

MASTERCOURSE

SECURITY MANAGER

Tutto sulle Responsabilità, le Competenze
e le Soluzioni oggi più efficaci

5 giorni di corso intensivo per conoscere

- ◆ La **funzione "Security"** in azienda e i suoi **compiti**
- ◆ I **costi** e il **budget** della Security
- ◆ Prevenzione degli **illeciti** dei **dipendenti** e altre forme di criminalità verso l'azienda
- ◆ **Intelligence, investigazione aziendale** e strumenti per contrastare illeciti e frodi
- ◆ La protezione dei dati alla luce del nuovo **Codice sulla Privacy**
- ◆ Il processo di **Risk Management** e gli strumenti di gestione del rischio
- ◆ **Sicurezza Informatica** e Telecomunicazioni
- ◆ Le nuove tecnologie di **sicurezza fisica** ed **elettronica**:
antintrusione, Tvcc, incendio, controllo accessi e tecniche biometriche

8 / 12 Novembre 2004

7 / 11 Marzo 2005

Milano, Hotel Hilton



Istituto Internazionale di Ricerca
Know how to achieve



Trasmettere a:

- > Security Manager
- > Resp. Sicurezza Informatica
- > Internal Auditor

8.45 Registrazione (1° giorno)

9.00 Inizio dei lavori

11.00 Coffee Break

13.00 Pranzo

15.45 Tea Break

17.30 Chiusura dei lavori

1° giorno

La FUNZIONE SECURITY

Qual è oggi il ruolo del Security Manager: responsabilità, obblighi ed evoluzione della figura

- Quali sono le funzione del Security Manager
- Quali sono i principali requirements di sicurezza in rapporto alle strategie aziendali
- Quali caratteristiche deve avere questa figura professionale, tra le più ricercate del momento
- Quali iniziative adottare per diffondere una cultura Security in azienda
- Come comunicare all'interno dell'azienda e con il management su aspetti di sicurezza
- Qual è la collocazione del Security Manager nell'organigramma e come si relaziona con le altre funzioni aziendali, in particolare con il responsabile dell'Information Technology e con il Facility Manager
- Come valutare i risultati in relazione agli obiettivi assegnati

Come sono cambiate le priorità nella gestione della security

- In che misura le complessità degli scenari hanno influenzato gli attuali lineamenti funzionali
- La norma UNI 10459: funzioni e profilo del professionista della Security aziendale

Come sensibilizzare il management aziendale dell'importanza della funzione

Francesco Giannoccaro
Sr. Security & Privacy Consultant
Roberto Cosa
Security Manager **DE AGOSTINI**

L'organizzazione di security nel sistema azienda

- Modelli organizzativi della security: la sicurezza in un'azienda TLC, peculiarità e obblighi
- Le risorse necessarie per la security
- Il budget e i costi della security
- La comunicazione della security per il miglioramento generale del sistema

Giuseppe Femia
Security Manager
VODAFONE ITALIA
Vicepresidente
AIPSA

Quando e come ricorrere ad un importante strumento di security: l'intelligence per contrastare le frodi, tutelare la capacità competitiva e prevenire gli illeciti aziendali

- L'investigazione a supporto delle azioni legali, civile e penali
 - *Fraud auditing, Investigative Due Diligence e Computer forensic*
- Intelligence aziendale e vantaggio competitivo:
 - *Competitive Intelligence, Cloaking methods, Sistemi di Early warning e Procedure aziendali relative a ciclo attivo e passivo*
- Security Intelligence:
 - *Misure preventive di tutela delle risorse umane e del contesto aziendale, Check up organizzativo*
- Responsabilità societaria ed etica aziendale:
 - *Bilancio sociale, Monitoraggio con benchmarks esterni, Codici etici e Compliance Program*

Sabrina Vai, Amministratrice Unica, **ETHIX**

2° giorno

TUTELA delle INFORMAZIONI

Come individuare gli strumenti idonei per proteggere il patrimonio intellettuale dell'azienda

