Istituto Internazionale di Ricerca
Know how to achieve

GRC FORUM

Tutte le misure a SUPPORTO del

SECURITY GOVERNANCE RISK & COMPLIANCE

METODOLOGIE ANALISI dei RISCHI	ASPETTI ECONOMICO-FINANZIARI	COMUNICAZIONE del RISCHIO
SICUREZZA INFORMATICA	CRISIS MANAGEMENT e BUSINESS CONTINUITY	ASPETTI NORMATIVI

Milano, 28 e 29 settembre 2010 - Starhotel Ritz

Con la preziosa ***esperienza*** *sul campo di* ***6 Security Manager*** *di grandi aziende:*

G. Femia, Presidente - **AIPSA** e Head of Corporate Security - **VODAFONE Italia**

U. Saccone, Corporate Security Senior Vice President - **ENI**

C. Pantaleo, Dir. Sistemi Tecnologie Protezione Patrimonio - **ATM**

R. Bernardi, Security Manager - **FINMECCANICA**

C. Corradi, Ict Security e Privacy Manager - **VODAFONE**

M. Carpino, Worldwide Corporate Security Director - **GUCCIO GUCCI**

M. Stancati, Dir. - **RIVISTA SCIENTIFICA INAIL** e Docente - **Università La SAPIENZA**

E con la ***consulenza*** *di:*

M. Mapelli, Segretario Generale - **AIPSI**

D. Forte, CEO - **DFLabs**

P. Lonero, Senior Manager - Security Risk & Compliance - **KPMG**

M. Vintiadis, Country Manager - **KROLL**

P. Traversa - Senior Security Consultant **POLIMATICA**

M. Lombardi, ITSTIME - **UNIVERSITÀ CATTOLICA**

F. Maccaferri - **PRAGMATICA CONSULTING**

Con il patrocinio di:

aipsa Associazione Italiana Professionisti Security Aziendale

aipsi

Trasmettere a:

> Security Manager
> Responsabile Affari Generali
> Responsabile Compliance
> Responsabile Sistemi Informativi
> Direttore Generale e Amministratore Delegato
> Risk Manager e Internal Auditor
> Responsabile Servizio Antifrode e Financial Manager
> Responsabile Legale

Un convegno **pratico** e **concreto** per:

- valutare come definire un **sistema integrato** di *Security* aziendale
- individuare le **strategie** per una corretta *mappatura* e *gestione* dei rischi in funzione della sicurezza: il *Risk Assessment*
- divulgare all'interno della propria organizzazione l'utilizzo delle **misure** di **sicurezza** quale supporto al perseguimento delle attività di business
- valutare l'efficacia della propria **policy** di sicurezza e definire **procedure** sicure e semplici
- approcciare la sicurezza con **logiche economiche** per essere credibili sulle proposte fatte
- valutare l'**impatto Economico-Finanziario** dei rischi per proporre e motivare investimenti adeguati
- ROI e **ROSI** (Return on Security Investment)
- **comunicare** i rischi ad ogni livello del *business*
- rendere la **cultura del rischio** e della sicurezza un *patrimonio comune* in azienda

Workshop post-Convegno:

SICUREZZA e PRIVACY in azienda

Milano, 30 settembre 2010

Partecipa con la FORMAZIONE FINANZIATA!

Per iscriversi: Tel. 02 83847.627 - Fax 02 83847.262 - Email: info@iir-italy.it - Sito: www.iir-italy.it

Istituto Internazionale di Ricerca
Know how to achieve

Maggio 2010

Egregio Dottore, Gentile Dottoressa,

La gestione della Sicurezza avviene in tutte le aziende, anche se spesso in forma non strutturata: infatti benché l'attività del Security Manager contribuisca fortemente alla Compliance aziendale e alla Risk Governance, la sua funzione non è ancora legittimata e viene spesso percepita come una voce di spesa.

Affinché il Security Manager possa supportare la Governance, ottimizzare il Rischio e dimostrare la Compliance assicurando al tempo stesso il presidio della sicurezza aziendale, deve acquisire sempre più un **approccio** orientato al ***business***, prendendo decisioni sempre più frutto di valutazioni ponderate economicamente e sviluppando un'accurata attenzione ai processi aziendali.

