



Associazione Italiana
Information Systems Auditors



Il successo del nostro XXIII Convegno Nazionale

Questo numero esce con qualche giorno di ritardo, perché volevamo dare ai soci, che non sono potuti venire al Convegno di Pisa, alcune informazioni sull'evento.

Come già da alcuni anni, anche a Pisa la platea dei soci è stata numerosa e partecipe. Al convegno hanno anche partecipato alcuni studenti della facoltà di Informatica

Un grazie a tutti i partecipanti ed ai relatori che, con la loro professionalità, hanno esposto temi interessanti ed innovativi, suscitando l'interesse della platea.

Un particolare ringraziamento al Prof. Baiardi ed al dott. Telmon che ci hanno permesso di accedere al prestigiosa sede della facoltà di Scienze matematiche, Fisiche e Naturali. Grazie anche a loro, inoltre, abbiamo potuto visitare, nella serata del 21 maggio, il Museo di Scienze Naturali, collocato presso la Certosa di Calci.

Quest'anno, i presenti sono stati 100.

I commenti nel "foyer" e la lettura dei questionari di valutazione ci aiuteranno a migliorare sempre più l'organizzazione di eventi.

AIEA ha partecipato

Nel mese di marzo 2009 si è concluso il Gruppo di Lavoro sulle "Competenze nella sicurezza delle informazioni" istituito dal "Forum delle competenze digitali", associazione senza scopo di lucro, alla quale partecipa AIEA, che promuove, valorizza ed accresce la diffusione della cultura e delle conoscenze in materia di competenze e professionalità nel settore dell'ICMT (Information, Communication & Media Technology) e delle Tecnologie Digitali.

Il Gruppo di lavoro, cui ha partecipato AIEA nella persona del socio Silvano Bari, ha prodotto un Rapporto in cui vengono analizzati gli schemi di accreditamento e certificazione esistenti in materia di sicurezza delle informazioni, individuati alcuni metodi di mappatura delle competenze, e proposta una lista delle principali certificazioni.

In particolare, nel Capitolo "La certificazione delle competenze nella sicurezza delle informazioni", curato da Silvano Bari, si analizzano:

- a) la tipologia e le diverse caratteristiche delle attestazioni concernenti le competenze del personale (prima, seconda e terza parte);
- b) il processo di accreditamento e certificazione con riferimento alle varie figure coinvolte;
- c) le norme e le guide di riferimento;
- d) lo stato dell'arte delle certificazioni delle competenze nella sicurezza delle informazioni, distinte per tipologia.

Il Rapporto sarà reso disponibile, a breve, a tutti i soci AIEA.



Assemblea Annuale

Il 1° luglio 2009 si terrà l'Assemblea annuale che sarà anche un'occasione per partecipare ad una "edizione speciale" di una Sessione di Studio, con un'interessante relazione, da parte del socio Stefano Aiello sul tema "Soluzioni organizzative e capacità manageriali mirate all'industrializzazione dei Servizi IT".

A breve vi daremo tutte le informazioni.

Elezioni probiviri triennio 2009-2012

Nei primi giorni di giugno è stata inviata, a tutti i soci, la documentazione e le istruzioni per l'elezione dei 3 Proviviri, previsti da statuto. Ricordiamo che il 30 giugno è in scadenza il mandato dell'attuale Comitato.

Come da istruzioni inviate, i soci sono pregati di inviare la scheda di votazione entro e non oltre il 15 giugno, in modo da poter chiudere lo spoglio delle schede ed arrivare alla designazione entro fine mese.

Un sollecito a votare, quindi, ai soci che ancora non lo avessero fatto.

Il trentennale di AIEA

L'otto ottobre di trent'anni fa nasceva AIEA. Un gruppo di pochissime persone, unite da comuni esperienze di lavoro ed obiettivi, fondava l'Associazione Italiana EDP Auditors. Con il tempo, il nome ha perso la sua natura di acronimo e ha assunto il significato di Associazione Italiana Information Systems Auditors ed i soci sono quasi 800. Il CD ha deciso di festeggiare il trentennale, organizzando in contemporanea a Milano, Roma e Torino tre Sessioni di Studio, di cui quella di Milano di una intera giornata

Gruppi di Ricerca

Gruppo di Lavoro "Traduzione Cobit 4.1"

COBIT 4.1 – sono stati tradotti e resi disponibili nell'area Downloading del sito l'"Executive Summary" ed i seguenti processi: ME1, ME2, ME3, ME4; DS1, DS2, DS3, DS4, DS5, DS6; AI1, AI2, AI3, AI4.

