

Information Security Governance ed incidenti informatici

Gerardo Costabile



“Il vero viaggio di scoperta non consiste
nello scoprire nuove terre ma nell’aver
nuovi occhi.”

M. Proust



Gerardo Costabile
Gruppo Poste Italiane
Security & Safety
Responsabile Sicurezza Logica

Member of “The International Association of Computer Investigative Specialists”

Member of “Antiphishing Working Group”

Socio Onorario dell’Associazione Informatici Professionisti

HTTC Member

Presidente IISFA Italian Chapter www.iisfa.it

C.I.F.I. - Certified Information Forensics Investigator



GRUPPO POSTE ITALIANE

Alcuni dati:

- 155.000 dipendenti
- 14.000 uffici postali
- 2.700 ATM
- 90 MLD di euro in contanti movimentati



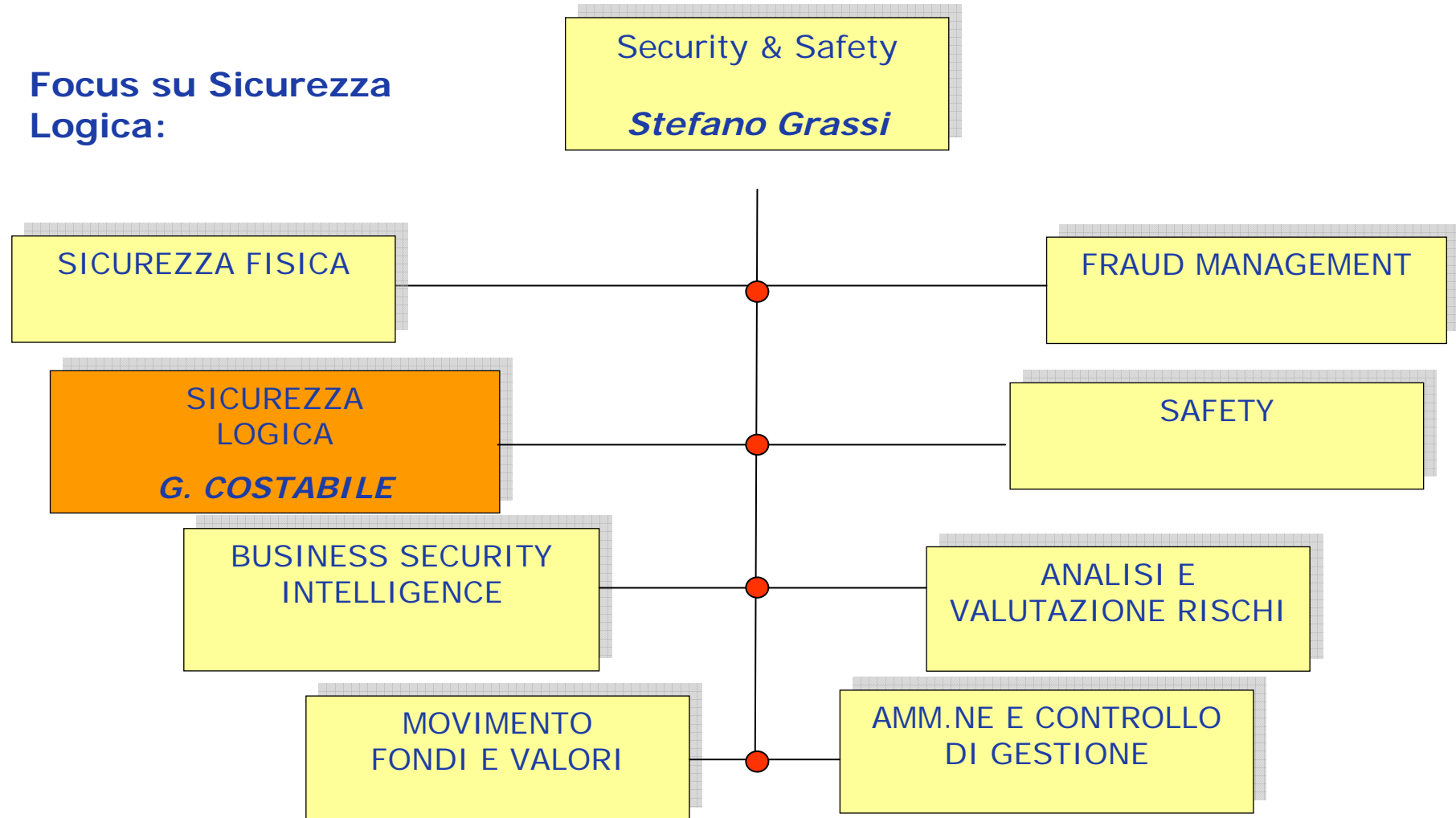
- 38.000 POS
- 17 collegamenti aerei al giorno
- 40.000 veicoli
- 30.000 motoveicoli
- 11 MLN di clienti

RILEVANZA DELLA SICUREZZA PER POSTE ITALIANE

- La tutela del patrimonio materiale e immateriale sono un valore imprescindibile per una società così esposta ai rischi come Poste Italiane
- Occorre, quindi, assicurare adeguati livelli di sicurezza nei diversi ambiti di applicazione (Fisica, Logica e Organizzativa).