Partecipi, dunque, al **SECURITY GOVERNANCE RISK & COMPLIANCE FORUM**, che IIR rivolge ai referenti della Sicurezza in azienda. Potrà trovare **casi reali** relativi alle **esperienze** sul campo maturate da Suoi colleghi di altre aziende e **applicazione** e **progetti dimostrativi** dei temi trattati rispetto a:

- Procedure di *Risk Assessment & Analysis* finalizzate alla Sicurezza aziendale
- Policy di *Crisis Management*
- Tecniche *Investigative*
- *Sicurezza Informatica*
- *Gestione Economica* della sicurezza
- Impatto *Economico-Finanziario* del rischio
- Logiche di *Comunicazione* del danno ai vertici aziendali
- Aspetti di *Comunicazione* della sicurezza in azienda

Potrà confrontarsi con colleghi ed esperti su:

- SOLUZIONI concrete ed efficaci
- come delineare STRATEGIE integrate per mettere in sicurezza
  - tutti i **processi** aziendali senza rallentarli
  - le **informazioni**
  - le **persone**
- in base a quali parametri valutare l'EFFICACIA della propria policy sulla sicurezza
- quali LINEE GUIDA adottare per PREVENIRE, FRONTEGGIARE e SUPERARE rischi e danni
- come definire PROCEDURE sicure e semplici per assicurare la sicurezza in azienda
- quali STRUMENTI strutturali, procedurali, operativi e culturali adottare per sviluppare un approccio efficace di Security

Si iscriva subito, inviando la scheda di iscrizione via fax al numero 02 83847262 oppure visitando il sito www.iir-italy.it .

I Relatori del Convegno ed io La aspettiamo a questa imperdibile occasione di **confronto**.

Cordiali Saluti,

Dott.ssa Lorena Quagliati
Conference Manager

Ecco 5 buoni motivi per cui diventare Sponsor:

- **best in class**: il convegno è promosso da IIR, leader nell'organizzazione di eventi per il mercato di riferimento
- **promotion**: il database IIR non ha rivali nell'industria degli eventi
- **top management**: il programma si rivolge ai decision maker che non incontrereste in una fiera
- **communication**: un team di professionisti dedicato al progetto vi garantirà la massima visibilità prima, durante e dopo l'evento
- **tailored solutions**: la vostra partecipazione risponderà esattamente ai vostri obiettivi di business

Contatta: Luca Maestri
e.mail: Luca.Maestri@iir-italy.it - tel. 02.83847208

FORMAZIONE FINANZIATA!

La partecipazione a questa iniziativa è possibile anche utilizzando i **voucher formativi** che i **Fondi Interprofessionali** mettono a disposizione per finanziare la formazione aziendale.
A tale proposito Istituto Internazionale di Ricerca, con i suoi Consulenti, è in grado di supportare le Aziende nell'individuare le fonti di finanziamento e gli aspetti gestionali e amministrativi legati all'utilizzo dei fondi, sia per i corsi e i convegni a catalogo che per i progetti formativi interni all'Azienda.

Per informazioni contattare il nr. 02.83847.624
oppure scrivere all'indirizzo voucherformativi@iir-italy.it

GRC - Security Governance Risk &

28 Settembre 2010

Chairman:
Umberto Saccone
Corporate Security Senior Vice President
Eni

8.30 *Registrazione Partecipanti*

9.00 *Apertura Lavori del Chairman*

Security Risk Assessment, Governance Risk e Compliance

9.15 **La Security Governance: conoscere le istanze in tema di sicurezza e definire un sistema integrato di security dell'azienda**
- Evoluzione della funzione e dei modelli organizzativi: dalla tutela del patrimonio e del business alla security resilience
- Perimetro attività e responsabilità del Security Management in azienda
- Strategicità della Business Security e della Risk Governance aziendale
  - I fattori di successo del sistema integrato di security
  - Il dialogo organizzativo e la comunicazione
- Total Risk Governance: Security 2.0

Giuseppe Femia, *Presidente* - **AIPSA Associazione Italiana Professionisti Security Aziendale**
e *Head of Corporate Security* - **VODAFONE Italia**
Inizia la sua carriera nel mondo della sicurezza pubblica come Ufficiale dei Carabinieri dal 70 al 79. Si inserisce nel contesto della sicurezza aziendale dal 1979, prima come Responsabile Security all'interno del Gruppo Olivetti e a partire dal 1996 ad oggi come Head of Corporate Security in Vodafone Italia. Dal 2008 è anche Presidente AIPSA.

