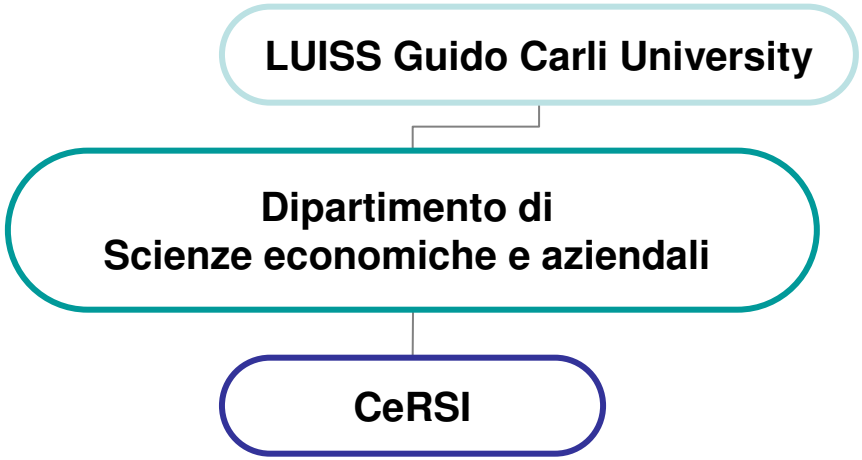
Investigazioni telematiche

Aspetti organizzativi e tecnici

(a cura dell'Ing. Paolo Spagnoletti **- CeRSI LUISS**)

CeRSI: Centro di ricerca sui Sistemi Informativi



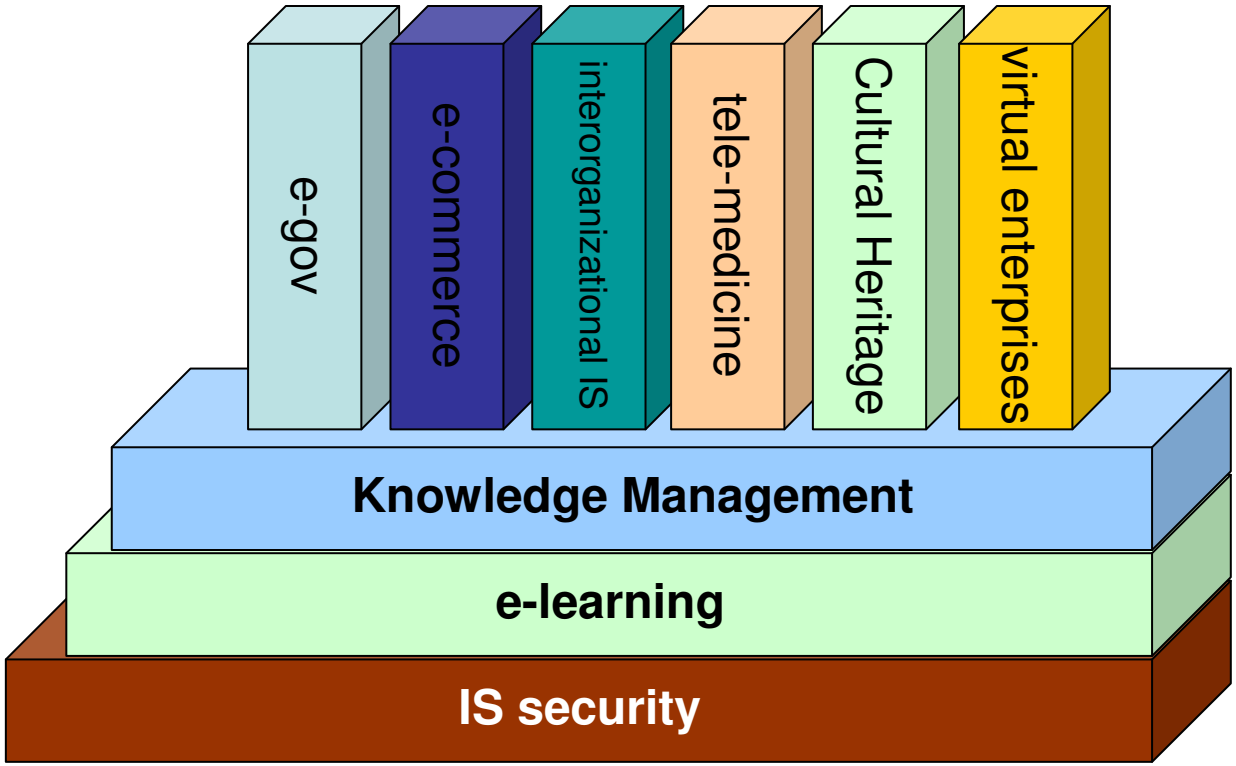
LUISS (Libera Università Internazionale degli Studi Sociali) "Guido Carli" is one of the most prestigious Italian private universities, strongly co-operating with the main Italian research centres, industries, and public administrations.

The Centro di Ricerca sui Sistemi Informativi (CeRSI) is in charge of the research, education and advice on computer science and information systems matters.

CeRSI: Centro di ricerca sui Sistemi Informativi

- in charge of research and education in Luiss on Information Systems and ICT
- supports PhD SIA, thesis, ECDL
- research projects:
  - attivi: OK-EG (Miur), MobiDis (CNR), EETH (Leonardo), Minerva (EC-IST), Tacit (EC-IST)
  - previsti: Virtuose, Ontodev, OTourism, FIRB,....
  - conclusi: VirtuEnt, FairsNet , Fairwis, MediMedia, e-commerceItaly, MedMark, Hermes
- conferences: Ethicomp99, OESSEO2001, Org2004

IS security


e-gov
e-commerce
interorganizational IS
tele-medicine
Cultural Heritage
virtual enterprises
Knowledge Management
e-learning
IS security

INDICE DELLA PRESENTAZIONE :

1. Introduzione
2. Scenario attuale
    1. minacce interne
    2. D.Lgs 231/2001
3. Investigazioni telematiche e internet
4. IS security Management
5. Computer forensics
6. Forensic accounting
7. Conclusioni
8. Riferimenti bibliografici e sitografici
9. Varie Q&A

Cybercrime

sistema informatico:

- obiettivo del crimine (attacchi alla conf, int, e disp, crime against computers)
- repository di informazioni utilizzate o generate nel commettere un crimine (sistema passivo di memorizzazione, computer assisted crime)
- strumento che consente di commettere un crimine (strum. di comunicazione per cybercrime, computer assisted crime)

cybercrime: crimine che lascia tracce digitali (Casey)

Crimine digitale vs crimine tradizionale

- numero elevato di potenziali sospetti
- difficile identificazione del crimine
- quantità di materiale probatorio
- facile contaminazione delle prove

Investigazioni telematiche

computer forensic: identificare, preservare ed analizzare informazioni memorizzate, trasmesse o prodotte da un pc o rete per riflettere sulla validità di ipotesi che cercano di spiegare le circostanze o cause di un'attività sotto investigazione, e che sia valida ai fini probatori

Investigazioni telematiche

intrusion forensic: recupero e analisi di informazioni da pc o reti sui quali ci sia il sospetto di violazioni. Tali informazioni possono includere dati di traffico, di payload, dati memorizzati su PDA, contenuto di flash memory, analisi della struttura organizzativa etc. e consentono all'investigatore di riflettere sulla validità di ipotesi che cercano di spiegare le circostanze o cause di un'attività sotto investigazione. Possibilmente le informazioni devono poter essere utilizzate come prove nel corso di procedimenti penali o civili.

entrambe condividono tecniche, metodi e strumenti tipici della computer security

INDICE DELLA PRESENTAZIONE :