Poste Italiane Security & Safety

Focus su Sicurezza
Logica:



Che cosa è IISFA?

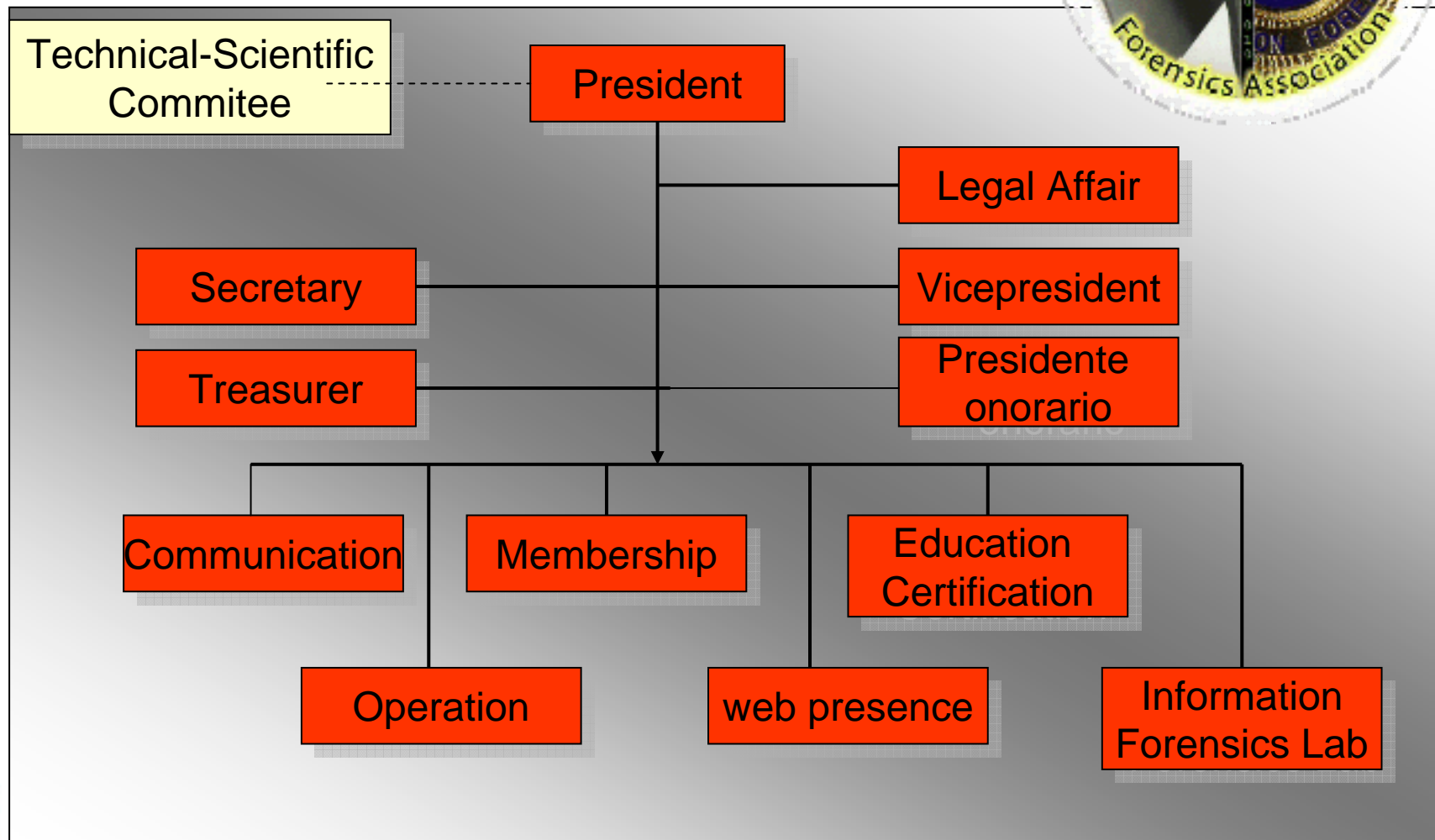
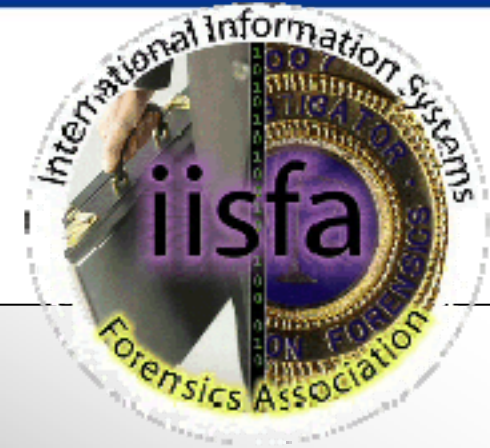


L'International Information Systems Forensics Association (IISFA) è un'organizzazione senza scopo di lucro con la missione di promuovere la disciplina dell'information forensics attraverso la divulgazione, l'apprendimento e la certificazione.