CASE HISTORY

10.15 **Quali valutazioni fare per definire la policy di *CRISIS Management*: previsioni, procedure e contromisure. L'esperienza di ENI**
- Approfondire l'evoluzione del corpus normativo verso la Security
- La Security nel Testo Unico 81/08 e nel D. Lgs. 231/01
- Il dovere di protezione dei dipendenti nel mondo
- Il modello di gestione e presidio della Sicurezza aziendale: la Security Eni
  - i suoi ambiti
  - i suoi strumenti
- Case study: il "progetto Iraq"

Umberto Saccone, *Corporate Security Senior Vice President* - **Eni**
Laureato in Scienze Politiche, ha frequentato master sulla tutela dei dati personali, sul rapporto privacy-security, infrastrutture critiche e sulla sicurezza nazionale presso il Defence Intelligence College di Washington. Dal 1974 al 2006 ha prestato servizio nell'Arma dei carabinieri dove ha raggiunto il grado di Generale di Brigata. Ha ricoperto numerosi incarichi in Italia e all'estero presso gli Organismi per l'Informazione e la Sicurezza. Nel 2006, congedatosi dall'Amministrazione militare, ha assunto l'incarico di Direttore della Security dell'Eni. È membro di numerosi "fora" tra le principali Oil Company, tra cui il G7 e l'OCSC.

11.15 *Coffee Break*

CASE HISTORY

11.30 ***Security Governance Risk*: il sistema di sicurezza nell'ambito degli approcci di Risk Assessment. L'esperienza di ATM**
- In che misura e a quali condizioni i sistemi di mappatura e gestione dei *Rischi* rappresentano uno strumento per fare convergere le iniziative che nascono nel perimetro della *Governance* aziendale
- In che modo è stata realizzata la mappatura del rischio in funzione della sicurezza organizzativa
  - policy e attività legate alla *Compliance*
  - procedure legate al business
  - istruzioni operative e l'impatto sui comportamenti dei dipendenti
  - definizione dei sistemi di controlli interni
- Risk & Business Impact Analysis sui processi aziendali: benefici e criticità
  - individuazione aspetti critici di processo
  - individuazione di indicatori di rischio
  - definizione di programmi di previsione del rischio e contromisure
- Quali misure sono state messe in atto per gestire i rischi globali e quelli locali al fine di mettere in sicurezza i maggiori processi aziendali senza rallentarli
  - che cosa è stato valutato
  - finalità
  - obiettivi
  - creare un modo efficiente di consolidare la policy tramite gli asset IT
- Incident Reporting quale strumento d'individuazione di nuovi rischi e loro inserimento nel ciclo di risk management
- Condivisione delle informazioni relative a rischi già emersi in altre realtà

Claudio Pantaleo, *Direttore Sistemi tecnologie Protezione Patrimonio* - **ATM Azienda Trasporti Milanesi**
Inizia nel 1975 la sua attività lavorativa in IBM; dal 1994, nella funzione Security Aziendale, affronta problematiche inerenti la Physical Security e Emergency Planning. Nel 1995 assume anche la funzione di intelligence operativa nella Security a livello mondiale sino a diventare Direttore Sicurezza Aziendale della IBM Italia. A febbraio 2004 assume l'incarico di Head of Security della British American Tobacco (BAT) e nel 2005 quello di Head of Security per l'area del Sud Europa. A gennaio 2009 diventa Security Manager in ATM.