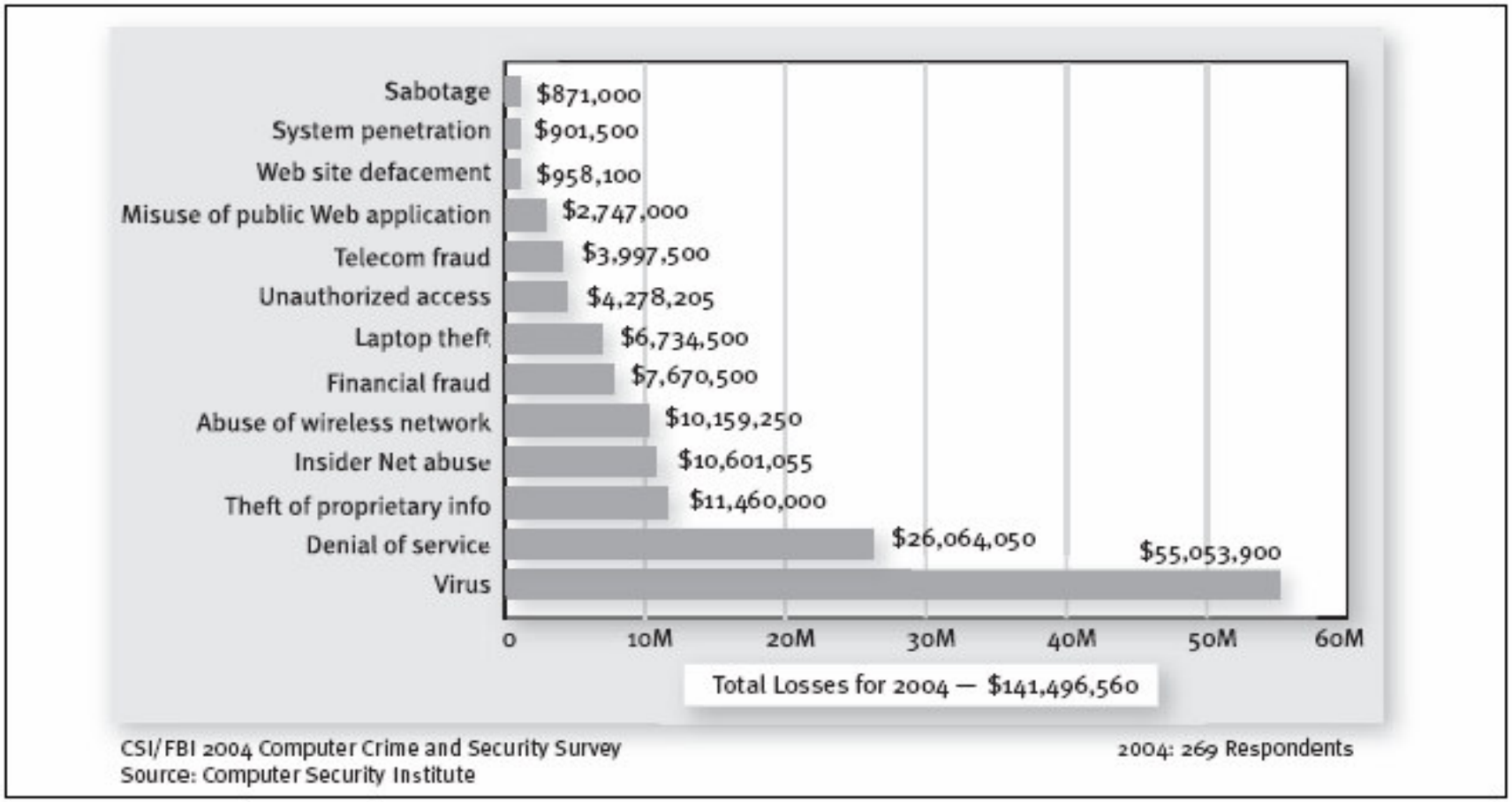
1. Introduzione
2. Scenario attuale
    1. minacce interne
    2. D.Lgs 231/2001
3. Investigazioni telematiche e internet
4. IS security Management
5. Computer forensics
6. Forensic accounting
7. Conclusioni
8. Riferimenti bibliografici e sitografici
9. Varie Q&A

Scopo dell'investigazione

- cause civili (computer fraud)
- procedure disciplinari interne (computer abuse)
- l'obiettivo è l'individuazione di:
  - azioni in corso
  - azioni già effettuate
  - azioni pianificate

Stakeholders

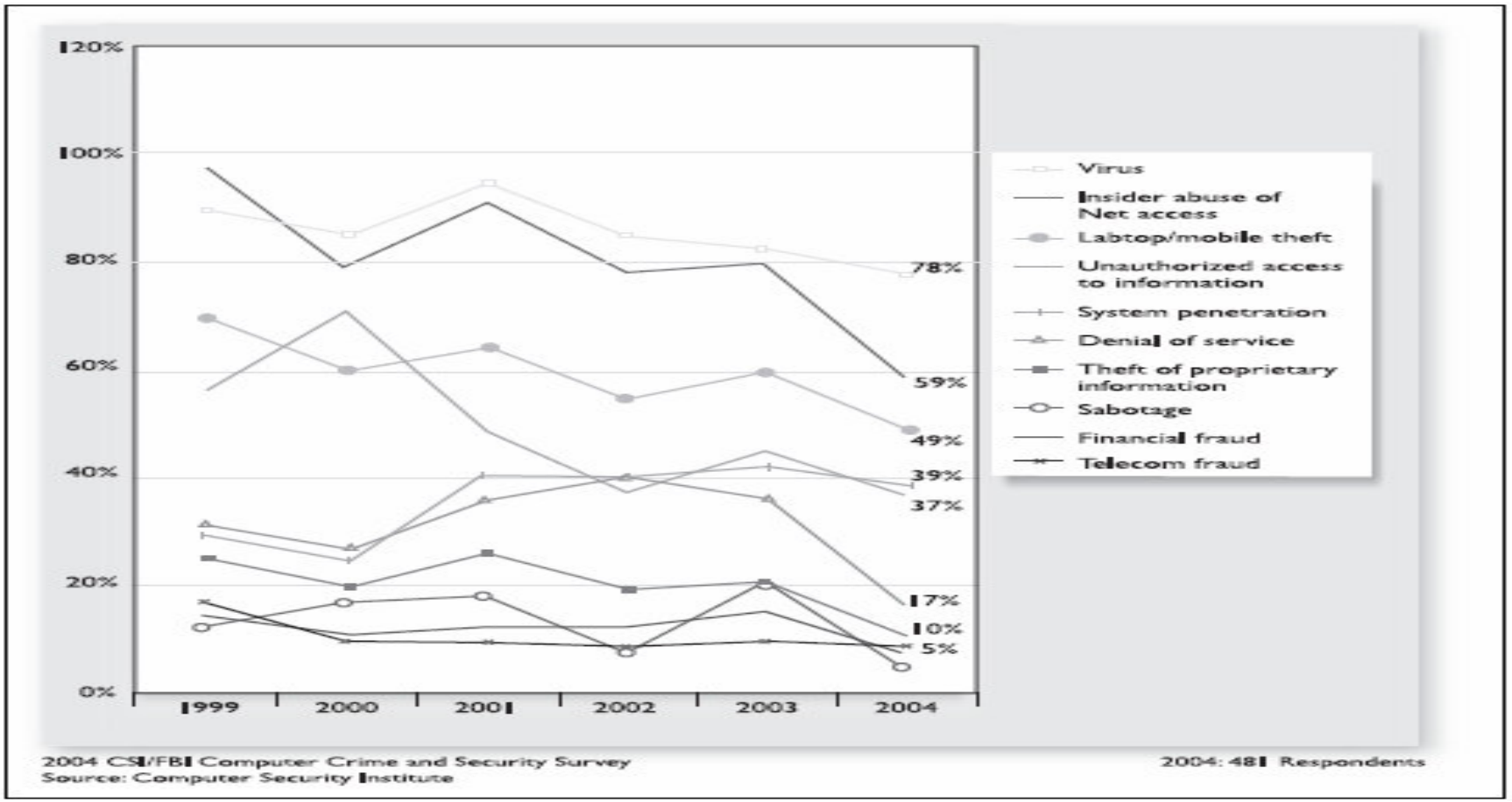
Danni economici: computer security incident



INDICE DELLA PRESENTAZIONE :