Business Continuity

Il Gruppo di ricerca è formato da una rappresentanza di ciascuna delle Associazioni AIEA, AUSED e ANSSAIF.

Il testo del documento è completo ed è ora avviata la procedura di approvazione da parte delle Associazioni promotrici in vista della pubblicazione della Guida AIEA. In particolare il testo è ora all'esame dei presidenti delle associazioni. Un grazie al socio Massimiliano Rinalducci che ha coordinato il GdR. Non appena il testo sarà approvato il contenuto sarà consultabile dai soci.

CobIT e legge 262

Il Gruppo di Ricerca AIEA è articolato in 6 sottogruppi chiamati Focus Group.

I partecipanti alla ricerca sono ben 17 soci divisi in 6 Focus Group i cui Relatori sono:

Alessandro Arca (FG5)

Giuliano Flesia (FG4)

Luca Nurisso (FG1 e FG6)



Dino Ponghetti (FG3)
Luca Turri (FG2)

Le tematiche dei Focus Group sono le seguenti:

- FG1: Introduzione e normativa di riferimento
- FG2: Dimensionamento delle verifiche e analisi dei rischi
- FG3: Controlli generali
- FG4: Controlli applicativi
- FG5: Campionamenti
- FG6: Valutazione del sistema di controllo e attestazioni finali

Le relazioni dei Focus Group 1, 2, 3, 4 e 6 sono giunte alla finalizzazione, come da programma, entro l'estate ed ora passano alla fase di convalidazione fra tutti i partecipanti al GdR; tale fase dovrà concludersi entro due mesi lavorativi e pertanto entro l'autunno, considerato il periodo di ferie estive. L'attività del Focus Group 5 è in svolgimento e si prevede che sarà ultimata essa pure entro l'autunno

Gruppo di Lavoro "Traduzione Val IT 2.0"

Sta lavorando, con il coordinamento di Guido Leone, il Gruppo di Lavoro che si occupa della traduzione della versione aggiornata di Val IT 2.0. In particolare delle seguenti pubblicazioni:

Enterprise Value: Governance of IT Investments - The Business Case
Enterprise Value: Governance of IT Investments - Getting Started with Value Management
Enterprise Value: Governance of IT Investments - The Val IT Framework 2.0
Sono stati rilasciati, in occasione del convegno di Pisa, i primi due documenti.

Sono stati rilasciati, in occasione del convegno di Pisa, i primi due documenti.

E' in corso la traduzione del terzo ("*The Val IT Framework 2.0*"), il rilascio della quale è previsto per l'ultimo trimestre dell'anno.

Dodicesima edizione Global Information Security Survey Ernst & Young

Ernst & Young, leader mondiale nei servizi professionali, ha annunciato l'avvio della dodicesima edizione della Global Information Security Survey (GISS), consolidata ricerca annuale diventata nel corso degli anni punto di riferimento per la comprensione dei principali driver, trend e sfide inerenti la sicurezza informatica.

Si tratta infatti di una ricerca condotta su scala mondiale (l'edizione 2008 ha coinvolto circa 1400 organizzazioni in più di 50 Paesi) con l'obiettivo di evidenziare come le più importanti aziende, enti pubblici ed organizzazioni no-profit si stanno attrezzando per continuare a garantire un adeguato livello di protezione delle informazioni in linea con le esigenze di business, specialmente in questo momento particolarmente difficile per alcune delle maggiori economie mondiali. La ricerca offre ai partecipanti l'opportunità di confrontare la propria situazione aziendale in materia di sicurezza con quella di aziende similari per dimensioni, fatturato, paese d'appartenenza o settore industriale di riferimento.

La survey 2009 si focalizza su aspetti di governance della sicurezza, organizzazione ed integrazione



con le altre funzioni aziendali, metriche di valutazione, analisi e gestione dei rischi, driver ed attività che guidano la gestione della sicurezza, standard di riferimento e business continuity.

Modalità di partecipazione:
La survey consiste di 35 domande che richiedono circa 45 minuti per la compilazione on line. Nel momento in cui i risultati saranno resi disponibili, tutti i partecipanti riceveranno un documento di sintesi generale dei trend in materia di sicurezza, nonché report personalizzati di comparazione tra la propria situazione ed i trend relativi al settore industriale di riferimento. Il tutto è completamente gratuito ed è gestito in maniera anonima.