www.iisfa.it

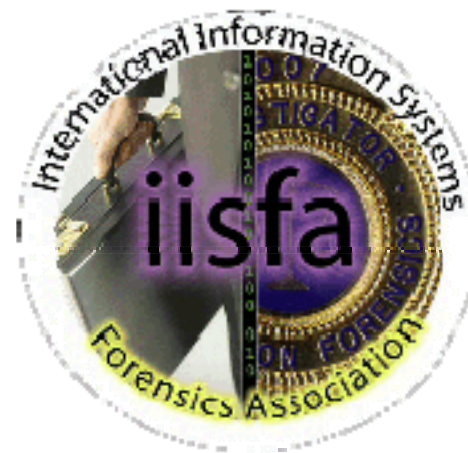


Board of directors IISFA

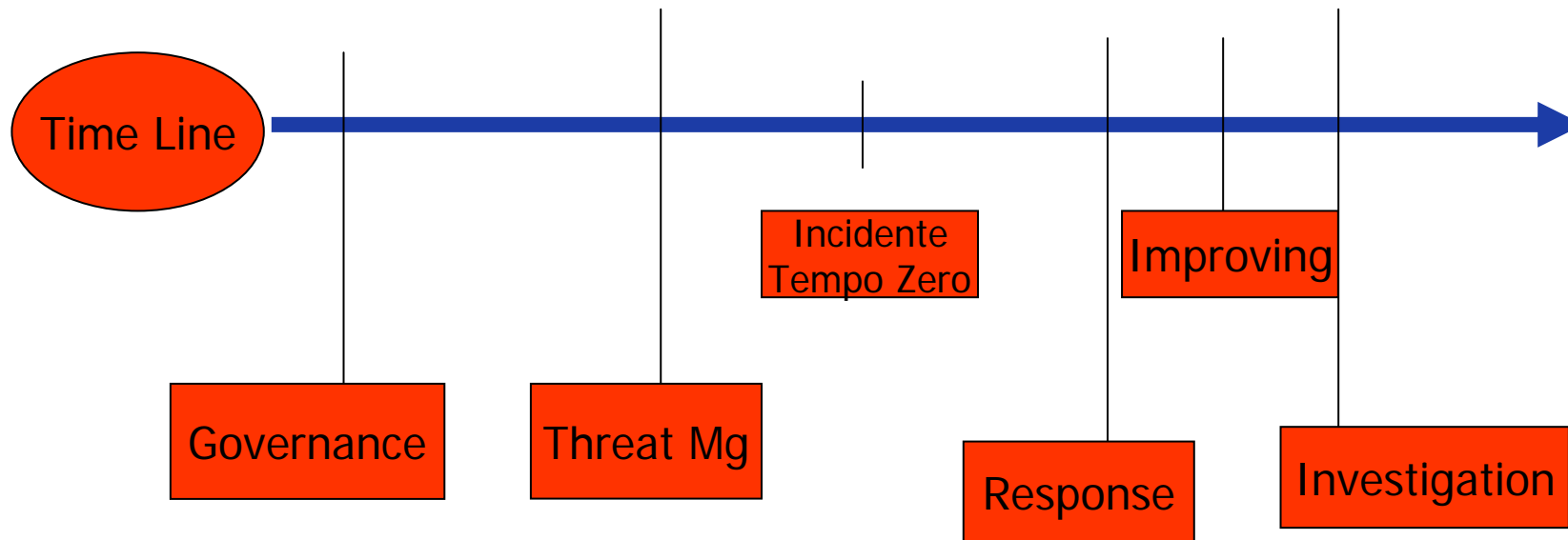


La certificazione CIFI

- ▶ Certified Information Forensics Investigator
 - Identifica il meglio nella professione di information forensics investigator.
 - E' sviluppata in modo specifico per coloro che hanno esperienze in ambito investigativo, corporate o law enforcement .
 - Il professionista CIFI dimostra di possedere esperienza su tutto il processo investigativo e rende riconoscibile la propria professionalità attraverso una certificazione riconosciuta a livello internazionale.
- ▶ Certificazione Industry independent
- ▶ Relativa a 6 aree di conoscenza (Common Bodies of Knowledge)
 - Auditing
 - Incident Response
 - Law and Investigation
 - Tools and Techniques
 - Traceback
 - Countermeasures
- ▶ Richiede di aderire ad uno specifico codice etico



Una parte del processo in Azienda....



In Azienda...

