L'azienda non effettua monitoraggio interno alla rete
- L'azienda non denuncierebbe un crimine informatico inside
- I danni provocabili dal mio comportamento sono lievi
- Le sanzioni penali sui crimini informatici sono lievi





Nel computer crime scompare il contatto fisico tra autore del reato e vittima



# la tecnomediazione



## LA TECNOMEDIAZIONE IN UN CRIMINE

- attenua la percezione da parte del delinquente degli effetti negativi prodotti sulla vittima;
- allarga la base dei possibili autori di reato rendendo adatti al crimine molti individui avulsi al mondo dell'illegalità;
- crea un fenomeno di illegalità distribuita in larghe aree sociali (ad esempio nell'ambito della violazione dei diritti d'autore);
- diffonde atteggiamenti di impunità su determinati crimini (spesso basati su errori cognitivi e logici);
- si accompagna ad una scarsa conoscenza delle leggi civili e penali in materia.

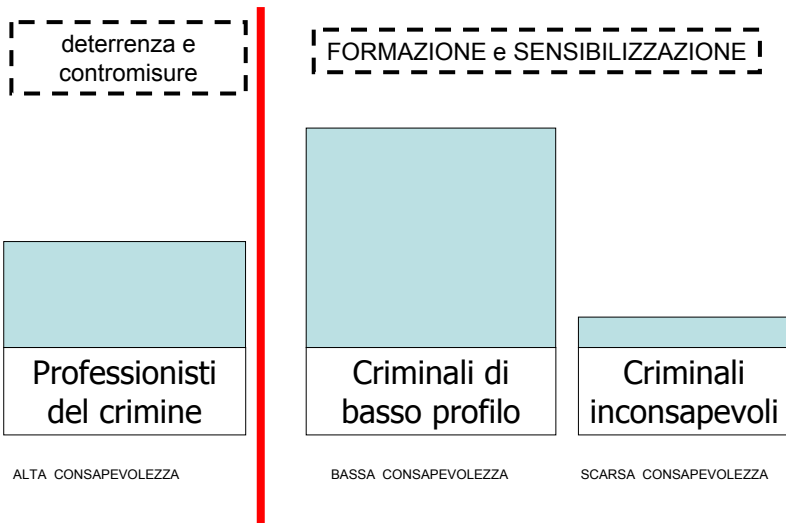


GLI ERRORI COGNITIVI DOVUTI ALLA  
TECNOMEDIAZIONE SI POSSONO  
CORREGGERE CON:

- STRUMENTI DI MISURAZIONE (interviste e questionari) per localizzare le distorsioni cognitive e gli atteggiamenti disfunzionali
- FORMAZIONE IN AULA
- FOCUS GROUP



## Il computer crime in azienda e la consapevolezza del crimine: le soluzioni





## Come prevenire il computer crime ad opera di insiders

1. Miglioramento delle tecnologie di sicurezza anche per gli attacchi provenienti dall'interno
2. Formazione capillare di tutto il personale della P.A. e delle aziende private alla "cultura della legalità informatica" e alla "cultura della sicurezza informatica"
3. Incentivare la ricerca scientifica sull'argomento
4. Creazione di una banca dati dei crimini informatici inside
5. Maggiore attenzione nella selezione del personale (anche C.I.T.I. e consulenti)



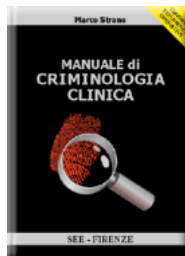
## Maggiore attenzione nella selezione del personale

- abitualmente le valutazioni più rigorose vengono effettuate dall'azienda nei confronti dei dipendenti che saranno inseriti in maniera più o meno stabile nell'organico (full-time o part-time)
- minore attenzione viene usualmente rivolta a soggetti che hanno rapporti di lavoro con posizione più esterna (es. consulenti, tecnici, manutentori) che rappresentano sovente l'ossatura dei lavoratori C.I.T.I (Critical Information Technology Insiders) nell'azienda.



## Selezione accurata anche dei consulenti informatici esterni

- nel settore informatico, anche soggetti che operano temporaneamente e marginalmente nella struttura aziendale acquisiscono un grande potere gestionale e possono essere in grado di procurare danni gravissimi in caso di disonestà.
- si rileva spesso un'approssimativa richiesta di informazioni da parte dell'azienda che assume dei consulenti (o dei dipendenti con contratti a termine) con scarsa valutazione di eventuali precedenti, (ad esempio di appartenenza a gruppi di hacking).
- si rileva talvolta reticenza di molti imprenditori nel fornire informazioni su loro ex-dipendenti per non rivelare problematiche aziendali riservate.



Quattro testi per approfondire

e su internet: [www.criminologia.org](http://www.criminologia.org)