Per maggiori informazioni e per partecipare alla survey vi invitiamo ad inviare una e-mail di richiesta all'indirizzo EY.InformationSecurity@it.ey.com

La fase di raccolta dei dati termina il 31 luglio 2009, data entro la quale i questionari devono essere completati.

Prolungato il termine della rilevazione per la Survey KPMG

Per rendere maggiormente significativa la rilevazione e tenendo conto del periodo "festivo" di fine maggio, il termine della survey è stato prolungato. Ricordiamo che la IT Internal Audit Survey in Italia È stata promossa da AIEA e KPMG. Infatti, AIEA e KPMG, a supporto dello sviluppo professionale dei propri associati, stanno programmato una rilevazione sullo stato dell'arte della funzione di IT Internal Audit. La rilevazione interessa un campione rappresentativo dei soci, scelto con un algoritmo che prevede l'individuazione di un solo socio per azienda.

I risultati della rilevazione saranno presentati alla Sessione di Studio organizzata a Milano, il prossimo 8 ottobre, ricorrenza del trentennale della fondazione di AIEA.

Insieme ai dati della rilevazione in Italia, KPMG presenterà i risultati della medesima iniziativa, già svolta a livello europeo.

AIEA sul numero di maggio del Global Communiqué ISACA

A pagina 3 del numero di maggio compare una intera colonna sulle attività svolte, nel 2008, per promuovere il capitolo di Milano nelle Università.

Ricordiamo che il referente di AIEA per le Università è Daniela Bolli, Consigliere AIEA.

Milan Chapter Academic Relations

In 2008, the ISACA Milan Chapter collaborated with the Association of International Education Administrators (AIEA) to promote the chapter to two Italian universities.

The goals for meeting with students at these universities included:

- *Making students aware of IT audit, security and governance topics*
- *Promoting AIEA as a strategic contact point for the job market*
- *Establishing a link between academic, professional and business entities*
- *Promoting AIEA as a knowledge base through its close relationship with ISACA* The first session took place in the first quarter of 2008 at the University of Rome II, with about 40 students who were attending the second year in business administration.

Students appreciated the session as an opportunity to face and, to some extent, discover a new profession, as well as to meet a world different from the academic one.

Subsequent sessions at University of Rome II targeted students attending the final year of schooling in various fields. The interest in those sessions was even higher than the first,



in large part because the focus was on real job opportunities.

The initial session at Florence University also took place in the first quarter of 2008 and involved about 30 students. In the second half of 2008, two more sessions were offered: the first one at the Turin Politecnico (engineering) IT department, with about 50 attendees, and the second at Milan Politecnico, with about 30 attendees. The latter, due to the presence of many foreign students, was held in English.

In all, both students and professors expressed interest in the IT topics presented. Students were mainly interested in ISACA certifications as an opportunity to achieve a formal professional qualification. Professors were interested in exploiting the contact with ISACA and AIEA to broaden their relations and knowledge at an international level. During 2009, the ISACA Milan Chapter plans to maintain the relationships established with these universities, by delivering, as they have requested, more sessions. Plans are also underway to contact other universities.

Riceviamo da Protiviti

In allegato, la Newsletter Protiviti n. 24 dal titolo **“Gestire e comunicare la crisi: un caso di successo”**.

Una crisi aziendale richiede grandi capacità di gestione sotto stress da parte del Management. Gestire una crisi aziendale come se fosse “normale operatività” è un atto i cui effetti potrebbero ripercuotersi all’interno e all’esterno dell’azienda, in un’escalation di eventi di difficile controllo; un’adeguata gestione della crisi può servire, al contrario, a comprendere il contesto in cui si è sviluppata e ad allestire adeguati presidi contro potenziali eventi di rischio.

Protiviti, in questo Insight, presenta l’approccio metodologico di Crisis Management & Communications e analizza un caso reale di successo.

I prossimi eventi di AIEA

Calendario Eventi AIEA

GIUGNO 2009

18..... Torino - Sessione di Studio

LUGLIO 2009

1.....Milano – Assemblea soci



Calendar of Events

Dates of conferences/events are indicated in **RED**; other dates and deadlines are indicated in **BLACK**.