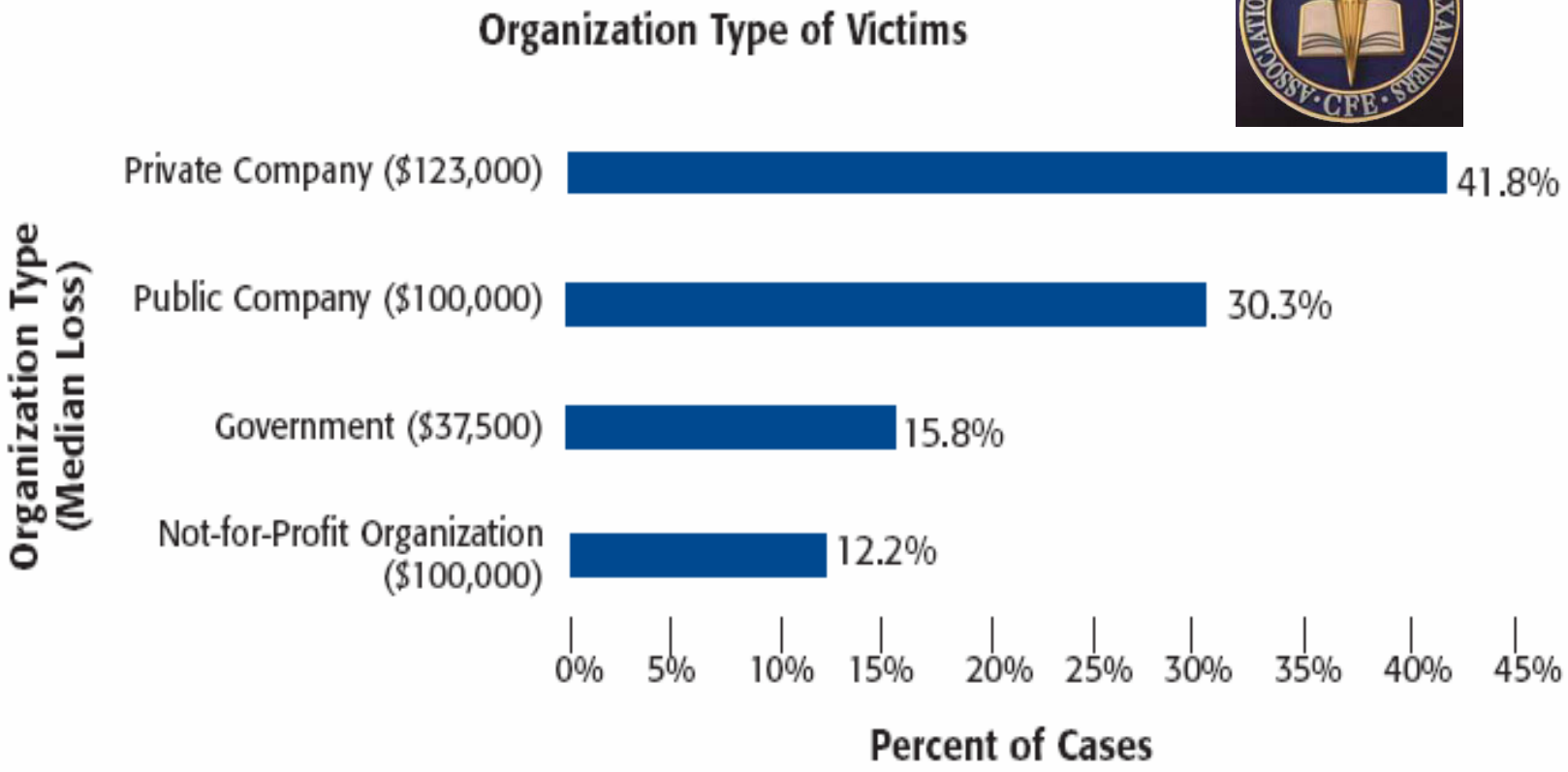
1. Introduzione
2. Scenario attuale
    1. minacce interne
    2. D.Lgs 231/2001
3. Investigazioni telematiche e internet
4. IS security Management
5. Computer forensics
6. Forensic accounting
7. Conclusioni
8. Riferimenti bibliografici e sitografici
9. Varie Q&A

Origine degli attacchi



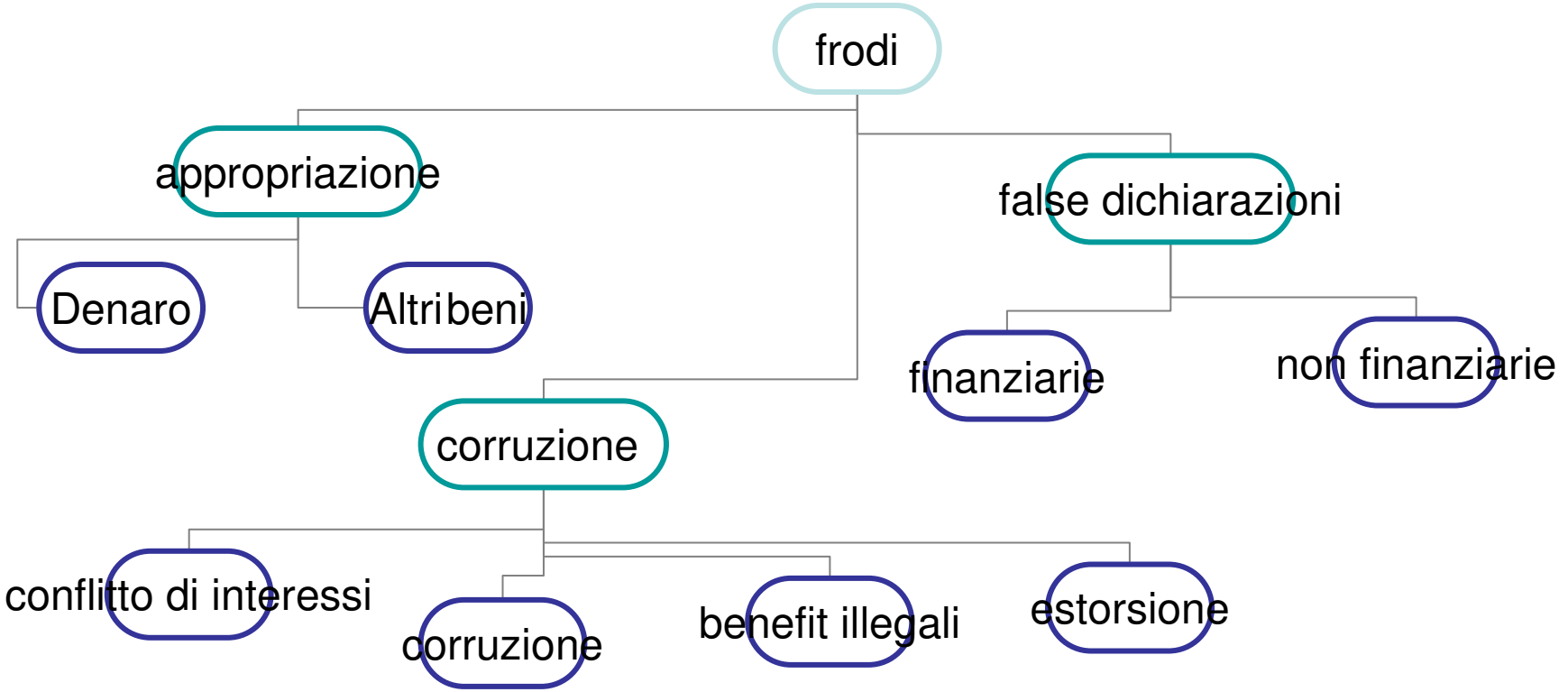
Danni economici: frodi interne

2004 Report to the Nation on Occupational Fraud and Abuse



Classificazione frodi

2004 Report to the Nation on Occupational Fraud and Abuse



Frodi interne

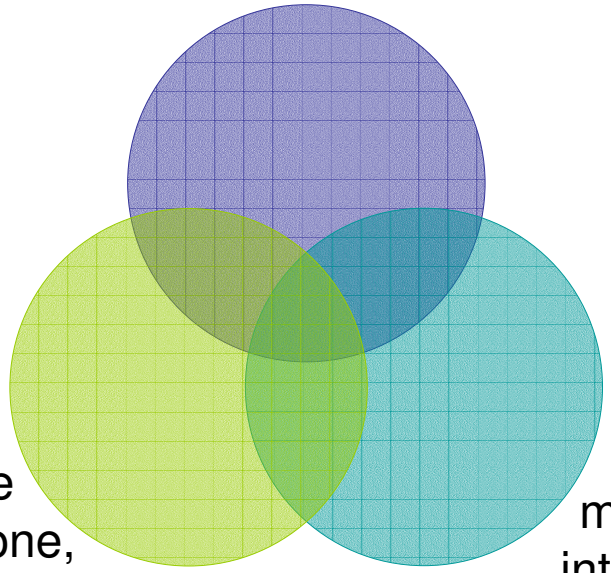
Esempi di frodi interne:

- fornitori fittizi
- duplicazione pagamenti
- furti di inventario
- manipolazione non autorizzata di dati
- divulgazione informazioni sensibili
- falsificazione bilanci e report
- commissioni segrete
- spese non autorizzate
- insider trading

I drivers della frode

Contromisure

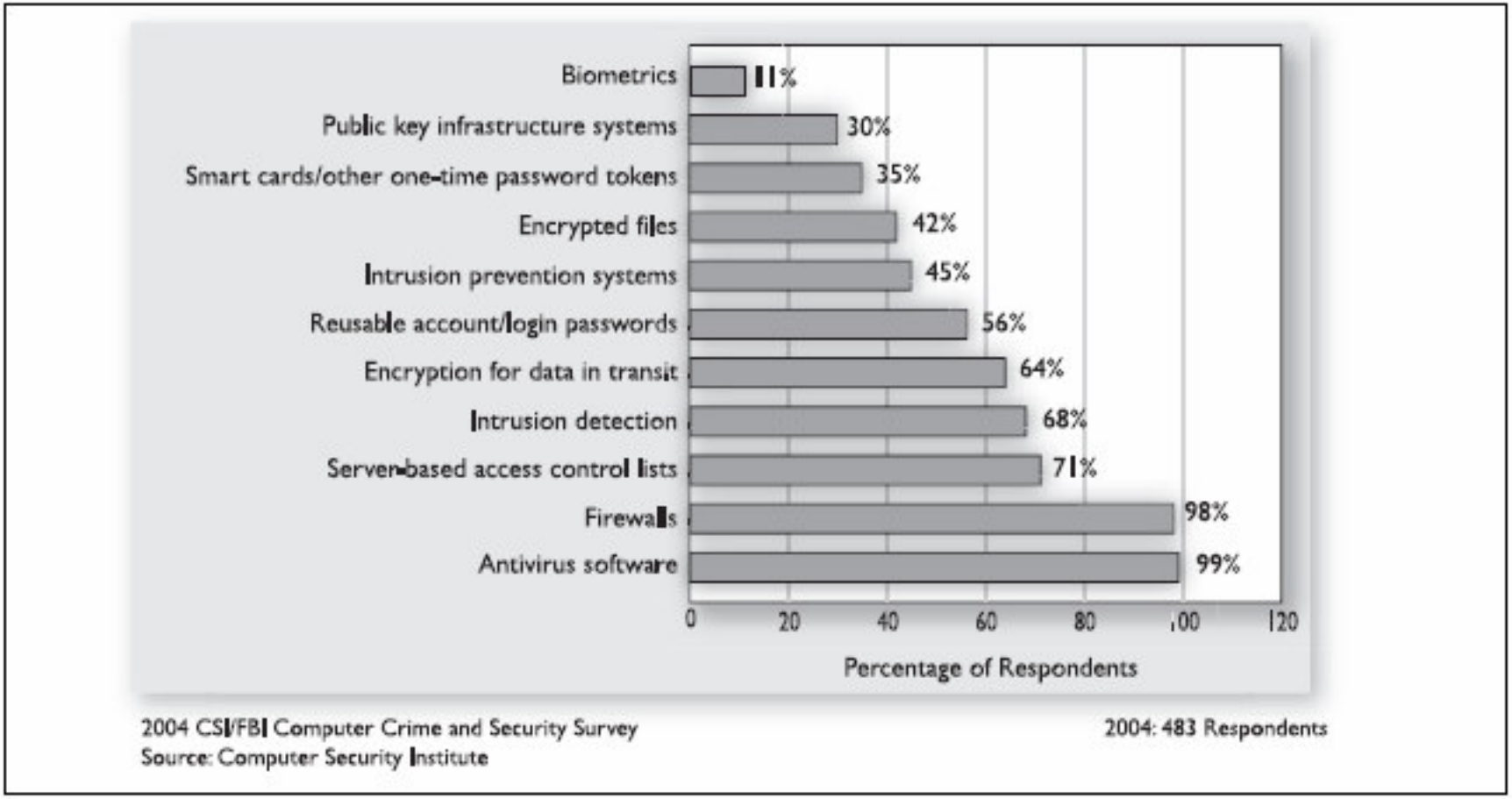
Tecnologiche
(tracciabilità, autenticazione, etc.)



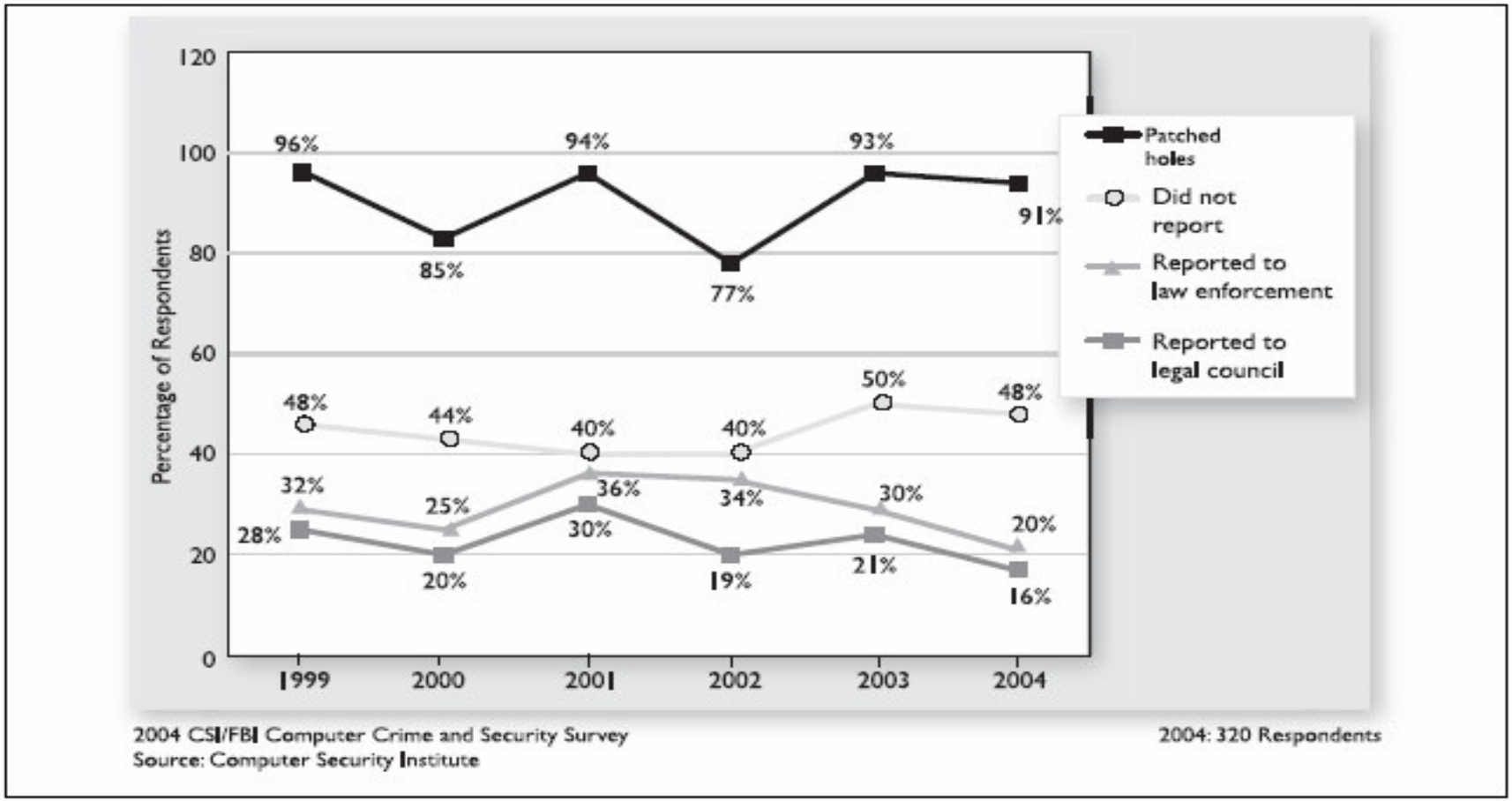
Organizzative
(policy, formazione,
campagne di awareness)