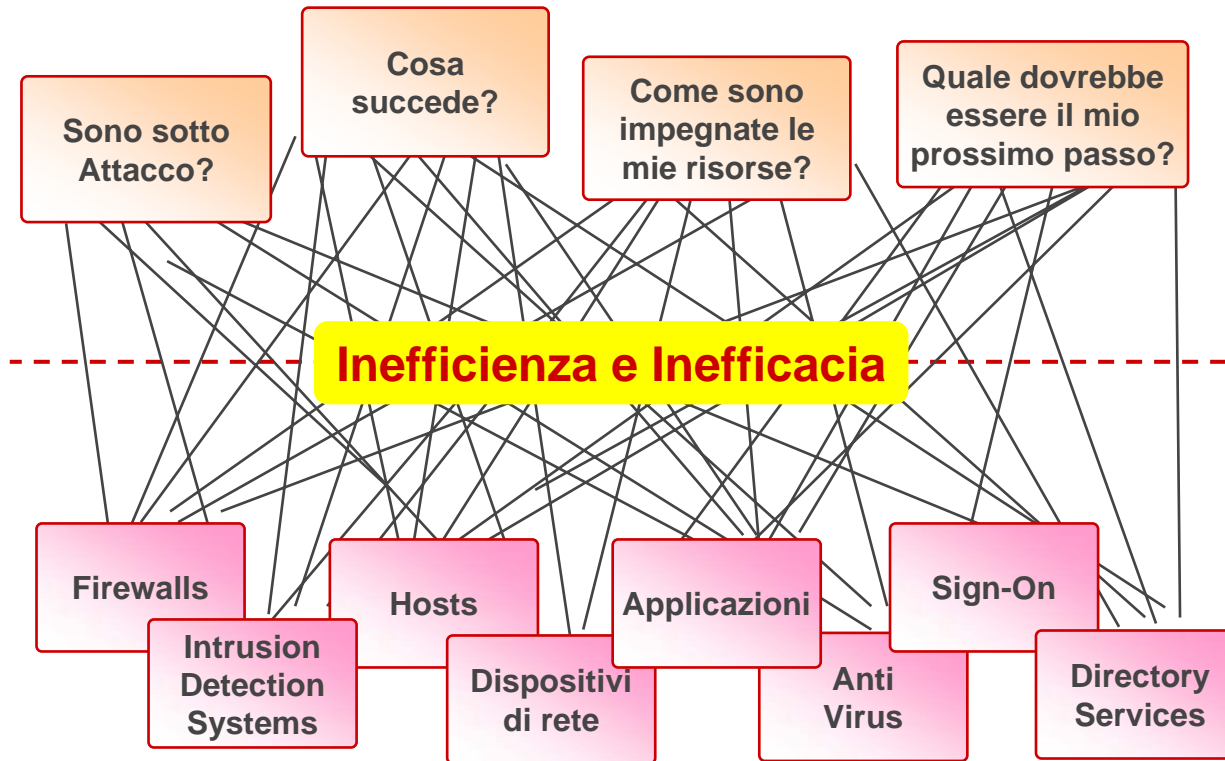
Information Forensics, Security Event & Incident Management

- Un prodotto SIM (Security Information Management) consente la gestione degli eventi di sicurezza che una azienda di grandi dimensioni produce:
- **Normalizza e Aggrega** gli eventi provenienti da tecnologie diverse e multivendor
- **Correla e Presenta** gli eventi raccolti per analisi real-time o la gestione di incidenti



Esigenze

Gestione non centralizzata



Infrastruttura di prodotti indipendenti

Impossibilità di individuare i rischi

Diversi attori coinvolti:

- Security monitors
- Analisti di Sicurezza
- Security managers
- Corporate management
- Auditors

Necessario per la gestione della sicurezza multilivello

Prodotti multi-vendor scelti tra i "best in class"

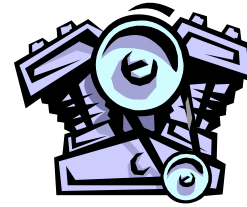
Ottimi prodotti ma che non sono in grado di interagire tra loro