I prossimi eventi ISACA:

June

- 11 June.....Deadline for contributions to volume 3, 2009, of *COBIT Focus*
- 13 June.....CISA, CISM and CGEIT exam administration
- 15-19 June **ISACA Training Week**, Vienna, Austria

July

- 1 July Early-bird registration deadline for the ISACA Training Week, Toronto, Ontario, Canada
- 15 July Early-bird registration deadline for Latin America CACS, San Jose, Costa Rica
- 15 July Early-bird registration deadline for Information Security and Risk Management Conference, Las Vegas, Nevada, USA
- 19-22 July **International Conference**, Los Angeles, California, USA

ISACA Benefit of the month

Member Benefit of the Month: **Listservs/Discussion Forums**

ISACA and the IT Governance Institute® (ITGI™) have established several listservs to enable individuals to find the group most suited to their professional interests. Each of the listservs offers excellent opportunities to share advice, seek assistance and raise pertinent questions. Information on each listserv and how to join is available at www.isaca.org/listserv.

Riceviamo da ISACA **Certification Update**

March Certifications

1,168 CISA certifications, 282 Certified Information Security Manager® (CISM®) certifications and 835 Certified in the Governance of Enterprise IT® (CGEIT®) certifications were awarded in March 2009.



- PRIVACY E DIRITTO D'ISPEZIONE AL LIBRO SOCI: TUTELATI GLI INTERESSI DEGLI AZIONISTI
- E-MAIL E FAX INDESIDERATI: NUOVO STOP DEL GARANTE
- COMUNI, AMMINISTRATORI DI CONDOMINIO E TASSA SUI RIFIUTI
- MIGLIORARE LA PRIVACY: LE AUTORITÀ EUROPEE PRONTE A FARE LA LORO PARTE

Privacy e diritto d'ispezione al libro-soci: tutelati gli interessi degli azionisti

Gli azionisti di una società per azioni hanno diritto di conoscere l'indirizzo e i dati degli altri soci, al fine di contattarli e di poter tutelare i propri legittimi interessi. La legge sulla privacy non limita la conoscibilità da parte degli azionisti dei dati personali contenuti nel libro soci e non si pone in contrasto con la trasparenza dell'attività societaria.

Lo ha chiarito il Garante intervenendo in seguito alla segnalazione di un cittadino cui non erano stati messi a disposizione i dati completi contenuti nel libro-soci dell'azienda di cui deteneva alcune azioni. La decisione dell'Autorità assume particolare rilevanza in particolare per i piccoli azionisti.

L'interessato - in base al diritto d'ispezione garantito dal codice civile (art.2422) - aveva chiesto di consultare e di ottenere copia integrale digitale del libro soci, senza che venissero oscurati gli indirizzi dei soci-azionisti. La richiesta era motivata anche dalla volontà di poter eventualmente convocare l'assemblea e di esercitare i diritti di denuncia previsti dalla legge.

La società aveva invece consentito l'accesso solo ai nominativi contenuti nel libro-soci, ma senza i recapiti, sostenendo di non poter fornire tali informazioni perché esse erano tutelate, in quanto dati personali, dal Codice della privacy. L'azienda aveva peraltro aggiunto a sostegno della sua posizione l'impossibilità di richiedere il necessario esplicito consenso a tutti i quasi 700.000 soci interessati.

L'Autorità, con un provvedimento di cui è stato relatore Giuseppe Chiaravalloti, ha precisato quanto stabilito in un provvedimento adottato nel 2000, affermando che la legge sulla privacy non impedisce affatto al socio, nell'esercizio del suo potere d'ispezione, di poter accedere ai dati personali e agli indirizzi degli altri azionisti e di ottenere estratti del libro soci "a proprie spese". L'accesso a tali informazioni, peraltro, essendo previsto da un preciso obbligo di legge, non richiede il consenso dei soci.

E' stata invece dichiarata inammissibile la richiesta avanzata dall'azionista di ordinare alla società di consentire l'ispezione al libro-soci, dal momento che tale potere non è rimesso al Garante della privacy. Per vedere tutelati tali diritti, l'interessato dovrà infatti rivolgersi all'autorità giudiziaria ordinaria.

E-mail e fax indesiderati: nuovo stop del Garante

Anche se i dati sono estratti dalle Pagine Gialle o dai registri pubblici, quando si usano sistemi automatizzati è obbligatorio acquisire prima il consenso dei destinatari. Continua l'azione del Garante contro lo spamming e il marketing disinvoltato. L'Autorità ha vietato l'ulteriore trattamento illecito dei dati personali a cinque società che inviavano pubblicità tramite fax e posta elettronica senza il preventivo consenso degli interessati.