12.30 **Conoscere e valutare le diverse soluzioni di *Risk Response***
- Che cosa comporta ideare e individuare contromisure
- Quali tipi di contromisure prendere in considerazione e in quali circostanze
  - soluzioni assicurative
  - soluzioni contrattuali
  - controllo interno
  - Incident Management
- Valutare gli impatti delle contromisure
  - Indicatori numerici di performance sulla sicurezza
- Come strutturare un controllo efficace sull'effettiva applicazione delle contromisure
- Il ruolo dell'*Internal Auditing* e del *Risk Management* nei sistemi di sicurezza interni
- Analisi di **Casi di Studio**

Dario Forte, *CEO* - **DFLabs**
CEO di DFLabs, azienda specializzata nell'Information Security Risk Management con sede in Italia e USA.
Laureato in Scienze dell'Organizzazione all'Università di Torino, Post graduate in sicurezza informatica e MBA (University of Liverpool), ha tenuto speech di livello internazionale, inclusa la Banca Mondiale e la NATO. È membro del Board of Advisors di Elsevier Science Group (UK) e Electronic Discovery Solutions Group (USA).

13.30 *Colazione di Lavoro*

CASE HISTORY

15.00 **In che modo Vodafone assicura la *Business Continuity*. La definizione del Business Continuity Plan (BCP): attività e fasi**
- Il Risk Assessment e la Business Impact Analysis
  - come vengono identificati i rischi
  - come vengono definiti gli scenari relativi all'impatto dei rischi
  - su quali basi viene costruito il piano di piano di business continuity
- Le strategie di business continuity ed il legame con i piani di contingency e disaster recovery tecnologico
- In che modo il BCP viene reso accettabile e applicabile a livello organizzativo
- In che modo il BCP viene testato e mantenuto nel tempo
- Quali verifiche vengono fatte a livello di Internal Audit
- Il ruolo di Vodafone Italia come infrastruttura critica del paese

Corradino Corradi, *Ict security e privacy manager* - **VODAFONE**
Dal 2002 è in Vodafone Omnitel NV come responsabile della sicurezza informatica e reti, del Business Continuity Management, della privacy e della data protection. È anche co-chairman del Vodafone Group Corporate Security forum e del gruppo di lavoro sul Business Continuity Management. In precedenza ha lavorato in Telesoft e Ericsson Telecomunicazioni per lo sviluppo di sistemi informatici.

16.00 **Metodologie di *Risk Analysis*: come identificare, analizzare e valutare i rischi di sicurezza. L'esperienza di FINMECCANICA**

CASE HISTORY

- Approcci organizzativi al Risk Analysis a fronte delle problematiche di accentramento e gestione partecipativa ai processi
  - il ruolo dei diversi attori aziendali e del sistema di sicurezza
  - sforzi e strumenti organizzativi
  - le verifiche di audit
- Come fare previsioni, analisi e valutazione dei rischi (prevenzione operativa)
- Di che cosa devono tenere conto i metodi di Risk Analysis e le logiche di mappatura dei rischi:
  - Quali valutazioni possono essere fatte e come a fronte di analisi di storicità
  - Come individuare le probabilità di accadimento degli eventi critici e come realizzare le proiezioni
  - Come effettuare valutazioni di impatto degli eventi negativi (errori, frodi, disastri)
  - Con quale criterio prendere misure preventive
  - Come individuare procedure operative di crisi in funzione dei rischi
- Problematiche connesse all'utilizzo dei metodi di analisi qualitativi e quantitativi

Romolo Bernardi, *Security Manager* - **FINMECCANICA**
Dal 2004 è Vice President del Group Security Office di Finmeccanica, quale riferimento della Security per il Gruppo in termini di Governance, Metodologie e Strumenti condivisi. Laureato in "Giurisprudenza" e in "Scienze della Sicurezza Interna ed Esterna" ha frequentato il Corso avanzato di Security Management all'Università "L. Bocconi". È Vice Presidente dell'AIPSA e membro del Consiglio Direttivo del CEPAS.

