



**ANSAAF**  
Associazione Nazionale Specialisti Sicurezza  
in Aziende di Intermediazione Finanziaria

---

# SMAU 2005: Le iniziative del sistema bancario per la continuità operativa e la sicurezza delle transazioni

Ing. A. C. Wright

# Argomenti trattati

---

- La normativa della Banca d'Italia
- Cosa stanno facendo le banche:
  - L'analisi del rischio informatico
  - Una nuova organizzazione della sicurezza
  - La redazione dei piani di emergenza
- Argomento di attualità: il furto di identità

# La normativa

---

Banca d'Italia si è posta l'obiettivo di far sì che siano intraprese tutte le iniziative volte a ridurre a un livello ritenuto accettabile i danni conseguenti a incidenti settoriali e catastrofi estese che colpiscono direttamente o indirettamente l'azienda oppure sue controparti rilevanti.

# La normativa

---

Ha quindi chiesto agli operatori di sistema e agli intermediari di predisporre un **piano di continuità operativa entro il 2006.**

## **Scadenza intermedia:**

Le banche appartenenti a gruppi bancari con un attivo consolidato superiore a 5 mld.euro entro il **30.6.2005** hanno dovuto presentare il progetto per la realizzazione del piano di continuità operativa.

# La normativa

---

## Punti qualificanti:

- Responsabilizzazione dei Vertici aziendali
- Identificazione dei processi critici e relativa filiera
  - Adozione di misure preventive, di emergenza e di ripristino commisurate ai rischi
    - Indicazione di misure “minime”
    - Accettazione formale del rischio residuo
      - Nomina di un responsabile BCM
      - Instaurazione di un ciclo formale di BCM
- Sinergie fra intermediari ed operatori di sistema

# Gli scenari definiti dalla normativa

---

## Quali scenari “minimi” vanno presi in esame?

- Distruzione o inaccessibilità di **strutture** nelle quali sono allocate unità operative o apparecchiature critiche;
- Indisponibilità di **personale** essenziale per il funzionamento dell'azienda;
- Interruzione del funzionamento delle **infrastrutture**;
- Alterazione dei **dati** o indisponibilità dei **sistemi** a seguito di attacchi perpetrati dall'esterno attraverso le reti telematiche;
- **Danneggiamenti** gravi provocati da dipendenti.

# Alcuni punti d'attenzione

---

- Gli scenari da prendere in esame e il loro mutarsi nel tempo
- Una variabile da non trascurare: la possibile durata di un evento disastroso
- Pianificare tutto?
- BCM e CM: due figure diverse?
- Business Continuity, Sicurezza Logica, Sicurezza Fisica, Risk Management: convergenze parallele?
- La stesura delle procedure di emergenza è un'opportunità per la revisione dei processi di business ed operativi?
- La manutenzione dei BCP

# Il Rischio informatico: lo studio della CIPA

---

- La CIPA aveva costituito nel 2003, presso la Banca d'Italia, un gruppo di lavoro per analizzare la tematica del "*rischio informatico*"
- Il gruppo di lavoro si basò sulla concreta esperienza dei rappresentanti delle banche (BdI, ABI, Centri Applicativi e dalle maggiori banche Italiane) e con l'ausilio dei più diffusi Standard internazionali, best practices e riferimenti normativi

# Il Rischio informatico: lo studio della CIPA

---

- Obiettivo del gruppo di lavoro:
  - Contribuire alla sensibilizzazione sulle problematiche di sicurezza, con l'emanazione di un documento che principalmente rappresenti:
    - La gestione del rischio informatico
    - Le aree di rischio, le minacce e le possibili contromisure
    - Indicazioni di carattere operativo ed organizzativo per una corretta implementazione delle *policy* di sicurezza

# Il Rischio informatico: lo studio della CIPA

---

Il documento, dopo essere stato aggiornato sulla base della recente normativa, è stato reso pubblico dalla Segreteria CIPA.

E' un utile riferimento per tutte le banche.