Capacità di
monitoraggio e
intervento anche
real time

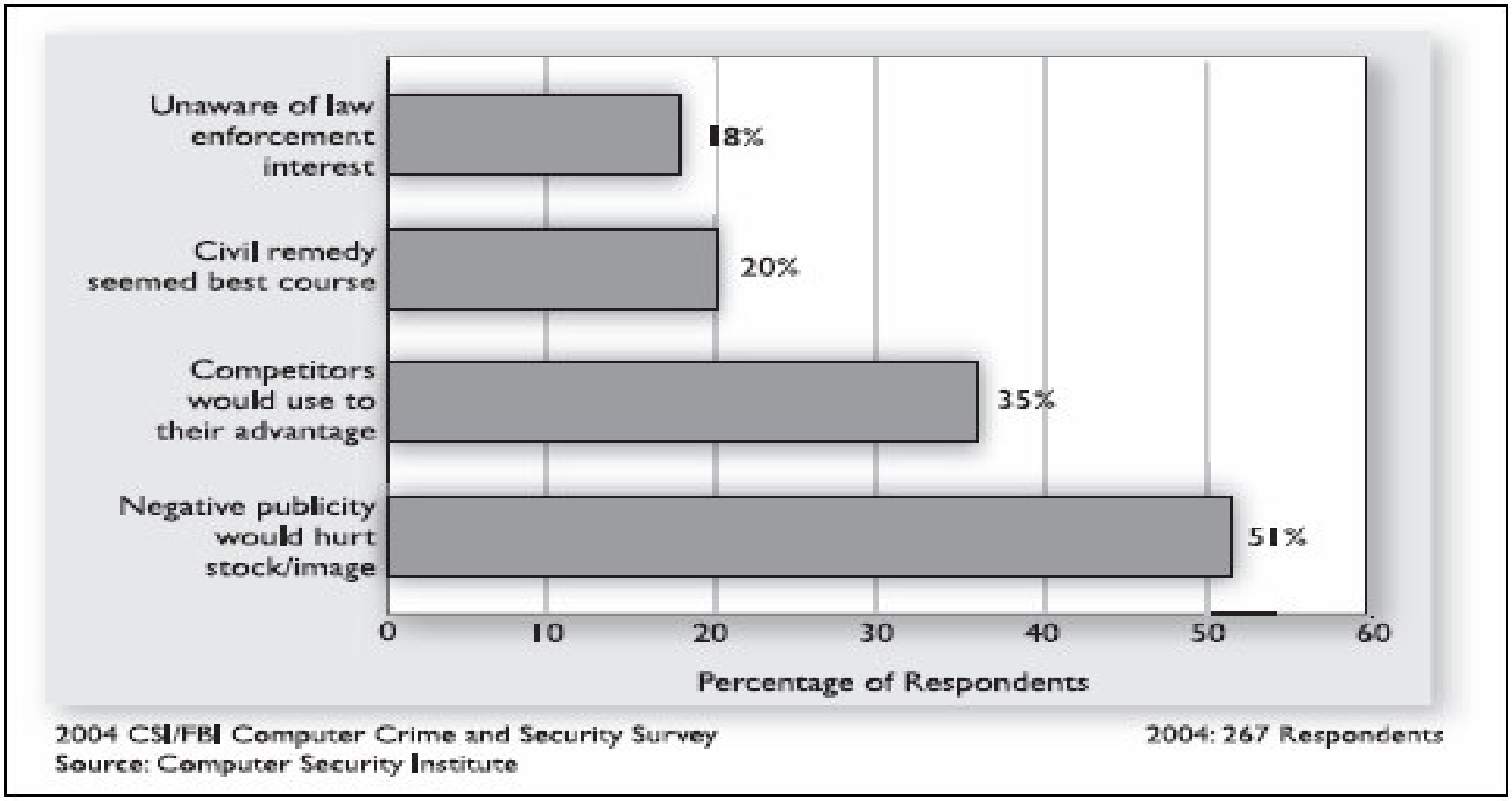
Tecnologie di sicurezza adottate



Azioni intraprese



Ragioni organizzative



INDICE DELLA PRESENTAZIONE :

1. Introduzione
2. Scenario attuale
    1. minacce interne
    2. D.Lgs 231/2001
3. Investigazioni telematiche e internet
4. IS security Management
5. Computer forensics
6. Forensic accounting
7. Conclusioni
8. Riferimenti bibliografici e sitografici
9. Varie Q&A

D.Lgs. 231/2001

- Introduzione nell'Ordinamento del principio della **responsabilità amministrativa** di persone giuridiche, di società e di associazioni anche prive di personalità giuridica, per **reati commessi a favore o a vantaggio dell'ente** da persone che rivestono funzioni di rappresentanza, amministrazione, direzione (**apicali**) o da **subordinati**.
- Fattispecie di reato attualmente disciplinate:
  - Reati contro la Pubblica Amministrazione – Artt. 24 e 25 (corruzione, concussione, malversazione, truffa, frode informatica)
  - Reati di falsità in monete e valori di bollo Art.25 bis
  - Reati societari Art.25 ter

D.Lgs. 231/2001

Fattispecie di reato attualmente disciplinate (segue):

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico Art.25 quarter
- Delitti contro la personalità individuale Art.25 quinqies (pornografia, prostituzione e sfruttamento minorile, riduzione in schiavitù, niziative turistiche volte allo sfruttamento della prostituzione minorile ecc.)

Sanzioni di carattere pecuniario e di carattere interdittivo (quali ad esempio sospensione o revoca di autorizzazioni, licenze o concessioni esclusione da finanziamenti, agevolazioni e contributi)

D.Lgs. 231/2001

possibilità di **esenzione** dalla responsabilità in capo all'ente, qualora l'organo dirigente dimostri (**elemento esimente**):

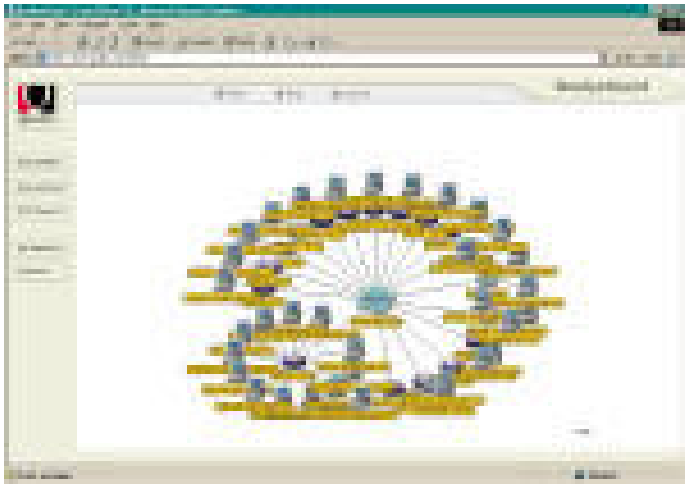
a) di aver adottato ed efficacemente attuato, prima della commissione del reato, modelli organizzativi e di gestione idonei a prevenire le fattispecie di reati precedentemente indicate;
b) di aver affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo il compito di vigilare sul funzionamento e sull'osservanza di detti modelli e di curare il loro aggiornamento;
c) che il reato è stato commesso eludendo fraudolentemente i modelli di organizzazione e gestione;
d) che non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di controllo di cui alla lettera b).