17.00 ***Metodologie* e modalità di svolgimento delle *Indagini Interne*: come pianificare l'Investigazione interna e di quali tipi di tecniche investigative è possibile avvalersi**

- Come pianificare una investigazione interna all'azienda: quali variabili devono essere tenute sotto controllo
- Come strutturarsi e quali risorse coinvolgere
- Conoscere le tecniche e le metodologie oggi disponibili e quali sono le più efficaci a seconda della propria realtà
- La gestione delle investigazioni: alcune indicazioni pratiche per mantenere l'integrità delle prove

Marianna Vintiadis, *Country Manager* - **KROLL**

17.45 *Chiusura Lavori 1° giorno*

29 Settembre 2010

Chairman:
Maurizio Mapelli
Segretario Generale, **AIPSI Associazione Italiana Professionisti Sicurezza Informatica**

9.00 *Apertura Lavori a cura del Chairman*

La dimensione economica della sicurezza

*Per facilitare e orientare i Decision Maker degli investimenti di sicurezza è essenziale dedicare attenzione agli aspetti **economici** dei progetti. Per fare questo diventa sempre più indispensabile per il Security Manager ragionare in termini **finanziari** al fine di giustificare gli investimenti, che devono essere proposti come il frutto di valutazioni e decisioni ponderate anche economicamente.*

9.15 **L'analisi e la quantificazione economica del *Rischio*: criticità e benefici**

- Definire e identificare i principali problemi in modo concreto e reale
  - rischi
  - minacce
  - conseguenze
- I danni possibili ai beni tangibili e quelli intangibili
- Il trattamento del rischio: accettare, ridurre o "trasferire"?
- Il peso della compliance normativa
- La struttura dei costi per le prevenzione: l'importanza della formazione

Maurizio Mapelli, *Segretario Generale* - **AIPSI Associazione Italiana Professionisti Sicurezza Informatica**
Socio Fondatore e Segretario dell'AIPSI, ISSA Italian Chapter; Consulente per TLC, Finanza e PMI. È stato per Italtel e Siemens Direttore della Information Technology e Security Manager. Ha partecipato a diversi Users' Groups di società internazionali di Informatica; è stato, inoltre, socio e Coordinatore Reti in AICA, membro di EIRMA e socio del ClubTI Milano. È Lead Auditor qualificato BS7799/ISO27001, certificato LoCSI.

10.15 **Il ritorno degli investimenti inerenti la sicurezza per sostenere le proprie *scelte*, giustificare le *spese necessarie*, ottenere *Commitment***

- Dal ROI al ROSI (Return On Security Investment)
- In che modo mettere in evidenza le valutazioni e le motivazioni degli investimenti
- Scegliere dove investire, come investire e spiegare le ragioni delle proprie scelte
- Aspetti economico-finanziari, aspetti quantitativi non economici, aspetti qualitativi
- In che misura è possibile misurare i ritorni degli investimenti in sicurezza?
- Quali strumenti per supportare le scelte dei vertici: sostenibilità del metodo

Pierluigi Lonero, *Senior Manager - Security Risk & Compliance* - **KPMG**
Dopo una significativa esperienza come ufficiale della Marina Militare durata sino al 2000, ha deciso di dedicarsi al settore della consulenza unendosi nel 2006 al network KPMG. Ha maturato significative esperienze nelle tematiche di Information System Governance - con focus su analisi Rischi, Sicurezza e Compliance normativa - e nella definizione e realizzazione di sistemi di reporting, sistemi complessi di indicatori KPI/KRI.

11.15 *Coffee Break*

11.30 **Sicurezza e obiettivi aziendali: come stimare un budget appropriato e farlo approvare**

La sicurezza nella sua accezione più estesa interviene ex-ante come strumento di prevenzione ed ex-post come strumento di reazione in tutti gli ambiti aziendali. La relazione con il Risk Management è diretta ed immediata: non ci può essere Risk Management senza Security Management. Il Security Management agisce da "circoscrittore" del rischio e le sue soluzioni lo rendono attendibilmente calcolabile, valutabile e in ultimo, (forse) sopportabile. Quanto è, tuttavia, il rischio sopportabile? Come si può determinare l'ammontare appropriato del budget per gli investimenti in sicurezza? Come lo si può sostenere?