# La struttura organizzativa per il BCM

---

- Business Continuity Management e Crisis Management sono strettamente legati.
- Il Disaster Recovery, pur essendo un'attività prevalentemente tecnologica, è strettamente legata alla B.C., e ne fa parte.
- L'analisi dei rischi, includendo l'analisi d'impatto, e la successiva individuazione delle misure da adottare per la mitigazione del rischio, richiedono peculiari esperienze, conoscenze presenti in molteplici Uffici e Direzioni.
- La formalizzazione delle responsabilità nel ciclo di Business Continuity Management è chiave per il successo.

# L'organizzazione della Sicurezza ICT

---

Si riportano qui di seguito alcuni stralci di uno studio di *benchmarking* eseguito tempo addietro da un socio.

Le principali conclusioni di detto studio:

*"La sicurezza è sempre più riconosciuta come parte integrante del business e gestita nell'insieme delle sue componenti in modo unitario a livello Corporate"*

*"La tendenza che si osserva è quella di creare una struttura di sicurezza autonoma, con responsabilità globale della sicurezza, budget proprio e riporto diretto al CEO/BoD"*

# L'organizzazione della Sicurezza ICT

---

- Il CSO/CISO riporta ancora prevalentemente al CIO, anche se si sta affermando la scelta di posizionare la sicurezza al di fuori delle strutture IT
  - CIO: 35% ca.
  - CEO/BoD: 15% ca.
  - Altri riporti del CEO (COO, CRO, CTO): 30% ca.
  - Altri: 20%
- La maggior parte delle aziende (ca. il 70%) ritiene di investire in sicurezza una cifra paragonabile a quella delle altre aziende con cui si confronta e, nell'ultimo anno, il budget dedicato alla sicurezza è cresciuto per il 65% delle aziende, attestandosi ad un valore pari a ca. il 7% di quello dell'IT

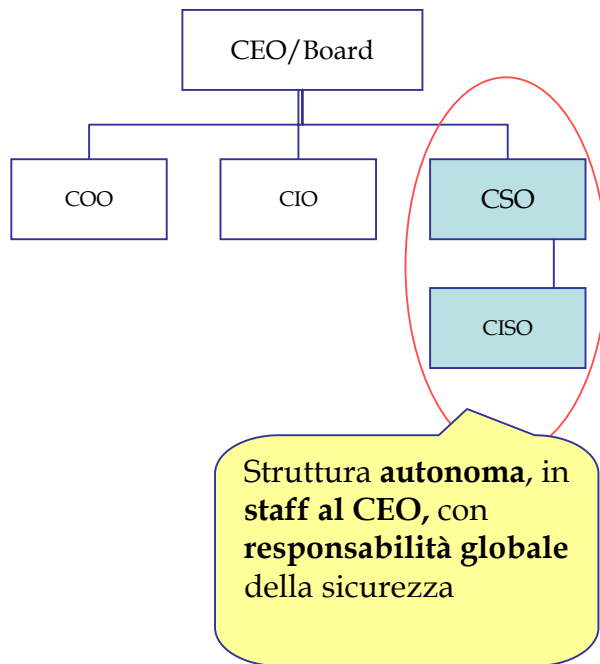
# L'organizzazione della Sicurezza ICT

---

- Il numero delle persone dedicate alla sicurezza è in rapida crescita in tutte le realtà e fra le maggiori istituzioni finanziarie il 28% di queste si avvale di uno staff superiore alle 100 unità

# Modello in diffusione

– *Referenze* –



- Swiss Bank Corporation
- HSBC
- The Royal Bank of Scotland
- Dresdner Bank
- Citigroup
- Republic National Bank New York
- Standard Chartered Bank
- Nike Inc.
- Thomson Corporation
- Hershey Foods Corporation
- Fidelity Investments
- State Street Global Advisors
- ING
- Eurobank
- Imperial Chemical Industries
- DuPont
- Google
- eBay
- ENI
- FIAT
- Pirelli