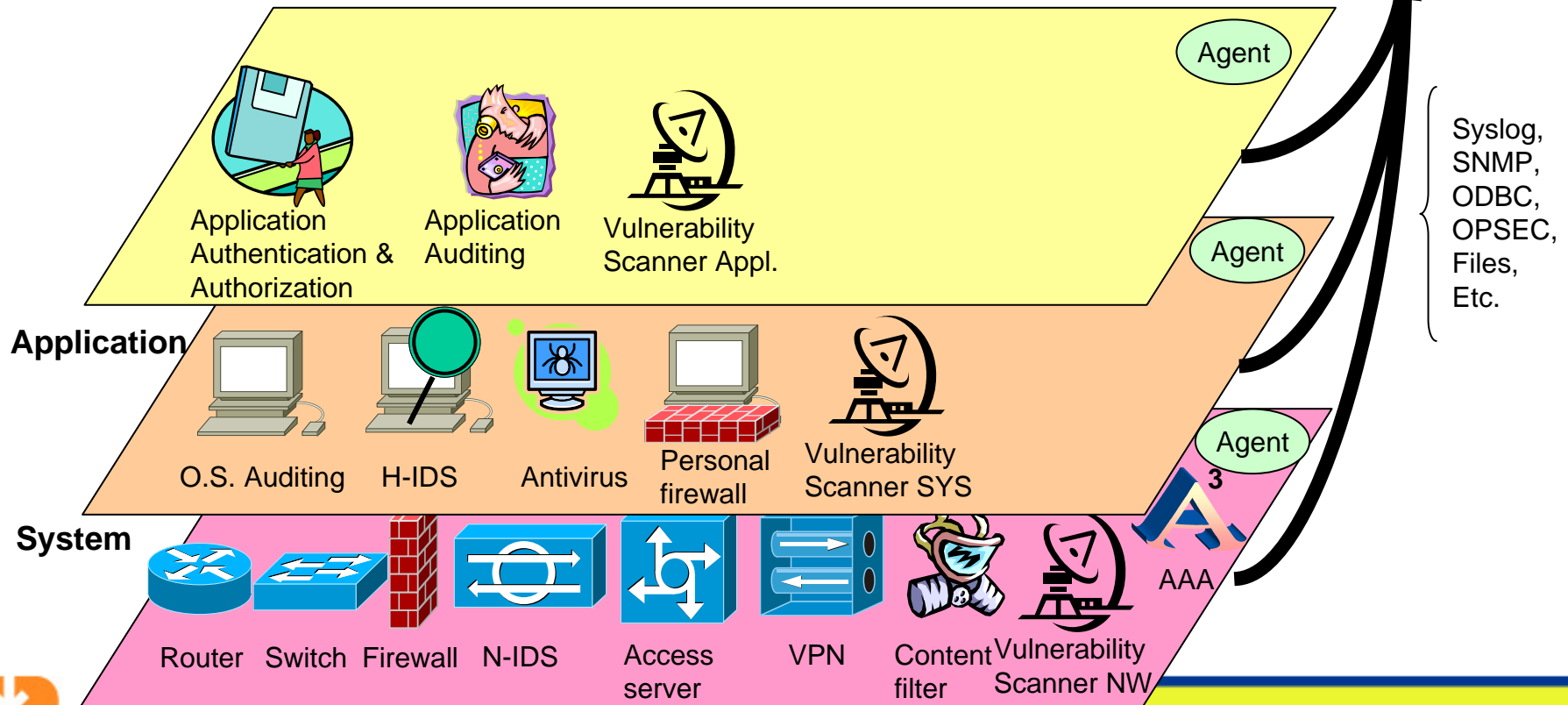
SEM Componente Core

SEM e
Fonti dati

SEM Componente di Raccolta



Fonti dati: layers



Network

Correlazione....

- ▶ **Vulnerability Correlation:** attraverso l'analisi e la correlazione delle informazioni provenienti dai dispositivi di Intrusion Detection è possibile determinare l'effettiva pericolosità di un attacco eliminando i falsi positivi o innalzando la priorità di eventi effettivamente pericolosi. Le informazioni raccolte dai Vulnerability Scanner possono andare a popolare il valore di *Esposizione* degli asset definiti.
- ▶ **Correlazione Rule Based:** la correlazione basata su regole, detta anche *scenario based*, consente di definire degli scenari di attacco, e ne permette la verifica real-time. Qualora si verificasse la sequenza di eventi prevista ed implementata attraverso opportune regole, vengono generati uno più nuovi eventi che denunciano in manifestarsi del relativo incidente.

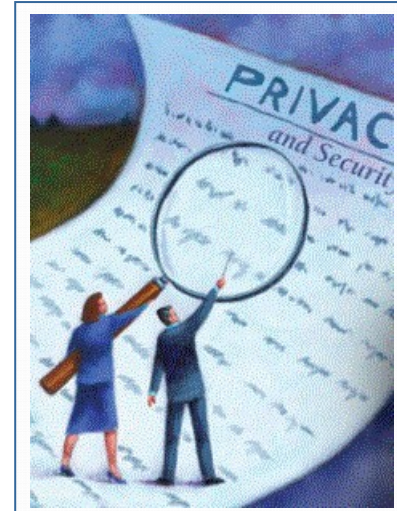


Ma....

- ▶ Incident Handling
- ▶ Policy
- ▶ Segregation of duty
- ▶ Etc.....



Necessità di un modello per affrontare e gestire i rischi di violazione alla Sicurezza delle Informazioni in azienda.