- I beni da tutelare e i relativi strumenti di protezione: gli *intangibile assets* con particolare riferimento a: Know how, brevetto, marchio, diritto d'autore
- Patrimonio intellettuale e sito Web dell'azienda
- Violazione del marchio e del copyright in Internet: le contromisure più efficaci

Conoscere la disciplina generale in materia di protezione dei dati personali

- Il quadro normativo delineato dal nuovo CODICE SULLA PRIVACY
- Gli obiettivi della legge ed i compiti dei soggetti coinvolti: titolare, responsabile, incaricati del trattamento dei dati
- I documenti obbligatori: notifica, informativa, consenso.
- Le misure minime sulla sicurezza del trattamento e l'organizzazione aziendale
- Il Documento Programmatico sulla Sicurezza alla luce del nuovo DISCIPLINARE TECNICO
- Il trattamento illecito dei dati personali e le conseguenze sanzionatorie
- Il trasferimento dei dati all'estero

Conoscere e risolvere le problematiche collegate ai reati informatici

- Come utilizzare i "controlli imposti" per superare il problema dei "controlli vietati"
- La responsabilità oggettiva dell'azienda per il fatto del dipendente come fondamento del diritto-dovere di controllo
- Quali sono i controlli elettronici alla luce della disciplina in materia di sicurezza del lavoro, di sicurezza e limitazioni nel trattamento dei dati personali e di reati informatici

Frank Geffers
Avvocato
STUDIO PUOPOLO, SISTILLI
GEFFERS & LUISE

Quali sono le misure preventive per tutelare l'azienda

- La definizione dell'organizzazione aziendale come strumento di sicurezza: il rischio di violazioni e le procedure interne
- I codici interni di comportamento: contenuto, vincolatività, sanzioni per la loro violazione
- Le misure di controllo interno: modalità, termini e i limiti di cui agli artt. 4, 6 e 8 dello Statuto dei Lavoratori
- Il personale interno per i servizi di Security: Guardie Particolari Giurate o no? I limiti di cui agli artt. 2 e 3 dello Statuto dei Lavoratori
- Un caso pratico

Come determinare le aggressioni al patrimonio aziendale

- La necessità di accertare un reato commesso contro l'azienda:
 - il reato: cenni
 - l'azienda quale persona offesa dal reato ed il patrimonio aziendale come oggetto del reato
 - l'accertamento del reato è oggetto del processo penale: la necessità di acquisire elementi di prova utilizzabili nel processo
- La reazione ed il limite della legittima difesa: modalità, termini e i limiti di cui all'art. 52 del Codice Penale
- Le aggressioni interne al patrimonio aziendale: casistica e patologie
- Le aggressioni esterne al patrimonio aziendale: casistica e patologie
- Un caso pratico

La responsabilità dell'impresa ed il d. legs. 231/01

- I modelli di organizzazione, gestione e controllo
- L'Organismo di Vigilanza: è una funzione di Security?

L'outsourcing delle funzioni di security

- La legislazione in materia di Vigilanza Privata
- Gli Istituti di Vigilanza Privata e le Guardie Particolari Giurate
- Gli Istituti di Investigazione e gli Investigatori

Giuseppe Menegazzi
Partner **SIMMONS & SIMMONS**
Presidente **A.N.I.V.P.**

Luca Basilio
Avvocato **SIMMONS & SIMMONS**

3° giorno

RISK MANAGEMENT

Il processo di Risk Management: dalla segnalazione dell'evento anomalo alla formulazione delle verifiche di efficacia

- Metodologie per quantificare i danni diretti, indiretti e consequenziali
- Gli strumenti a disposizione dei Security Manager per la valutazione economica degli investimenti di protezione del patrimonio
- Come creare un efficace sistema di *Incident Reporting* aziendale
- Il monitoraggio dell'analisi costi/benefici degli interventi di security e l'adozione di strumenti evolutivi e correttivi

Conoscere quali sono gli strumenti di gestione del rischio e come applicarli correttamente