# Modello con riporto al CEO

---

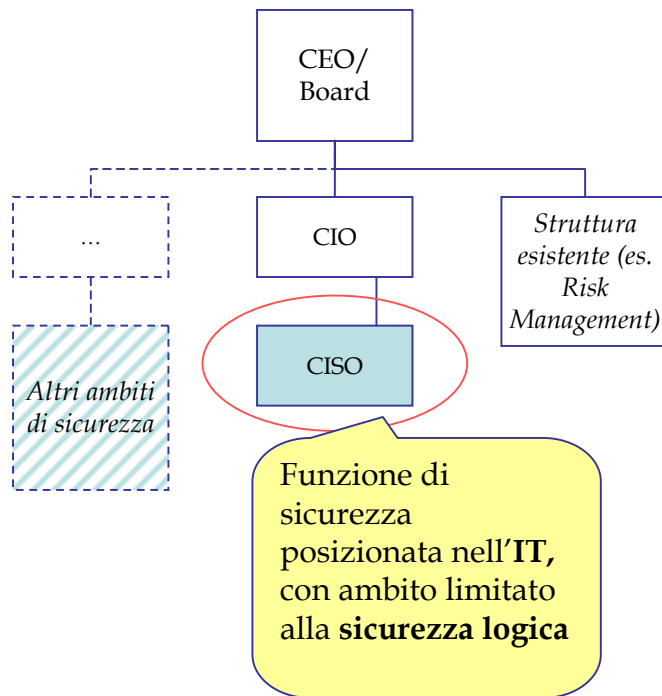
- Si osserva come tendenzialmente tutte le aziende certificate BS7799 abbiano la funzione sicurezza dipendente da un CSO, che riporta direttamente al CEO/BoD, e che tale modello organizzativo è stato adottato principalmente dalle aziende USA e UK
- Il CSO ha la responsabilità globale della sicurezza (interna, esterna, fisica, logica, personale) e di tutti i suoi aspetti (strategia, governo, controllo e implementazione)
- Il CSO ha alle sue dipendenze:
  - un CISO, che ha la responsabilità della protezione delle informazioni e da cui dipendono:
    - IT Security Manager (sicurezza informatica)
    - IT Security Architect (risponde all'IT Security Manager e si occupa della pianificazione e sviluppo delle architetture di sicurezza)
    - IT Security Incident Manager (incidenti Informatici)
  - un Physical Security Officer (PSO), che gestisce la sicurezza fisica della struttura, incluse le eventuali norme di personal safety degli impiegati

# Modello con riporto al CEO

---

- La parte investigativa, ove presente, è composta dal:
  - Capo dell'internal auditing, paritetico al CSO risponde come quest'ultimo al CEO
  - Chief Investigation Officer, che si occupa delle investigazioni interne e riporta al capo internal auditing. Il Chief Investigation Officer ha, inoltre, una serie di Senior Investigators, che si occupano di frodi/illeciti/violazioni delle politiche, anche di tipo AUP/Information Security. Si avvale dello staff di IT security per le operazioni di incident response e digital forensic

# Il modello prevalente nelle banche



## – Referenze –

- Merrill Lynch
- Bank of America
- American Express
- ABN Amro
- National Bank Of Belgium
- Crèdit Agricole
- Indosuez
  
- Banco Santander Central Hispano Americano
- Banco Bilbao Vizcaya Argentaria
- Solvay
- Carnival Group
- *Maggioranza Banche italiane*

# Quale futuro?

---

Continueremo ad avere una separazione fra le diverse "Sicurezze" e la Business Continuity?

Avremo un modello "centralizzato" o "decentrato"?

# La protezione delle transazioni

---

Tra gli scenari “minimi” della normativa della Banca d’Italia sono ampiamente sottolineati quelli relativi agli attacchi dall’esterno e dall’interno dell’Azienda (virus, hackers, ecc.).

Parliamo ora molto brevemente di alcune tipologie di attacco agli intermediari finanziari, tralasciando, per questa volta, di parlare di virus per brevità di esposizione: ciò anche se ci sarebbe da domandarsi perché non ci sono più danni così elevati come in passato provocati dai virus. Tutti più bravi?

Parlerò del furto d’identità, tema molto attuale in questi giorni.