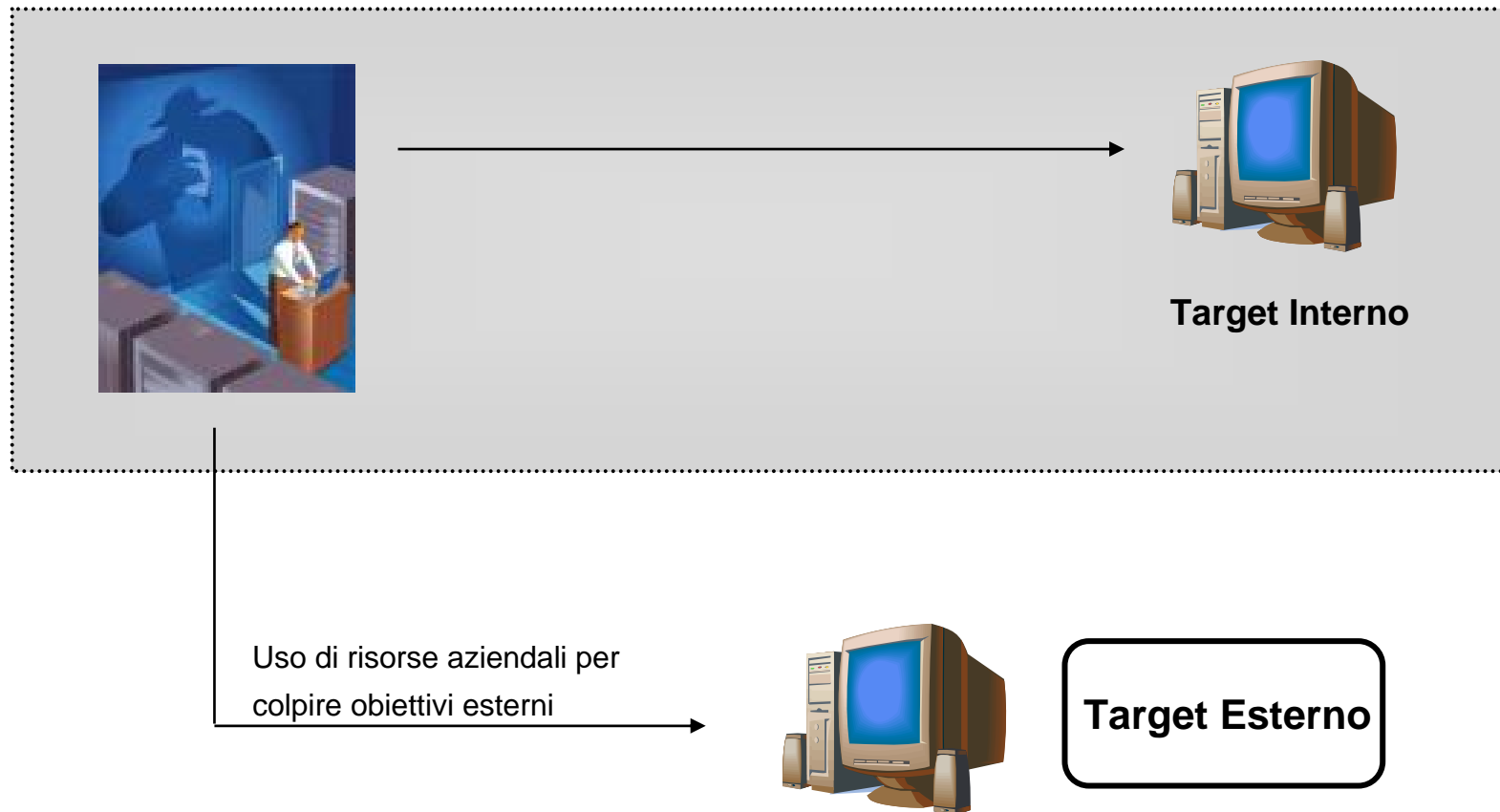


Dall'analisi delle possibili violazioni perpetrabili (ad esempio, ma non solo, dai c.d. insider) dovrebbero essere definite una serie di contromisure organizzative-tecnologiche per la difesa delle informazioni critiche aziendali.

Tali contromisure potranno fornire inoltre una serie di evidenze utilizzabili dalle Forze dell'Ordine per l'individuazione delle responsabilità



Obiettivo dell'attacco dell'insider



Istruzioni al personale per l'uso corretto dei sistemi informativi

- ▶ Le Istruzioni al personale definiscono le regole per l'accesso, l'utilizzo e la protezione delle risorse informative da parte del personale aziendale onde ridurre al minimo i rischi di indisponibilità, accesso non autorizzato, distruzione o perdita anche accidentale delle stesse.
- ▶ Vengono inoltre definite le responsabilità e le conseguenze in caso di mancato rispetto delle regole.
- ▶ A tali regole sono soggetti anche i consulenti appartenenti ad imprese esterne che, per finalità lavorative, accedono ed utilizzano le risorse informative dell'Azienda.



Istruzioni al personale per l'uso corretto dei sistemi informativi

Posta Elettronica

- ▶ Ogni casella di posta è generalmente nominativa ed univocamente assegnata ad una persona fisica, quindi "personale", pertanto ogni utente è direttamente responsabile, disciplinarmente e giuridicamente, del suo utilizzo e del contenuto dei messaggi inviati.
- ▶ La casella di posta, pur se assegnata personalmente, non è da considerarsi privata ma aziendale poiché costituisce semplicemente uno strumento di lavoro messo a disposizione dall'Azienda per svolgere le attività legate alle mansioni assegnate.



Istruzioni al personale per l'uso corretto dei sistemi informativi


Internet

- ▶ L'Azienda fornisce, limitatamente alle strutture che ne hanno necessità, l'accesso alla rete internet tramite le postazioni di lavoro di propria competenza.
- ▶ E' possibile in tal senso accedere ad internet tramite l'intranet aziendale.
- ▶ L'utente deve farne uso secondo il criterio di ragionevolezza e professionalità.
- ▶ L'utilizzo di internet è consentito soltanto per scopi leciti e legati alle attività lavorative



Istruzioni al personale per l'uso corretto dei sistemi informativi

Internet

- ▶ L'utente è tenuto al rispetto delle norme d'uso ed è ritenuto, disciplinarmente e giuridicamente, responsabile per danni arrecati attraverso l'uso privato, improprio o illecito della connessione ad internet.
- ▶ L'Azienda non potrà essere considerata dal dipendente responsabile di danni da lui ricevuti nel caso di uso privato, improprio o illecito del servizio.
- ▶ L'Azienda si riserva la facoltà di disporre controlli specifici ed agire disciplinarmente e/o giuridicamente nei casi di utilizzo  at0, improprio o illecito del servizio.