Il Garante è intervenuto a seguito delle segnalazioni di alcuni utenti che continuavano a ricevere e-mail e fax indesiderati nonostante non avessero mai manifestato alcun consenso all'uso dei loro dati per questo scopo. Lo società coinvolte (due inviavano lo spam tramite posta elettronica, tre tramite fax) in alcuni casi fornivano l'informativa e la richiesta di consenso contestualmente all'invio del primo fax o della prima e-mail che avevano già un contenuto di carattere commerciale.

L'Autorità ha ribadito, invece, che l'uso di sistemi automatizzati per inviare messaggi promozionali, anche quando si tratti di dati estratti da elenchi categorici o da albi, impone la preventiva acquisizione del consenso da parte dei destinatari. Alle cinque società è stato dunque vietato l'ulteriore trattamento illecito dei dati degli utenti interessati, i quali non potranno dunque più essere disturbati. La mancata osservanza del divieto del Garante espone anche a sanzioni penali.

Comuni, amministratori di condominio e tassa sui rifiuti

L'amministratore non gli dà ascolto e al condomino arrivano due cartelle Tarsu. E' accaduto ad un inquilino milanese che, ritenendo scorretto ed arbitrario l'utilizzo dei propri dati personali, è ricorso al Garante per la privacy.

Oggetto della segnalazione il fatto che l'amministratore, trasmettendo agli uffici del Comune il modello contenente la denuncia di "occupazione e detenzione di locali e aree" ai fini del calcolo e del versamento della tassa per lo smaltimento dei rifiuti solidi urbani (c.d. Tarsu) riferito alla sua posizione tributaria, non avrebbe tenuto in debito conto la sua intenzione – comunicata diversi mesi prima – di procedere direttamente a tale adempimento.

L'amministratore, dal canto suo, ha rappresentato all'Autorità di aver svolto lecitamente il trattamento dei dati del condomino in questione, dando esecuzione agli obblighi derivanti dal regolamento comunale, in particolare la compilazione di una scheda riepilogativa recante i totali dei dati raccolti, relativamente alle unità immobiliari del complesso abitativo.

Il Garante, pur riconoscendo l'effettiva liceità del trattamento posto in essere dall'amministratore, ne ha contestato il mancato rispetto del principio di correttezza. Se l'amministratore, infatti, avesse avuto cura di verificare che la dichiarazione del condomino era effettivamente già stata resa ai competenti uffici del Comune avrebbe evitato i disagi poi effettivamente verificatisi.

Il Garante ha dunque prescritto all'amministratore di porre in essere, prima di espletare le procedure relative procedure di calcolo delle tasse, ogni scrupolosa verifica delle denunce già effettuate da parte degli occupanti dello stabile amministrato.

Migliorare la privacy: le Autorità europee pronte a fare la loro parte

Alla recente conferenza europea delle Autorità di protezione dati di Edimburgo (23-24 aprile), i riflettori sono stati puntati sulla capacità del quadro attuale di norme e meccanismi di regolazione di fare fronte alle nuove "sfide" tecnologiche e globali. Significativi i risultati raggiunti.

- Nella Dichiarazione finale i Garanti hanno affermato con forza il patrimonio di esperienza e conoscenza che l'Europa può e deve apportare alla ricerca di soluzioni ed approcci sempre più condivisi per garantire la tutela dei dati personali a livello mondiale. La Dichiarazione

sottolinea, in proposito, la necessità di guardare ai molti punti in comune che già contraddistinguono il quadro normativo europeo e internazionale. Ma soprattutto invita i soggetti coinvolti, pubblici privati e istituzionali, a lavorare per mettere a punto norme e standard che - a partire dai principi di protezione dati già affermati - siano in grado di garantire e promuovere i diritti e le libertà fondamentali; di sviluppare nelle tecnologie approcci che prevedano la privacy come elemento essenziale ("privacy by design"); di realizzare una efficace protezione dei dati personali guardando in particolare ai rischi per i singoli e per la società nel suo complesso.

- E' stata adottata anche una Risoluzione sugli accordi bilaterali e multilaterali stipulati fra Paesi europei e non-europei per quanto riguarda la cooperazione giudiziaria e di polizia in materia penale (il cosiddetto "III Pilastro"). Considerata l'esistenza di troppe difformità nelle garanzie fissate da tali accordi per quanto riguarda la protezione dei dati, i Garanti chiedono agli Stati di garantire livelli uniformi di tutela anche attraverso l'inserimento di clausole-standard concernenti la protezione dei dati personali.