- La visione estesa della sicurezza
- La debolezza del Security management ovvero la difficoltà nel giustificare un costo certo rispetto all'evento incerto
- *Risk appetite* e obiettivi aziendali:
  - perchè investire
  - dove investire
  - quanto è sostenibile investire nella sicurezza
- Il "costo" reputazionale e strategico del rischio residuo
- Controllo di processo e sicurezza: dove e come il Security Management può intervenire usando gli strumenti del risk management
- ISO31000: il risk management ha il suo standard. Quale ruolo per il Security Management?

Fabio Maccaferri, *AD* - **PRAGMATICA CONSULTING**
Per quindici anni Programme Manager presso primarie Aziende impiantistiche italiane, ha in seguito co-fondato ed è stato Direttore Generale della BeS Consulting, dove ha sviluppato servizi nell'ambito dell'Enterprise Risk Management, Business Continuity Management, Compliance, Governance Organizzativa e Business Innovation. È inoltre docente a contratto presso l'Università Cattolica e collabora con il CETIF, Centro di Ricerca su Tecnologie, Innovazione e Servizi Finanziari.

12.30 ***Security Governance Risk & Compliance* e Sicurezza Informatica: in che modo definire un modello di *Governance* dell'*ICT Security* rispettoso sia degli aspetti strategici e di policy sia degli aspetti operativi dell'IT**

- In che modo e in che misura la sicurezza informatica consente di assolvere le esigenze di

- protezione, confidenzialità, integrità e disponibilità delle informazioni e dei dati
- protezione fisica e sicurezza logica
- privacy e Compliance con normative e standard
- Business Continuity

• Con quali mezzi massimizzare la sicurezza della rete informatica
- i principali rischi di attacco
- le principali contromisure
- controlli di sicurezza dei programmi

• Come presidiare la rapida evoluzione tecnologica (virtualizzazione, cloud computing) e definire appropriate contromisure (tecniche e non)
• Modelli di governance dell'information security
• Nuove sfide

Paolo Traversa, *Senior Security Consultant* - **POLIMATICA**
Si occupa di sicurezza informatica dal 1996. Ha collaborato con alcune delle principali realtà industriali e finanziarie, quali Fiat, Iveco, Case New Holland, Finmeccanica, CRIF, per la definizione di policy ed architetture di sicurezza curando sia gli aspetti operativi che procedurali e metodologici.

13.30 *Colazione di Lavoro*

Sicurezza e comunicazione: un approccio integrato

15.00 ***Comunicare* la Sicurezza ai vertici aziendali: criticità e benefici**

CASE HISTORY

• Il ruolo della direzione
• Su quali aspetti focalizzarsi e su quali argomenti fare leva
- percezione del ruolo della Security
- evidenza dell'utilità aziendale
- comunicare valutazioni e motivazioni agli investimenti

Come diffondere, condividere e contribuire a *rendere attuative* le policy di sicurezza rivolte alle funzioni aziendali operative

• Come impostare un sistema organizzativo per promuovere la sicurezza
- implementazione
- auditing e azioni correttive
- management review e miglioramento continuo

• Il ruolo dei manager di linea e del middle management
- suggerimenti e spunti sul comportamento da mantenere

Massimiliano Carpino, *Worldwide Corporate Security Director* - **GUCCIO GUCCI**
Nel Gruppo Gucci dal 2006, è direttore del dipartimento Worldwide Corporate Security, che si occupa, a livello globale, di tutte le attività di prevenzione e tutela del patrimonio tangibile e intangibile per le aree corporate, retail e supply chain. Avvocato esperto di diritto penale d'impresa, è professore a contratto presso l'Università Cattolica del Sacro Cuore di Milano, laurea specialistica in Scienze della Criminalità e Tecnologie per la Sicurezza. Ha ottenuto la certificazione internazionale CPP ed è membro di AIPSA e ASIS.