INDICE DELLA PRESENTAZIONE :

1. Introduzione
2. Scenario attuale
    1. minacce interne
    2. D.Lgs 231/2001
3. Investigazioni telematiche e internet
4. IS security Management
5. Computer forensics
6. Forensic accounting
7. Conclusioni
8. Riferimenti bibliografici e sitografici
9. Varie Q&A

Evoluzione investigazioni telematiche

prima di internet: investig. su singolo PC, forze di polizia



dopo internet:

nuovi skills, tracce frammentate, difficoltà di ricostruzione del caso

Ruolo di internet

- nuovi tipi di crimine (interventi sanzionatori a livello normativo)

ma anche…

- la connettività globale accresce il numero di crimini che lasciano tracce digitali: un crimine può essere avviato, pianificato, e parzialmente eseguito nel ciberspazio

Criticità

- conflitto tra competitive objectives (obiettivi di business) e good behaviour (leggi, regolamenti, aspetti etici)
- privacy (diritti dell'uomo) e crime discovery (monitoraggio e tracciabilità)

INDICE DELLA PRESENTAZIONE :

1. Introduzione
2. Scenario attuale
    1. minacce interne
    2. D.Lgs 231/2001
3. Investigazioni telematiche e internet
4. IS security Management
5. Computer forensics
6. Forensic accounting
7. Conclusioni
8. Riferimenti bibliografici e sitografici
9. Varie Q&A

Standard BS7799

- Un riferimento per la certificazione della capacità di un'organizzazione di tutelare il proprio patrimonio informativo e di mantenere tale capacità nel tempo
- Una raccolta di *best practice* in materia di sicurezza delle informazioni
- Un riferimento metodologico per la gestione della sicurezza del patrimonio informativo aziendale

Ambito degli Standard

- La sicurezza dell'informazione è vista nel senso pieno dell'accezione, **non limitato alla sfera delle tecnologie informatiche per il trattamento**

- Ogni organizzazione dovrebbe proteggere le informazioni che tratta mediante un Sistema di Gestione della Sicurezza delle Informazioni composto di **componenti logiche, fisiche e organizzative**

I concetti fondamentali

1. Politica di sicurezza dell'informazione

2. Sistema di Gestione della Sicurezza delle Informazioni
   (Information Security Management System, ISMS)
3. Controlli di sicurezza

4. Dichiarazione di applicabilità
   (Statement of Applicability, SoA)

Standard
BS 7799 - 2:2002

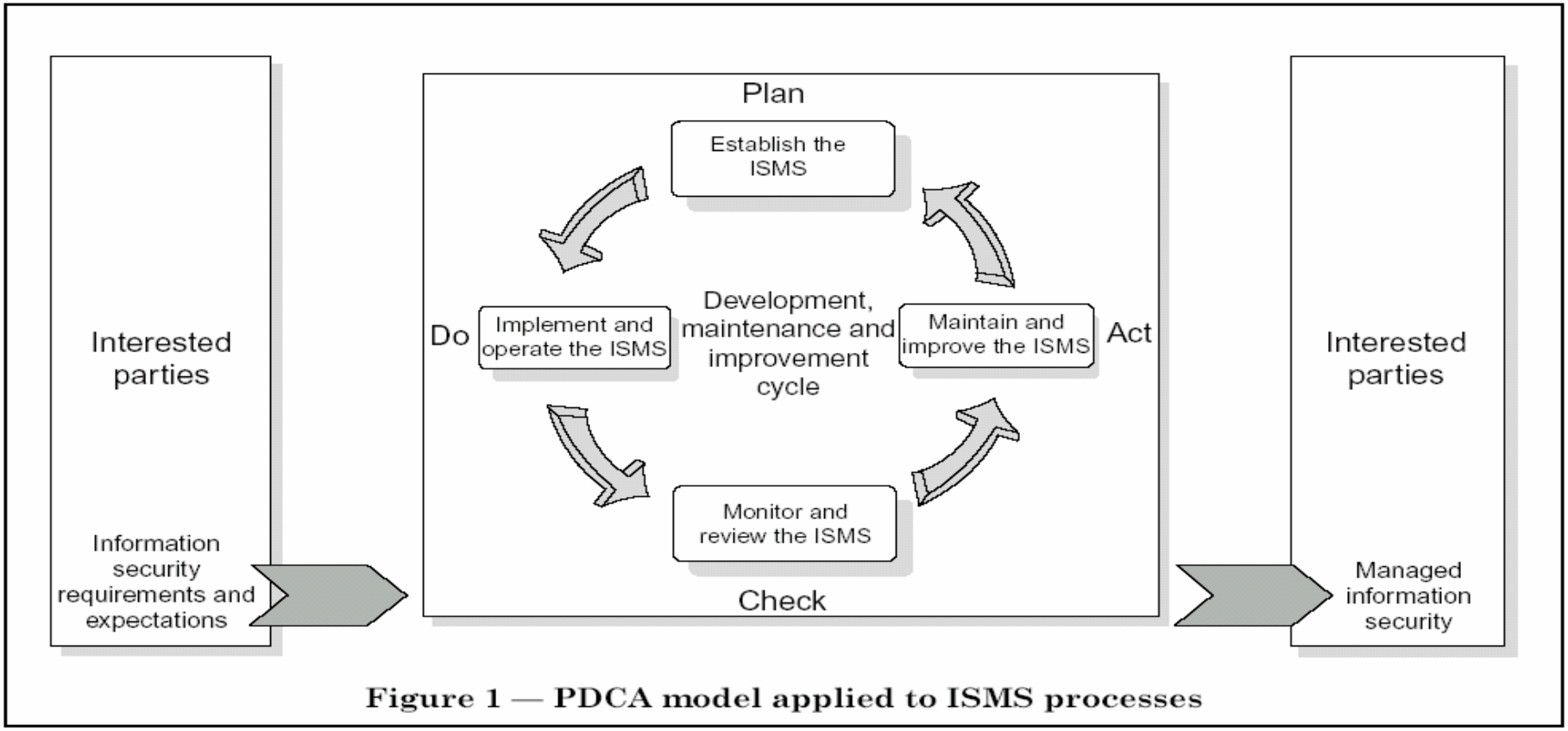


Figure 1 — PDCA model applied to ISMS processes

Computer security vs Computer forensics

stessi strumenti e dati ma
scopi differenti

CS

prevenzione (risk management, analisi costi/benefici)

CF

investigazione (tracciabilità)

INDICE DELLA PRESENTAZIONE :

1. Introduzione
2. Scenario attuale
    1. minacce interne
    2. D.Lgs 231/2001
3. Investigazioni telematiche e internet
4. IS security Management
5. Computer forensics
6. Forensic accounting
7. Conclusioni
8. Riferimenti bibliografici e sitografici
9. Varie Q&A

Computer forensics

riguarda:

-Raccolta,

-Conservazione,

delle prove identificabili in un sistema di elaborazione, come pure **l'uso** di queste prove in un procedimento legale.

Computer forensics

PROVE:
FISICHE (Componenti HW);
LOGICHE (Dati).

La parte FISICA comprende la Ricerca ed Acquisizione (**search and seizure**) delle prove. Ovvero, l'investigatore acquisisce (per quanto possibile) tutti quei media che possono essere connessi con il crimine.

La parte LOGICA della CF riguarda l'estrazione dei dati grezzi da qualsiasi fonte rilevante. Questo processo è noto anche come Scoperta dell'informazione (**information discovery**)

Computer forensics

Il TOOL (*organizzativo*) più importante per l'investigatore è la salvaguardia della prova stessa, ovvero la "catena della custodia" (**chain of custody**).

Essenzialmente, tiene traccia:
— di chi ha avuto in custodia la prova;
— di quali operazioni sono state condotte sulla prova.

OBJ: dimostrare che la prova non è stata alterata (accidentalmente o maliziosamente)

Computer forensics

SIMILARITA' E DIFFERENZA CON ALTRI FENOMENI INVESTIGATIVI

SIMILARITA':
Le prove, quando maneggiate con imperizia, o con una catena di custodia debole, possono diventare inutili

DIFFERENZE:
Sono richiesti una composizione di capacità del processo investigativo classico più una buona expertise nel settore della CS (meglio, dell'ICT).