- La Conferenza di Edimburgo ha anche confermato a capo del Gruppo di lavoro europeo in materia di cooperazione giudiziaria e di polizia (WPPJ), per un successivo mandato di altri due anni, il presidente dell'Autorità italiana, Francesco Pizzetti. La Conferenza ha infine adottato il "manuale" elaborato dal Gruppo per definire alcuni criteri applicabili alle attività di ispezione e monitoraggio concernenti la materia del III Pilastro.

L'attività del Garante. Per chi vuole saperne di più Gli interventi e i provvedimenti più importanti recentemente adottati dall'Autorità

Misure in materia di propaganda elettorale - Esonero dall'informativa - provvedimento del 2.4.2009 (G.U.n. 85 dell'11 aprile 2009)

Conferenza dei Garanti europei a Edimburgo - Comunicato del 22.4.2009

Pizzetti: migliorare e rendere più effettiva la protezione dei dati dei cittadini europei - Comunicato del 23.4.2009

Pizzetti confermato presidente del gruppo di lavoro dei garanti europei sulla cooperazione giudiziaria e di polizia - Comunicato del 27.4.2009

NEWSLETTER

del Garante per la protezione dei dati personali
(Reg. al Trib. di Roma n.258 del 7/6/99).
Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.
Tel: 06/69677751 - Fax: 06/69677755. *Newsletter* è consultabile sul sito Internet www.garanteprivacy.it



- INFORMAZIONE SCORRETTA AL TEMPO DI FACEBOOK
- BIGLIETTI ON LINE, PRIVACY PIÙ GARANTITA
- SANITÀ: SISTEMA INFORMATIVO PER LE DIPENDENZE E PRIVACY
- VIDEOSORVEGLIANZA ED ESIGENZE DI SICUREZZA

Informazione scorretta al tempo di Facebook

I giornalisti che utilizzano notizie, fotografie e dati personali tratti dai social network devono sempre verificare le informazioni raccolte per esercitare con correttezza il diritto di cronaca.

E' quanto ha ribadito il Garante intervenendo su segnalazione di due cittadini, i quali avevano visto pubblicata da alcuni quotidiani la propria immagine presa da Facebook erroneamente associata a persone omonime decedute. In un caso si trattava di un incidente stradale, nell'altro di una vittima del terremoto avvenuto in Abruzzo.

I nomi pubblicati nei servizi di cronaca erano corretti, ma le fotografie ad essi associate erano state trovate facendo una semplice ricerca su Internet e scaricando l'immagine presente nei profili che i due segnalanti avevano aperto nel famoso social network. I giornalisti non avevano, dunque, verificato l'ipotesi che si potesse trattare di semplici casi di omonimia e hanno dato per decedute le persone sbagliate. Nel caso della vittima del terremoto, la fotografia errata, pubblicata da un quotidiano, era stata riproposta anche da due testate televisive nazionali.

Queste immagini - ha stabilito il Garante, con due provvedimenti di cui è stato relatore Mauro Paissan - non dovranno essere più pubblicate, diffuse né riproposte nell'archivio on-line delle testate coinvolte.

Associando l'immagine di una persona all'identità di un'altra, sono stati diffusi dati errati, mettendo in atto in tal modo un illecito trattamento dei dati personali.

Il Garante ha, pertanto, vietato alle testate, due locali e tre nazionali, di diffondere ulteriormente le fotografie dei segnalanti. L'Autorità ha imposto la cancellazione delle immagini anche dal sito web e dall'archivio storico on-line di uno dei quotidiani interessati che - dopo aver informato seppur tardivamente i lettori dello sbaglio commesso - continuava a rendere comunque accessibile da Internet la fotografia pubblicata per errore.

Biglietti on line, privacy più garantita

Il consenso all'uso dei dati non deve mai essere condizionato

Il consenso all'uso dei nostri dati non può mai essere condizionato, ma libero e consapevole. Non si può negare un servizio richiesto a chi non vuole sottoscrivere un modulo in cui non viene garantita la libertà del consenso. E' per questo motivo che il Garante ha vietato ad una società che opera su Internet l'ulteriore trattamento dei dati personali dei clienti.

La società, specializzata nella vendita on line di biglietti per eventi musicali, teatrali, sportivi e culturali, al momento della registrazione sottoponeva ai clienti un modulo che non permetteva di prestare un consenso specifico e differenziato. Era presente infatti una sola casella, per giunta già contrassegnata con l'apposito segno di "spunta". In questo modo i clienti oltre a dare il consenso all'uso dei propri dati personali, indispensabile per poter usufruire del servizio, lo prestavano automaticamente anche per le finalità di marketing. Chi non sottoscriveva il modulo così com'era non riceveva il servizio.