# Quali tipologie di furti d'identità

---

1. Uso fraudolento dei codici (esempi: carta carbone; skimming; phishing; trojan; ecc.)
2. Uso fraudolento dell'identità
3. Creazione di una nuova identità

# Quali tipologie di furti d'identità

---

Un esempio.

Lo skimming.

# Sembra un ATM "normale"...



---

# Ma non è così!



# ..e la telecamera? Dov'è?

Queste informazioni si possono trovare sul sito:  
<http://www.snopes.com/crime/warnings/atmcamera.asp>



# Il Cliente è protetto? Come?

---

Tutte le Aziende adottano sistemi sempre più sofisticati per proteggere i loro Clienti. Ad esempio, i prelievamenti Bancomat vengono protetti con nuova tecnologia (smart card, algoritmo decifrazione più sofisticato; ecc.)

La sfida è sulla prevenzione, ma la lotta è molto dura: ad ogni nuova misura protettiva, corrisponde una nuova invenzione da parte dei criminali.

Occorre quindi anche la collaborazione di tutti, inclusi i Clienti.

# Alcuni consigli ai Clienti

(che è bene ripetere sempre!)

---

- Non dare informazioni riservate agli sconosciuti;
- Non fidarsi di chi telefona a casa chiedendo il numero del conto o della carta di credito;
- Guardare chi sta alle spalle mentre si acquista (attenti anche al portafoglio!);
- Non spedire via posta assegni circolari o dati riservati;
- Non lasciare la posta nella cassetta per più giorni;
- preoccuparsi se non arriva alla solita data una comunicazione con dati riservati (es:estratto conto);
- Fare attenzione a cosa si getta nella spazzatura;

# Alcuni consigli...

---

- ... insospettirsi se vi sono dei cambiamenti, non immediatamente giustificabili, in mezzi e strumenti abitualmente usati (es: nel cash dispenser; nel modo di comunicare della banca; ecc.);
- Usare password non facili da indovinare;
- Aggiornare il sistema operativo del computer ogni qual volta viene messa a disposizione una "patch" dal fornitore;
- Installare, e mantenere aggiornati, un sistema antivirus e, possibilmente, un personal firewall;
- Fornire informazioni on-line solo a siti sicuri e a intermediari finanziari che offrano sistemi di accesso sicuro...

# ANSSAIF

---

*Associazione Nazionale degli Specialisti di Sicurezza  
in Aziende di Intermediazione Finanziaria.*

Associazione senza scopo di lucro.

Soci ordinari e fondatori sono funzionari e dirigenti dei  
maggiori gruppi bancari.

Fra i soci sostenitori: ABI, CLUSIT, ICAA, AIEA, BassNet, BMC  
Software, EDS, Ernst&Young, IBM, KPMG, ONESIS,  
Siemens Informatica, Symantec, VP-Tech.

# ANSSAIF

---

L'Associazione è stata costituita per perseguire i seguenti obiettivi:

- 1) contribuire alla maturazione, in tutte le sedi opportune, anche universitarie, della consapevolezza dei problemi connessi alla necessaria protezione dei beni informatici, dei dati e delle informazioni, per garantirne la riservatezza, l'integrità e la disponibilità;
- 2) promuovere studi e ricerche nel campo della sicurezza ICT, curando altresì di individuare processi e momenti di integrazione della sicurezza logica e di quella fisica;
- 3) conservare il patrimonio di esperienze professionali degli specialisti di sicurezza del settore, anche al termine della loro attività lavorativa;
- 4) curare la condivisione di esperienze e conoscenze atte a migliorare l'attività professionale degli associati;

# ANSSAIF

---

- 5) curare la promozione culturale e l'aggiornamento dei soci;
- 6) concorrere alla formazione di giovani specialisti;
- 7) fornire informazioni sulla regolamentazione in ordine a tutti gli aspetti concernenti gli obblighi delle Aziende e dei Responsabili della sicurezza nei confronti delle norme.

[www.anssaif.it](http://www.anssaif.it)

# The End

---

Grazie per l'attenzione.