Computer forensics

SIMILARITA' E DIFFERENZA CON ALTRI FENOMENI INVESTIGATIVI

COMPLESSITA'

-sorgenti di dati;

La prova non è un singolo oggetto, ma può nascere dall'inferenza del processo cognitivo applicato su diversi oggetti, nessuno di per sé costituente una prova.

-Volatilità

Data la natura digitale della prova, la stessa può essere facilmente alterata, senza possibilità di rilevamento

Computer forensics

SKILLS:

Buona conoscenza dei SO;

Buona conoscenza della pratiche di Amm.ne di diversi sistemi;

Buona conoscenza dei principi di sicurezza dei sistemi

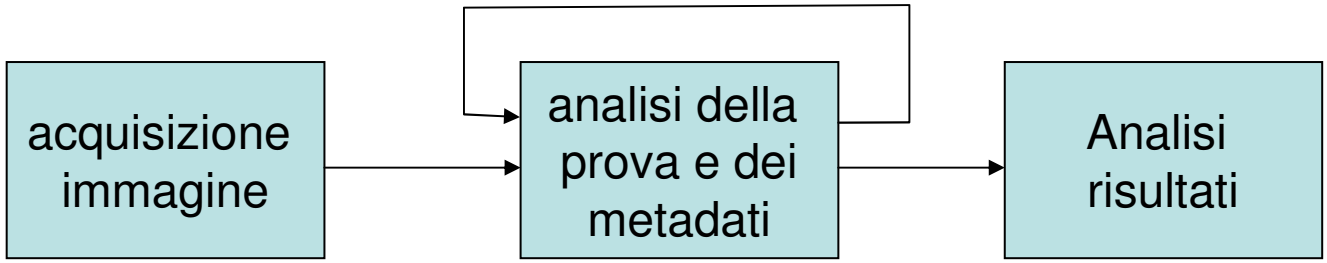
Deve essere un ottimo investigatore: Immaginazione, capacità di analisi, inferenziali e deduttive.

TOOLS:

HW / SW ….

- sviluppati in proprio;
- di uso pubblico.

Modello operativo



I metadati sono le informazioni generate durante il processo di investigazione (file timestamps, autore, permessi, etc.) che rendono variabile il volume dei dati da analizzare nel corso del processo stesso

Approccio metodologico

Un esempio di metodologia applicabile per l'analisi forense si compone di due parti:

1. search and seizure;
2. information discovery.

Come visto, possiamo equipararle ad un processo FISICO e ad un processo LOGICO.

Nel search and seizure, l'investigatore interviene sulla scena del crimine e si confronta con il compito di recuperare ed elaborare le **prove** (prove fisiche, ovvero i dispositivi).

L' information discovery richiede che l'investigatore acceda ai dati nel tentativo di localizzare ed elaborare le informazioni che possono validare od invalidare una qualche tesi.

Approccio metodologico

(A) Pianificazione	**(B)** Raggiungere e rendere "sicura" la scena del crimine	**(C)** Documentare la scena del crimine	**(D)** Ricerca delle prove	**(E)** Recuperare le prove	**(F)** Elaborare le prove

Descrizione ad alto livello del processo di Search and Seizure

Approccio metodologico

(A) Pianificazione	**(B)** Ricerca delle prove	**(C)** Elaborazione delle prove

Descrizione ad alto livello del processo di Information Discovery

Approccio metodologico

La metodologia presentata ha indirizzato le due aree principali su cui poggia la Computer Forensics:

- search and seizure
- information discovery.

Sebbene differenti nella modalità di condotta, entrambe condividono alcuni elementi principali:

-le prove debbono essere il più possibile salvaguardate dall'essere compromesse;

-le prove debbono essere back-upate e autenticate;

-tutte le attività debbono essere estensivamente documentate.

-Il laboratorio forense, dove verrà effettuata la fase di information discovery, gioca un ruolo fondamentale, dal momento che deve costituire un luogo "sicuro" per il deposito e l'analisi delle prove.

Approccio metodologico

Tutte le attività svolte sono finalizzate a preservare la “catena della custodia”. Infine, l’utilizzo di appropriati tool SW facilitano:

- Il mantenere un approccio strutturato;

-La gestione dei log;

-L’attività di back-up

-L’attività di analisi;

-L’attività di reportistica.

INDICE DELLA PRESENTAZIONE :

1. Introduzione
2. Scenario attuale
    1. minacce interne
    2. D.Lgs 231/2001
3. Investigazioni telematiche e internet
4. IS security Management
5. Computer forensics
6. Forensic accounting
7. Conclusioni
8. Riferimenti bibliografici e sitografici
9. Varie Q&A

Ruolo dell'auditor

- individua anomalie di comportamento
- identifica frodi nelle organizzazioni
- prende parte ai processi di gestione del rischio
- assicura il corretto funzionamento organizzativo misurandone l'efficienza, l'avanzamento tecnologico, la moralità, I rischi etc.

Forensic accounting

Oltre alle funzioni dell'auditor tradizionale, sta emergendo una nuova funzione di accounting il cui scopo è non solo quello di individuare comportamenti anomali ma anche di indagare sugli stessi: tale funzione è detta di **forensic accounting**

skills
- investigativi
- accounting
- technologici

Strumenti e metodi

I Computer Assisted Audit Tools and Techniques (CATTs) sono gli strumenti di cui devono disporre l'auditor ed il forensic accountant per indagare su attività anomale. Tra le principali funzioni:

- information retrieval and analysis
- rilevazione frodi
- audit reporting
- monitoraggio continuo

Inoltre fattori critici di successo sono:

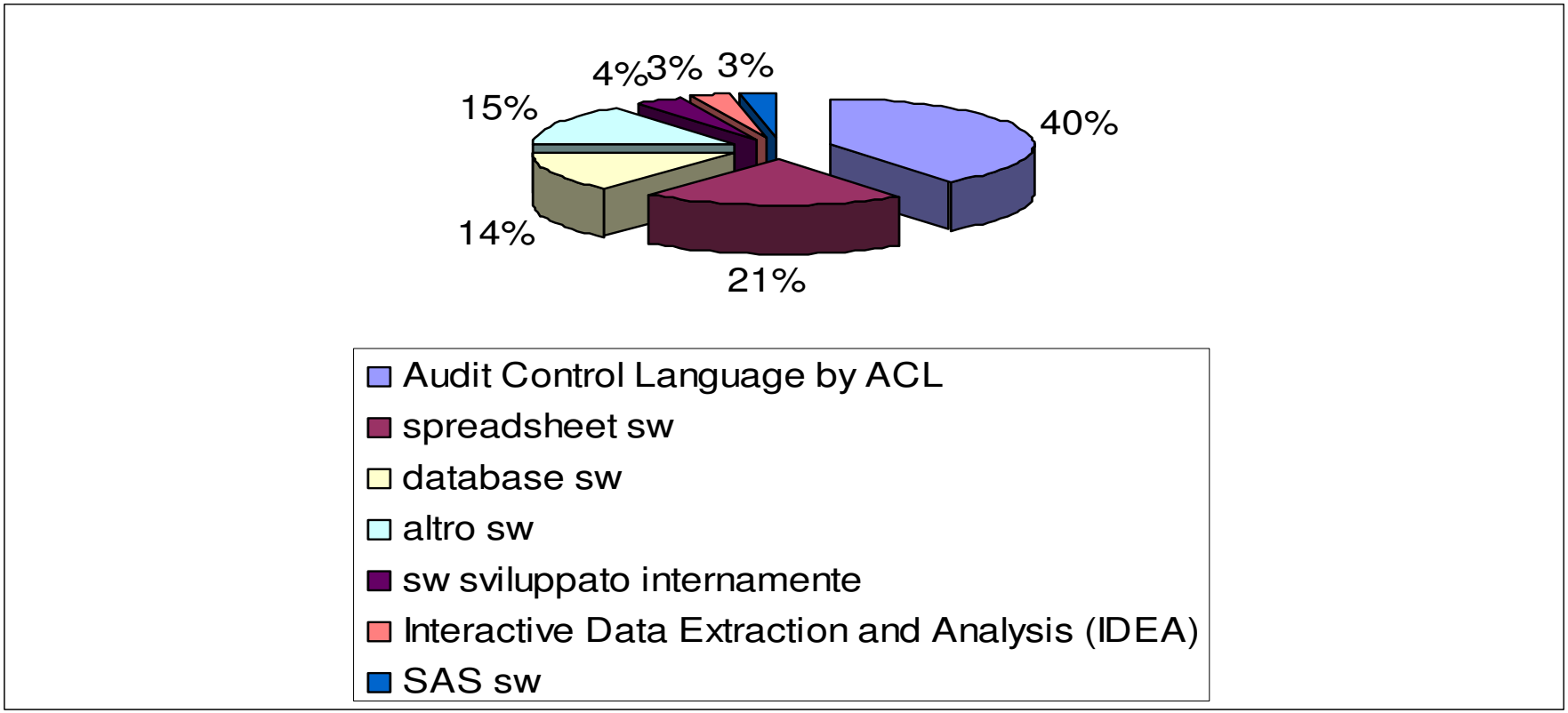
- applicazione di corrette tecniche di analisi
- l'utilizzo dei dati più appropriati
- l'abilità nell'interpretare correttamente i risultati