Intervenuto a seguito della segnalazione di un cittadino, il Garante ha vietato alla società l'ulteriore trattamento dei dati illegittimamente acquisiti, disponendo, inoltre, la riformulazione del modulo di iscrizione al sito con l'obbligo di fornire ai clienti la possibilità di prestare consensi differenziati.

"Il consenso che noi diamo all'uso dei nostri dati non può mai essere condizionato, ma deve poter essere espresso liberamente e in maniera consapevole - ha commentato il relatore del provvedimento, Giuseppe Fortunato - Non si possono imporre scelte ai clienti e ai consumatori o chiedere un consenso generico per usi diversi. Non si può negare un servizio o una prestazione a chi non vuole fornire i propri dati per finalità di marketing".

Sanità: sistema informativo per le dipendenze e privacy

Maggiore protezione per i dati di tossicodipendenti e alcolisti che si sottopongono a programmi di recupero socio-sanitari: elevate misure di sicurezza dei flussi di dati e delle reti telematiche, uso di dati anonimi quando non sia possibile ricorrere a codici, selettività e tracciabilità degli accessi.

E' un sì condizionato quello che il Garante privacy ha reso al Ministero del lavoro, della salute e delle politiche sociali sullo schema di decreto che istituisce il sistema informativo per le dipendenze (Sind). regioni e province autonome mettono a disposizione del Sind informazioni relative a strutture, attività e personale dei servizi che si occupano delle dipendenze. Tra gli obiettivi che si intendono raggiungere mediante il Sind, il monitoraggio dell'attività dei servizi, del volume delle prestazioni, delle caratteristiche dell'utenza e la valutazione del grado di efficienza e di utilizzo delle risorse.

Nel parere l'Autorità chiede innanzitutto che nel decreto siano indicate con maggiore precisione le finalità che si intendono perseguire e che giustificano la raccolta dei dati. Il Garante chiede, poi, che le regioni e le province autonome che non sono in grado di rendere non direttamente identificabili i pazienti (perché non dispongono di sistemi di codifica) utilizzino solo dati anonimi. Nello schema dovranno essere inoltre specificati gli uffici e il personale del ministero, delle regioni e delle province cui è consentito il trattamento delle informazioni e che il Ministero potrà avere accesso all'insieme delle informazioni raccolte nel Sind, mentre regioni e province potranno trattare solo le informazioni che inseriscono. Particolare attenzione deve essere inoltre posta nel caso in cui persone tossicodipendenti abbiano chiesto di mantenere l'anonimato nei rapporti con i servizi sanitari. Per innalzare ulteriormente le garanzie per i pazienti il Garante ritiene necessario che lo schema sia integrato con indicazioni mirate in materia di sicurezza: in particolare, perfezionando la disposizione che prevede il ricorso a tecniche di cifratura dei dati sensibili e prevedendo il tracciamento delle operazioni di accesso al sistema dedicato alla memorizzazione dei dati. Dovranno essere infine individuate modalità per la distruzione sicura dei supporti (hard disk, cd etc.) che contengono dati sensibili.

Videosorveglianza ed esigenze di sicurezza

Nei musei di Napoli le telecamere potranno conservare le immagini più a lungo

Il polo museale napoletano potrà conservare per trenta giorni le immagini raccolte da sistemi di videosorveglianza installati presso alcune aree museali,

fino a che permangono specifiche e comprovate esigenze di sicurezza.

Lo ha stabilito il Garante per la protezione dei dati personali che ha accolto la richiesta della Soprintendenza campana di poter prolungare, nel rispetto dei principi generali che regolano l'installazione e la gestione di sistemi di videosorveglianza, il tempo di conservazione delle immagini delle riprese video in alcuni musei. La Soprintendenza si era attivata in seguito all'allerta per un sopraggiunto allarme terroristico, inoltrata dal Comando dei carabinieri-tutela del patrimonio culturale. Al fine di prevenire eventuali attentati, l'Arma dei carabinieri aveva quindi suggerito di rimodulare il piano di sicurezza predisposto per la tutela e la conservazione delle opere, aumentando anche il tempo di conservazione delle immagini registrate dagli impianti di videosorveglianza. In base ai principi generali indicati nel Codice della privacy e nel provvedimento generale sulla videosorveglianza del 2004, le immagini e i dati relativi a persone identificate o identificabili possono essere conservate per un periodo limitato. Tale limite, tuttavia, può essere modificato in relazione alla necessità eccezionale derivante da un evento accaduto o realmente imminente, o in seguito alla richiesta dell'autorità giudiziaria o della polizia, motivata da un'attività investigativa in corso.