- Quali sono gli step di analisi dei rischi e come integrare efficacemente: Tecnologie, Procedure e Risorse Umane
- Come gestire la fase di valutazione dei rischi
- In che modo impostare una fase propositiva finalizzata ad una migliore gestione operativa dei rischi

Come definire un piano di emergenza in linea con le politiche di crisis management e gestione dei rischi

Carlo Mastrangelo
Direttore Generale
M & P RISK AGENCY

4° giorno SICUREZZA INFORMATICA

Come realizzare un check up sulla sicurezza ICT e quali sono i ruoli del management e del security manager

- Come individuare i sistemi più esposti
- Classificazione delle vulnerabilità
- In che modo approcciare i problemi riscontrati attraverso l'analisi per trovare la soluzione più adeguata
- La perseveranza del Security Manager

Dall'analisi del rischio e delle vulnerabilità alla definizione e adozione delle soluzioni più efficaci

- Considerare la security come processo ciclico
- Quali sono i piani di adeguamento e come vengono definiti
- Quali sono i diversi processi di security

Vulnerability Assessment come metodologia di controllo secondario

- Quali sono le azioni per la messa in sicurezza
- Come definire ed effettuare i controlli secondari per una maggiore efficacia

La gestione di intrusioni e attacchi in caso di outsourcing della sicurezza

- Qual è il ruolo della sicurezza per garantire un livello di SLA (Service Level Agreement) in linea con gli impegni contrattuali
- Il ruolo della prevenzione come rimedio
- Come stipulare il contratto

Sabino Ciffo

CISM - Certified Information Security Manager
Business Continuity & Security Solution Manager
GLOBAL VALUE SERVICES

5° giorno SICUREZZA FISICA ed ELETTRONICA

Cosa si intende per "sistema di sicurezza"

- Quali sono i criteri per la definizione dei profili di protezione: Sicurezza fisica, Sicurezza logica e Sicurezza organizzativa
- Come individuare le esigenze organizzative e funzionali per rispondere adeguatamente alle minacce da rischio esterno: livello accettabile di rischio residuo
- Quali sono i sottosistemi: fisici (passivi), elettronici (attivi), trasmessivi, gestionali, procedurali

- Qual è l'esigenza d'integrazione dei sottosistemi con l'attività dell'elemento umano e di connessione ad unica funzione gestionale, al fine di assicurare integrità e continuità d'Impresa
- Come classificare gli uffici per tipologia di rischio ed adeguare gli strumenti di tutela

Quali sono le tecniche di protezione dei siti a rischio

- Criteri d'impiego delle componenti principali di protezione fisica: blindature opache e trasparenti
- La protezione elettronica:
 - Logica d'impiego dei principali rivelatori per ambienti interni ed esterni: fattori negativi e positivi
 - La centrale locale di gestione
 - Alimentazione, cablaggi e problematiche installative
- Il controllo televisivo:
 - Le componenti fondamentali di sottosistema
 - Il processo gestionale
 - La trasmissione a distanza del segnale
 - Videoregistrazione digitale ed organizzazione degli archivi
- Il controllo accessi: funzionalità fondamentali ed evoluzione delle varie tecniche
 - Il progressivo affinamento delle tecniche biometriche
- La centralizzazione degli allarmi autonoma ed in outsourcing
- Mezzi d'offesa del terrorismo e nuove metodologie di contrasto

Come progettare un sistema di sicurezza

Come monitorare e valutare, efficienza ed efficacia del sistema di security

- L'audit periodico della sicurezza sotto l'aspetto tecnico e procedurale

Lo stato dell'arte del progetto di legge sulla sicurezza privata

Gianfranco Bonfante
Presidente ITASFORUM
Amministratore Unico
SECURITY CONSULTING SERVICE

Cosa hanno detto di noi...