16.00 **La comunicazione nell'ambito della gestione delle emergenze in azienda: come proteggere le persone e informare in condizioni di crisi**

• Qual è la relazione tra gestione della crisi e comunicazione e informazione
• Come è possibile comunicare in modo efficace
• In che modo anticipare la crisi per gestirla al meglio
• Come favorire comportamenti adattivi per le situazioni d'emergenza
• Quando e come ricorrere agli esperti

Marco Lombardi, *ITSTIME (Italian Team for Security Terroristic Issues & Managing Emergencies), Dip. di Sociologia* - **UNIVERSITÀ CATTOLICA**
Responsabile del progetto ITSTIME presso l'Università Cattolica, insegna Gestione della crisi e comunicazione del rischio. È un esperto di gestione delle emergenze e ha sviluppato studi sulla gestione di sistemi complessi e sistemi sotto stress, con particolare attenzione alla dimensione della sicurezza in una molteplicità di ambiti.

16.45 **Comunicazione di *Crisi* e qualità della Comunicazione Organizzativa nell'ottica della Sicurezza**

• La leva strategica della Comunicazione Interna
• La funzionale continuità fra Comunicazione Interna e Comunicazione Esterna
• I vantaggi di avere un unico portavoce
• ***Crisis Management** Team*
- i modelli internazionali di riferimento
- l'esperienza nella quotidianità aziendale

• La gestione comunicativa della crisi nell'era dei *New Media*
• ***Crisis Communication Management**: un vademecum* in A4
• Le **Case History** offerte dalla cronaca

Marco Stancati, *Direttore* - **RIVISTA SCIENTIFICA INAIL** e *Docente* - **Università La SAPIENZA di ROMA**
Attualmente docente di "Comunicazione interna" e di "Pianificazione dei media" alla Sapienza di Roma e Consulente Direzionale, dal 1999 al 2008 è stato Direttore Centrale della Comunicazione dell'INAIL dove, dal 2004 al 2008 è stato anche Membro del Crisis Management Team.

17.30 *Chiusura Lavori*

Workshop post-Convegno

Con possibilità di iscrizione separata!

SICUREZZA e PRIVACY in azienda

MILANO, 30 SETTEMBRE 2010

• *Le ultime Novità in materia di Privacy e loro impatti sulla Sicurezza aziendale*
• *Quali sono i limiti delle tecnologie di sicurezza e come utilizzarli senza incorrere in rischi*
• *Gestire le informazioni sensibili secondo le regole della Privacy*
• *Che cosa comportano i Sistemi di videosorveglianza*

9.00 *Registrazione Partecipanti*

Analisi di casi specifici e ultimi provvedimenti del GARANTE

9.30 *Apertura Lavori*

Sicurezza e Privacy IT

• Misure minime e misure idonee per la protezione dei dati personali
• Privacy e sistemi IT:
- Il provvedimento del 13 ottobre 2008 in materia di rifiuti di apparecchiature elettriche ed elettroniche (RAEE)
- Il provvedimento del 27 novembre 2008 del Garante sugli Amministratori di Sistema
- Impatti dei provvedimenti su organizzazione della sicurezza e sui sistemi IT

Sicurezza e Privacy dei Lavoratori

• Uso degli strumenti elettronici da parte dei lavoratori
• Amministratori di sistema e privacy dei lavoratori
• Sicurezza e le linee guida del Garante per gli strumenti elettronici
• Aspetti tecnici del provvedimento dell'8 aprile 2010 in materia di videosorveglianza

***Elio Florio**, Funzionario del Dipartimento Risorse tecnologiche,* **GARANTE per la PROTEZIONE dei DATI PERSONALI**

16.00 *Chiusura Lavori*

Nell'arco della giornata è previsto un coffee break intorno alle 11 e una colazione di lavoro intorno alle 13

Step 1 Sì, desidero partecipare a:

✓	Titolo	Data	Codice
❒	CONVEGNO:	28-29 settembre 2010	A 4490 C
❒	WORKSHOP:	30 settembre 2010	A 4490 W

Step 2 Iscrizione

CONVEGNO	PREZZO
❒ Entro il 18/07/2010:	€ 1.395
❒ Entro il 12/09/2010:	€ 1.495
❒ Dopo il 12/09/2010:	€ 1.595

WORKSHOP
❒ € 745

+ 20% IVA per partecipante

SAVE 200 €!!

SAVE 100 €!!

Le offerte sono valide esclusivamente per i pagamenti pervenuti entro la data di scadenza della promozione

SECURITY GRC FORUM

SCONTO RELATORE 200€

PRIORITY CODE:.....