Data Classification e Policy sulla sensibilità delle informazioni

Data Classification

- ▶ Al fine di proteggere adeguatamente il patrimonio informativo aziendale, è necessario procedere alla definizione di una policy sulla sensibilità delle informazioni e di una metodologia di classificazione dei dati che tenga conto della loro criticità in termini di riservatezza, integrità e disponibilità (RID).
- ▶ La metodologia di classificazione definita costituirà il punto di partenza per la strutturazione del processo aziendale di assegnazione e gestione dei profili autorizzativi per gli utenti.



Data Classification e Policy sulla sensibilità delle informazioni

Policy di Sensibilità delle Informazioni

Indirizza la gestione delle informazioni trattate dall'azienda, al fine di proteggere le stesse a prescindere dall'origine, dal supporto o dalla fase di elaborazione.

Tale policy deve contenere:

- ▶ Il dettaglio del processo di classificazione, riclassificazione e declassificazione delle informazioni.
- ▶ La definizione di ruoli e responsabilità inerenti il processo di classificazione di sicurezza, gestito da una struttura interna dell'Azienda.



Data Classification e Policy sulla sensibilità delle informazioni

Policy di Sensibilità delle Informazioni

- ▶ La mappa e la definizione degli asset informativi che devono essere censiti con i relativi Data-Owner (registro delle informazioni classificate).
- ▶ I principi di conservazione e distruzione delle informazioni.
- ▶ L'aggiornamento di tutto il framework documentale a supporto del processo.
- ▶ Il modello delle classi di sicurezza.
- ▶ Le contromisure di sicurezza associate alle etichette di classificazione.



Controlli difensivi

I controlli difensivi sono quei controlli che si rendono necessari (e quindi giustificati e legittimi) per garantire la tutela del patrimonio aziendale.

Attraverso tali controlli è possibile prevenire gli illeciti o nel caso in cui questi siano già stati compiuti, individuarne gli autori.

Principi Normativi

- Impianti audiovisivi art. 4 L.300/70 (Statuto dei lavoratori).
- D.Lgs. n. 196/03.
- Art. 616 c.p.: violazione, sottrazione, soppressione di corrispondenza.

Sentenza Cass. pen. 8 ottobre 1985

“E’ legittimo il controllo del datore di lavoro sul dipendente infedele che si renda autore di un comportamento illecito e contrario ai suoi doveri, che esuli dalla specifica attività dello stesso, perché realizza un attentato al patrimonio dell’azienda, con la conseguente cessazione da parte del titolare dell’impresa dell’osservanza dell’obbligo di ottemperare ai precetti normativamente previsti”



Sentenza Cass. 16 settembre 1997 n.9211

“L’installazione in azienda, da parte del datore di lavoro, di impianti audiovisivi è assoggettata ai limiti previsti dall’art. 4 dello Statuto dei Lavoratori anche se da essi derivi solo una mera potenzialità di controllo a distanza sull’attività lavorativa dei dipendenti, senza che peraltro rilevi il fatto che i dipendenti siano a conoscenza dell’esistenza di tali impianti. “



Controlli difensivi

Sentenza Cass. sez. lav., n. 4746/2002

“Ai fini dell’operatività del divieto di apparecchiature per il controllo a distanza dei lavoratori previsto dall’articolo 4 della l. n. 300 del 1970 (Statuto dei Lavoratori) è necessario che il controllo riguardi l’attività lavorativa, mentre devono ritenersi certamente fuori dall’ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore, quali ad esempio i sistemi di controllo degli accessi ad aree riservate, o, appunto gli apparecchi di rilevazione delle telefonate ingiustificate. ”



Tribunale Milano 31 marzo 2004

“Il divieto del controllo a distanza dell’attività dei lavoratori posto dall’art. 4 S. L. non si estende ai cosiddetti controlli difensivi, i quali, peraltro, non costituiscono una categoria a sé esentata, a priori, dall’applicabilità delle previsioni dell’art. 4, ma semplicemente un modo per definire controlli finalizzati all’accertamento di condotte illecite del lavoratore che non rientrano nell’ambito di applicazione del divieto perché non comportano la raccolta anche di notizie relative all’attività lavorativa. ”



Monitoraggio della sicurezza

- ▶ Le registrazioni delle operazioni effettuate (ad esempio i file di log) inerenti le attività degli utenti e gli eventi che possono compromettere la sicurezza delle risorse informative devono essere tracciati, memorizzati e conservati per un periodo di tempo ritenuto idoneo (anche in conformità alle normative vigenti) a supportare future attività di accertamento e “gestione degli incidenti”.
- ▶ Devono essere definite procedure per il monitoraggio e il successivo accertamento del corretto utilizzo degli strumenti di elaborazione delle informazioni.