Ecco cosa hanno detto i Partecipanti alle precedenti edizioni del Security Manager Mastercourse:

"Utile per inquadrare il ruolo del Security Manager, della funzione Security, e per conoscere responsabilità, competenze e tecnologie"

Funzionario Responsabile
Area Servizi Generali
UFFICIO ITALIANO DEI CAMBI

"In linea generale giudizio positivo"
HR Security

IT TELECOM ITALIA

"Fornisce importanti e interessanti spunti di riflessione. Opera alcune distinzioni di concetto che non mi erano così evidenti"
Risk Manager
LINEA

Competenze e Ruolo in azienda del Security Manager

Il ruolo del Security Manager oggi è sempre più importante in azienda, e nuove sono le competenze richieste.

Conoscere procedure, persone, sistemi e tecnologie, è tra i primi doveri del Responsabile Security.

Per garantire la sicurezza globale dell'organizzazione è necessario che il Security Manager sviluppi delle competenze manageriali adeguate a gestire aspetti tecnici, organizzativi, economici ed umani legati alla Sua funzione.

Perché questo Mastercourse è UNICO

Questo Mastercourse fornisce in soli 5 giorni una formazione avanzata.

Si tratta di un corso ESCLUSIVO ed UNICO che tratta in maniera sintetica tutti gli aspetti che un Security Manager preparato e competente deve conoscere:

- Sicurezza Fisica
- Sicurezza Logica
- Sicurezza Organizzativa

In particolare verranno analizzati gli aspetti:

- legali (tutela dei dati personali, tutela del patrimonio intellettuale e reati informatici)
- lavoristici (controllo dei dipendenti, prevenzione, investigazioni, prova e uso della prova)
- tecnologici, economici (budget e costi)
- organizzativi

Al fine di consentire l'apprendimento immediato di quanto analizzato in aula, le illustrazioni teoriche verranno accompagnate da numerosi esempi e casi pratici.

Ai partecipanti verrà rilasciato un attestato di partecipazione

A chi si rivolge questo Mastercourse

In particolare i diretti interessati sono:
Security Manager, Resp. Sicurezza Aziendale
Internal Auditor, EDP Auditor,
Resp. Formazione, Ispettorato,
Resp. Servizi Generali

5 GIORNI FULL IMMERSION PER:

- Tutti coloro che vogliono approfondire gli aspetti essenziali della Sicurezza
- I Security Manager già certificati secondo la N. 10549 per il necessario aggiornamento

SI', DESIDERO PARTECIPARE A:

SECURITY MANAGER MASTERCOURSE

8 - 12 novembre 2004

Cod. A 2116 C

7 - 11 marzo 2005

Cod. A 2229 C

€ 2.835 + 20% IVA per partecipante

La quota di iscrizione comprende la documentazione, la colazione e i coffee break. Per circostanze imprevedibili, l'Istituto Internazionale di Ricerca si riserva il diritto di modificare il programma, i relatori, la sede dell'evento.

5 MODI PER ISCRIVERSI

Telefono: 02.83.847.627

Fax: 02.83.847.262

E-mail: conferenze@iir-italy.it

Web: www.iir-italy.it

Posta: Istituto Internazionale di Ricerca S.r.l.
Via Forcella, 3 - 20144 Milano

MODALITA' DI PAGAMENTO

- versamento sul ns. c/c postale n° 16834202
- assegno bancario - assegno circolare
- bonifico bancario (Banca Popolare di Sondrio Ag. 10 Milano)
c/c 2805/07 ABI 05696 - CAB 01609 - CIN Z
intestato a **Istituto Internazionale di Ricerca**;
IBAN: IT29 Z056 9601 6090 0000 2805 X07; Swift POS 01 T22MIL
indicando il codice prescelto

- carta di credito: Diners Club EuroCard/MasterCard
 CartaSi Visa American Express

N°

Scadenza / Titolare:

Firma del Titolare:

N.B. Non saranno ammessi in aula i delegati la cui quota d'iscrizione non sia pervenuta prima dell'evento. Copia della fattura/contratto di adesione verrà spedita a stretto giro di posta.