Tecniche di supporto

- data mining
  - analisi statistica dei dati (regressione, correlazione, dispersione,regole di associazione, etc.)
  - alberi delle decisioni
  - reti neurali
- patterns di numeri e cifre
  - analisi delle cifre (legge di Benford)
  - occorrenze cicliche
  - duplicazione numeri
  - dimensione relativa
- analisi visiva
  - link analysis
  - time-line analysis
  - clustering

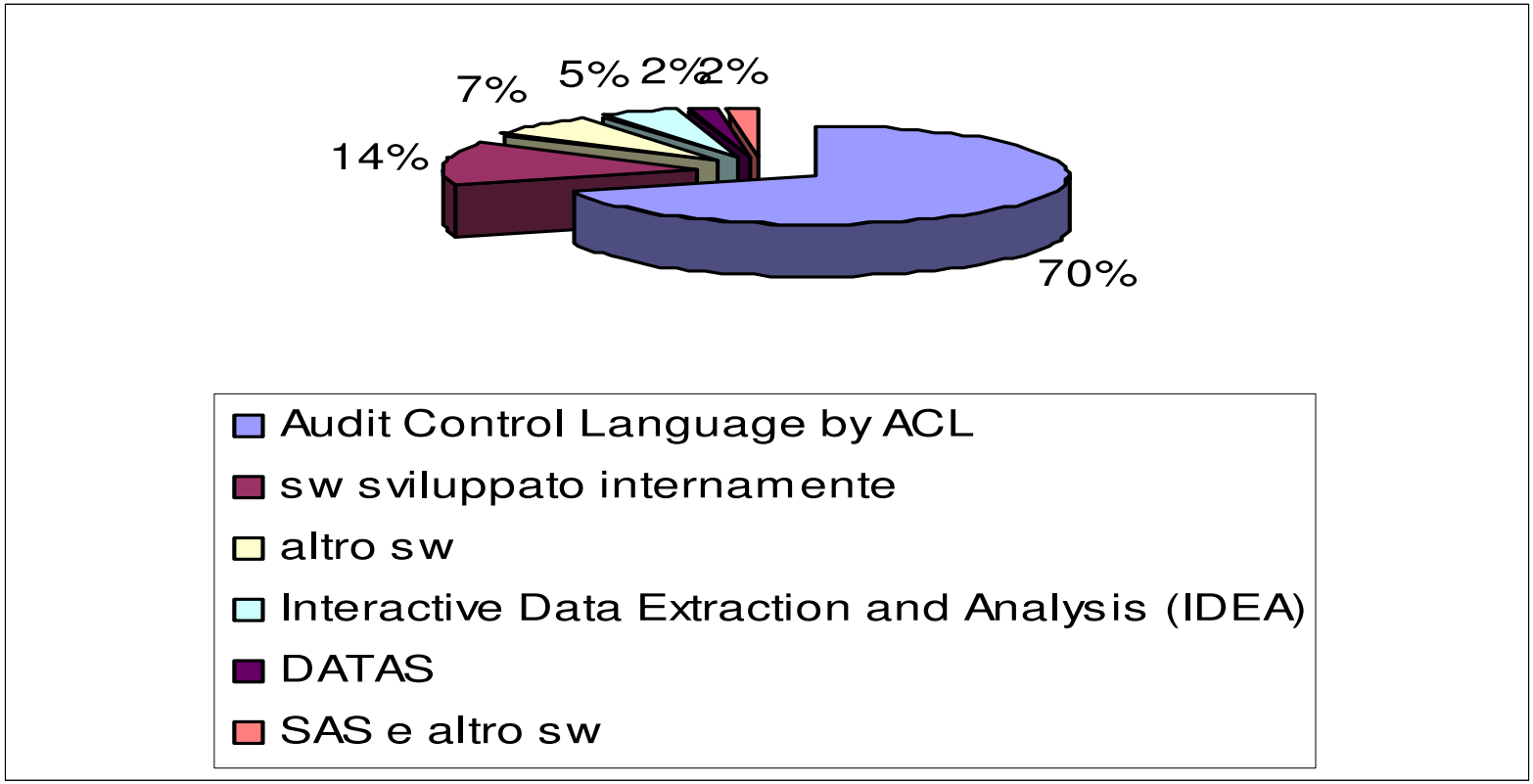
Strumenti

estrazione ed analisi dati



Strumenti

prevenzione e rilevamento frodi



Strumenti

Data mining tools

- Clementine by Integral Solutions Ltd
- Darwin by Thinking Machines
- Enterprise Miner by SAS Institute
- Intelligent Miner for Data by IBM
- Pattern Recognition Workbench by Unica Technologies Inc.

INDICE DELLA PRESENTAZIONE :

1. Introduzione
2. Scenario attuale
    1. minacce interne
    2. D.Lgs 231/2001
3. Investigazioni telematiche e internet
4. IS security Management
5. Computer forensics
6. Forensic accounting
7. Conclusioni
8. Riferimenti bibliografici e sitografici
9. Varie Q&A

Conclusioni

Futuri sviluppi di ricerca

- Forensic data mining
- test categorization
- authorship attribution
- profiling
- link analysis
- stegoforensic analysis
- criptanalysis

INDICE DELLA PRESENTAZIONE :

1. Introduzione
2. Scenario attuale
    1. minacce interne
    2. D.Lgs 231/2001
3. Investigazioni telematiche e internet
4. IS security Management
5. Computer forensics
6. Forensic accounting
7. Conclusioni
8. Riferimenti bibliografici e sitografici
9. Varie Q&A

Riferimenti bibliografici e sitografici

U.S. Department of Justice**,** Office of Justice Programs, *National Institute of Justice,*
"**Forensic Examination of Digital Evidence:A Guide for Law Enforcement**", USA, April 2004

Association of Chief Police Officers (ACPO), National High-Tech Crime Unit (NHTCU)
"**Good Practice Guide for Computer based Electronic Evidence**", UK.

CSI/FBI Computer Crime and Security Survey 2004

ACFE 2004 Report to the Nation on Occupational Fraud and Abuse

Riferimenti bibliografici e sitografici

Handbook of Computer Crime Investigation
by Eoghan Casey

Computer Forensics
by Warren G. Kruse II, Jay G. Heiser

Digital Evidence and Computer Crime
by Eoghan Casey

A Methodology for Computer Forensics Analysis
by Roberto Di Pietro and Luigi V. Mancini

INDICE DELLA PRESENTAZIONE :

1. Introduzione
2. Scenario attuale
    1. minacce interne
    2. D.Lgs 231/2001
3. Investigazioni telematiche e internet
4. IS security Management
5. Computer forensics
6. Forensic accounting
7. Conclusioni
8. Riferimenti bibliografici e sitografici
9. Varie Q&A

Varie Q&A

pspagnoletti@luiss.it

http://cersi.luiss.it