La soluzione più CONVENIENTE

CONVEGNO + WORKSHOP

❒ Entro il 18/07/2010: € 1.995

❒ Entro il 12/09/2010: € 2.130

❒ Dopo il 12/09/2010: € 2.230

SCONTO SPECIALE previsto per la partecipazione di

❒ **2 persone** della stessa azienda **250 euro** complessivi

❒ **3 persone** della stessa azienda **400 euro** complessivi

su ogni linea di prezzo

Non è valido per il solo Workshop

DOVE

STARHOTEL RITZ
Via Spallanzani, 40 - (MM1-Lima o P.ta Venezia)
20129 MILANO - Tel. 02.2055

Ai partecipanti saranno riservate particolari tariffe per il pernottamento

Fax:	E-mail:	Web:	Posta:	Telefono:
02.83.847.262	iscrizioni@iir-italy.it	www.iir-italy.it	Via Forcella, 3 - 20144 Milano	02.83.847.627

Step 3 Dati del Partecipante (è necessario l'invio di una scheda per ogni partecipante)

NOME: COGNOME:

FUNZIONE: TEL.: CELL.:

SÌ, DESIDERO ESSERE AGGIORNATO SU FUTURE INIZIATIVE VIA (*segnalare eventuale preferenza*):

❒ FAX: ❒ E-MAIL

Step 4 Dati dell'Azienda

RAGIONE SOCIALE: SETTORE MERCEOLOGICO:

INDIRIZZO:

CITTÀ: CAP: PROV.:

CONSENSO ALLA PARTECIPAZIONE DATO DA: FUNZIONE:

PARTITA IVA: TEL.: FAX:

INDIRIZZO DI FATTURAZIONE (SE DIVERSO):

CITTÀ: CAP: PROV.:

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 ❒ 201-500 B ❒ 501-1.000 A ❒ + 1.000

MODALITA' DI PAGAMENTO

Il pagamento è richiesto a ricevimento fattura e in ogni caso prima della data di inizio dell'evento.

Copia della fattura/contratto di adesione verrà spedita a stretto giro di posta.

☐ versamento sul ns. c/c postale n° 16834202

☐ assegno bancario - assegno circolare

☐ bonifico bancario (Banca Popolare di Sondrio Ag. 10 Milano)
c/c 000002805x07 ABI 05696 - CAB 01609 - CIN Z
intestato a **Istituto Internazionale di Ricerca;**
IBAN: IT29 Z056 9601 6090 0000 2805 X07;
Swift POSOIT22 indicando il codice prescelto

• carta di credito:

○ Diners Club ○ EuroCard/MasterCard

○ CartaSi ○ Visa

N° ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

*Codice di sicurezza CVV**..... *Scadenza* ☐☐/☐☐

Titolare: .....

Firma del Titolare: .....

** Per la maggior parte delle carte di credito, il codice CVV è costituito dagli ultimi tre numeri riportati sul retro della carta sopra la striscia della firma*

La quota di iscrizione comprende la documentazione, la colazione e i coffee break.
Per circostanze imprevedibili, IIR si riserva il diritto di modificare senza preavviso il programma e le modalità didattiche, e/o cambiare i relatori e i docenti

IIR si riserva la facoltà di operare eventuali cambiamenti di sede dell'evento

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. I dati raccolti potranno essere comunicati ai partner di I.I.R. e a società del medesimo Gruppo, nell'ambito delle loro attività di comunicazione promozionale; *(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).
Potrà trovare ulteriori informazioni su modalità e finalità del trattamento sul sito: www.iir-italy.it

La comunicazione potrà pervenire via: e-mail: variazioni@iir-italy.it - fax: 02.8395118 - telefono: 02.83847634

MODALITA' DI DISDETTA

L'eventuale disdetta di partecipazione (o richiesta di trasferimento) al convegno dovrà essere comunicata in forma scritta all'Istituto Internazionale di Ricerca entro e non oltre il 6° giorno lavorativo (compreso il sabato) 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.

TIMBRO E FIRMA

Stampa n. DaA4490