Monitoraggio della sicurezza

- ▶ Gli strumenti di monitoraggio devono essere protetti contro i rischi di accesso non autorizzato e/o di alterazione.
- ▶ Tutte le attività effettuate dall'amministratore di sistema e dall'operatore di sistema devono essere tracciate.
- ▶ I guasti ed i malfunzionamenti devono essere tracciati ed analizzati e devono essere intraprese opportune azioni correttive



Incidenti informatici e graduazione dei controlli

I controlli devono essere effettuati attraverso una formale procedura volta all'identificazione fisica dell'autore dell'illecito solo dopo aver effettuato:

- ▶ Analisi aggregate del traffico di rete rivolte a specifici servizi (ad esempio utilizzo della posta elettronica, accessi internet, log di piattaforme di sicurezza infrastrutturale).
- ▶ Emissione di comunicazioni di carattere generale relative ad un utilizzo anomalo degli strumenti aziendali e l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite.
- ▶ Ripetizione delle analisi all'interno di singole aree aziendali ed emanazione di ulteriori comunicazioni.
- ▶ Ulteriore analisi anonima e conseguente controllo individualizzato in caso di permanenza della situazione non conforme.



Provvedimento Garante		Azienda
Modalità di utilizzo Posta elettronica e della rete Internet	Devono essere indicate le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli	<ul style="list-style-type: none"> • Information Security Policy • Istruzioni al personale per l'uso corretto dei sistemi informativi
L'adozione e la pubblicità di un disciplinare interno		<ul style="list-style-type: none"> • Istruzioni al personale per l'uso corretto dei sistemi informativi: <ul style="list-style-type: none"> -Distribuzione (anche tramite mail) -Pubblicazione sulla Intranet aziendale
Adozione di misure di tipo organizzativo	Attenta valutazione dell'impatto sui diritti dei lavoratori	<ul style="list-style-type: none"> • Istituzione di un Gruppo di lavoro interfunzionale composto da rappresentanti di Risorse Umane, Affari Legali, Sicurezza Aziendale, Servizi Informatici
	Individuazione preventiva (anche per tipologie) dei lavoratori a cui è accordato l'utilizzo della posta elettronica e dell'accesso a Internet;	<ul style="list-style-type: none"> • Information Security Policy • Istruzioni al personale per l'uso corretto dei sistemi informativi
	Individuazione delle ubicazioni riservate alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;	



Provvedimento Garante		Azienda
Adozione di misure di tipo organizzativo rispetto alla "navigazione" in Internet	L'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa	<ul style="list-style-type: none"> • Istruzioni al Personale • Procedura Operativa • Utilizzo di applicativi di URL filtering basati su database
	La configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni	
	Il trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;	<ul style="list-style-type: none"> • Procedura Operativa • Conservazione dei log sull'utilizzo della navigazione internet su base dati separate non direttamente correlate con le anagrafiche dipendenti
	L'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;	<ul style="list-style-type: none"> • Security Policy Data Retention
	La graduazione dei controlli	<ul style="list-style-type: none"> • Information Security Policy • Procedura Operativa - Monitoraggio corretto utilizzo Risorse Informative



Provvedimento Garante		Azienda
Adozione di misure di tipo organizzativo rispetto all'utilizzo della posta elettronica	La messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali	<ul style="list-style-type: none"> • Information Security Policy. • Creazione di indirizzi di posta elettronica impersonali
	L'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;	<ul style="list-style-type: none"> • Dato l'elevato costo per l'azienda potrebbe essere concesso come benefit aziendale per particolari tipologie di utenti (anche con canone annuo/mensile come per il cellulare aziendale) • Necessità, in caso positivo, di aggiornare le information security policy
	La messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;	<ul style="list-style-type: none"> • Istruzioni al personale per l'uso corretto dei sistemi informativi. • Utilizzo di client di posta che permettano le funzionalità previste dal provvedimento (ad esempio Microsoft Outlook)



Provvedimento Garante		Azienda
Adozione di misure di tipo organizzativo rispetto all'utilizzo della posta elettronica	Consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.	<ul style="list-style-type: none"> • Istruzioni al personale per l'uso corretto dei sistemi informativi (ad esempio è già tecnicamente possibile con exchange e outlook).
	L'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;	<ul style="list-style-type: none"> • Implementazione di un apposito disclaimer all'interno dei messaggi di posta elettronica
	La graduazione dei controlli	<ul style="list-style-type: none"> • Information Security Policy. • Procedura Operativa - Monitoraggio corretto utilizzo Risorse Informative



Principi sempre validi...

Documento del gruppo di lavoro composto da rappresentanti delle autorità competenti per la protezione dei dati nei diversi Stati membri istituito presso la Commissione europea (ex art. 29 Direttiva 95/46/CE) riguardante la vigilanza ed i controlli sulle comunicazioni elettroniche effettuate dal posto di lavoro

Il rispetto dei seguenti principi è indispensabile perché qualsiasi attività di controllo sulle comunicazioni elettroniche effettuate sul posto di lavoro risulti legittima e giustificata.

- Principio di necessità
- Principio di finalità
- Principio di trasparenza
- Principio di legittimità
- Principio di proporzionalità
- Accuratezza e conservazione dei dati
- Sicurezza



Grazie per l'attenzione.....

Gerardo Costabile