MODALITA' DI DISDETTA

L'eventuale disdetta di partecipazione al convegno dovrà essere comunicata in forma scritta all'Istituto Internazionale di Ricerca entro e non oltre il 10° giorno lavorativo precedente la data d'inizio dell'evento. Trascorso tale termine, sarà inevitabile l'addebito dell'intera quota d'iscrizione. Saremo comunque lieti di accettare un Suo collega in sostituzione purché il nominativo venga comunicato via fax almeno un giorno prima della data dell'evento.

DOVE

HOTEL HILTON




VIA GALVANI, 12 - (Stazione Centrale) - MILANO

TEL. 02.69831 *Ai partecipanti saranno riservate particolari tariffe per il pernottamento*

UN'OPPORTUNITA' PER FARSI CONOSCERE:

La Conferenza costituisce l'occasione ideale per raggiungere nuovi clienti, stabilire preziosi contatti con potenziali partner, acquisire maggiore visibilità sul mercato.

Se la Sua Società è interessata a:

- allestire uno spazio espositivo; 
- acquistare spazi pubblicitari all'interno degli Atti del convegno; 
- sponsorizzare coffee break e colazioni; 

contatti: **Mariella Fossi** al n. **02 83847251** -E-mail: **mfossi@iir-italy.it**

Si unisce alle oltre 400 Aziende che hanno scelto le nostre formule pubblicitarie per promuovere la loro immagine!

SCHEDA DI ISCRIZIONE

Sconto euro200 soci Clusit
per iscrizioni entro il 30 settembre 2004

PRIORITY CODE:..A2116clu.....

TUTELA DATI PERSONALI - INFORMATIVA

Si informa il Partecipante ai sensi del D. Lgs. 196/03; (1) che i propri dati personali riportati sulla scheda di iscrizione ("Dati") saranno trattati in forma automatizzata dall'Istituto Internazionale di Ricerca (I.I.R.) per l'adempimento di ogni onere relativo alla Sua partecipazione alla conferenza, per finalità statistiche e per l'invio di materiale promozionale di I.I.R.; (2) il conferimento dei Dati è facoltativo: in mancanza, tuttavia, non sarà possibile dar corso al servizio. In relazione ai Dati, il Partecipante ha diritto di opporsi al trattamento sopra previsto. Titolare e Responsabile del Trattamento è l'Istituto Internazionale di Ricerca, via Forcella 3, Milano nei cui confronti il Partecipante potrà esercitare i diritti di cui al D. Lgs. 196/03 (accesso, correzione, cancellazione, opposizione al trattamento, indicazione delle finalità del trattamento).

La comunicazione potrà pervenire via:

e-mail: variazioni@iir-italy.it - fax: 02.8395118 - telefono: 02.83847634

DATI DEL PARTECIPANTE:

NOME: _____ COGNOME: _____

FUNZIONE: _____

INDIRIZZO: _____

CITTÀ: _____ CAP: _____ PROV.: _____

TEL.: _____ TEL. CELL.: _____

SI, DESIDERO RICEVERE INFORMAZIONI SU ALTRI EVENTI VIA (segnalare eventuale preferenza): _____

FAX: _____

E-MAIL: _____

CONSENSO ALLA PARTECIPAZIONE DATO DA: _____

FUNZIONE: _____

DATI DELL'AZIENDA:

RAGIONE SOCIALE: _____

SETTORE MERCEOLOGICO: _____

FATTURATO IN EURO: 6 0-10 Mil 5 11-25 Mil 4 26-50 Mil 3 51-250 Mil 2 251-500 Mil 1 + 501 Mil

N° DIPENDENTI: G 1-10 F 11-50 E 51-100 D 101-200 C 200-500 B 501-1.000 A + 1.000

PARTITA IVA: _____

INDIRIZZO DI FATTURAZIONE: _____

CAP: _____ CITTÀ: _____ PROV.: _____

TEL.: _____ FAX: _____

TIMBRO E FIRMA