Il Garante, con un provvedimento di cui è stato relatore Giuseppe Chiaravalloti, ha quindi autorizzato la Soprintendenza a conservare sino a trenta giorni le riprese dei sistemi di videosorveglianza dei siti museali più esposti al rischio terrorismo, evidenziando però che il permesso temporaneo continuerà a valere solo nel caso in cui persistano comprovate esigenze di sicurezza.

L'attività del Garante. Per chi vuole saperne di più

Gli interventi e i provvedimenti più importanti recentemente adottati dall'Autorità

Conservazione dei dati di traffico: proroga dei termini - 29 aprile 2009 - provvedimento del 2.4.2009 (G.U. n. 107 dell' 11 maggio 2009)

Niente più nomi dei medicinali sullo scontrino fiscale rilasciato dalle farmacie - Comunicato del 7.5.2009

"Social Network: attenzione agli effetti collaterali" - Opuscolo informativo del Garante - 11.5.2009

Pazienti Udine su Facebook: il Garante privacy ha avviato accertamenti - Comunicato del 14.5.2009

NEWSLETTER

del Garante per la protezione dei dati personali
(Reg. al Trib. di Roma n.258 del 7/6/99).
Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.
Tel: 06/69677751 - Fax: 06/69677755. Newsletter è consultabile sul sito Internet www.garanteprivacy.it



Insight

N. 24 – Maggio 2009

Gestire e comunicare la crisi: un caso di successo

Il termine “crisi” suggerisce istintivamente un momento, nella vita di una persona o di un’azienda, dalle conseguenze non prevedibili e generalmente sfavorevoli.

Tuttavia, da un punto di vista etimologico, “crisi” indica una “separazione”, un “momento di svolta” (dal greco *krisis*) e in questo senso sottolinea non il momento specifico del suo manifestarsi, ma il cambiamento che fenomeni di questo tipo sono in grado di determinare.

Nella fase storica che stiamo vivendo, “crisi” è uno dei termini più ricorrenti nei media e nell’opinione pubblica, in riferimento all’impatto economico-finanziario che essa sta esercitando a livello globale.

Accanto a questo significato ne esiste un altro, ed è quello che qui ci interessa, applicato al ciclo di vita del business di un’azienda, per il quale una crisi va intesa come “evento o serie di eventi che possono generare un impatto significativo sulla continuità del business o sulla reputazione dell’azienda e/o dei propri marchi e prodotti”.

Le due definizioni sono strettamente connesse: è infatti vero che una crisi a livello globale può ripercuotersi a cascata sulle singole realtà; ed è vero anche l’opposto, cioè che crisi di singole aziende (si vedano ad esempio i casi Enron e Worldcom) possono imporre l’adozione di provvedimenti per l’intero mercato, e non solo per la specifica azienda coinvolta.

Nel presente contesto economico e finanziario le tematiche legate al Crisis Management & Communication sono di grande attualità: lo scenario è quello di aziende coinvolte in riorganizzazioni aziendali, riduzioni del personale, chiusure di sedi o dismissioni di stabilimenti.

Queste iniziative vanno considerate e gestite sia in termini di impatti sui processi interni, sia in quanto fonti di possibili conflitti con dipendenti o altri stakeholder e richiedono pertanto di identificare i rischi e definire le migliori strategie per mitigare le conseguenze sul business.

In scenari come quelli descritti, l’adozione di un piano di Crisis Management & Communication si dimostra determinante per il contenimento dei possibili impatti, fornendo inoltre l’occasione per l’analisi e la revisione dei processi interni alle aziende, nell’ottica di una maggiore robustezza rispetto a eventi che ne possano compromettere la continuità.

Una crisi aziendale è forse il momento nella vita di un’azienda che richiede le più grandi capacità di gestione sotto stress da parte del Management.

Gestire una crisi aziendale come se fosse “normale operatività” è un atto i cui effetti potrebbero ripercuotersi sull’azienda e al suo esterno in un’escalation di eventi di difficile controllo.

Al contrario, un’adeguata gestione della crisi fornisce elementi essenziali sia per la comprensione del contesto esistente, sia per allestire adeguati presidi contro potenziali eventi di rischio.

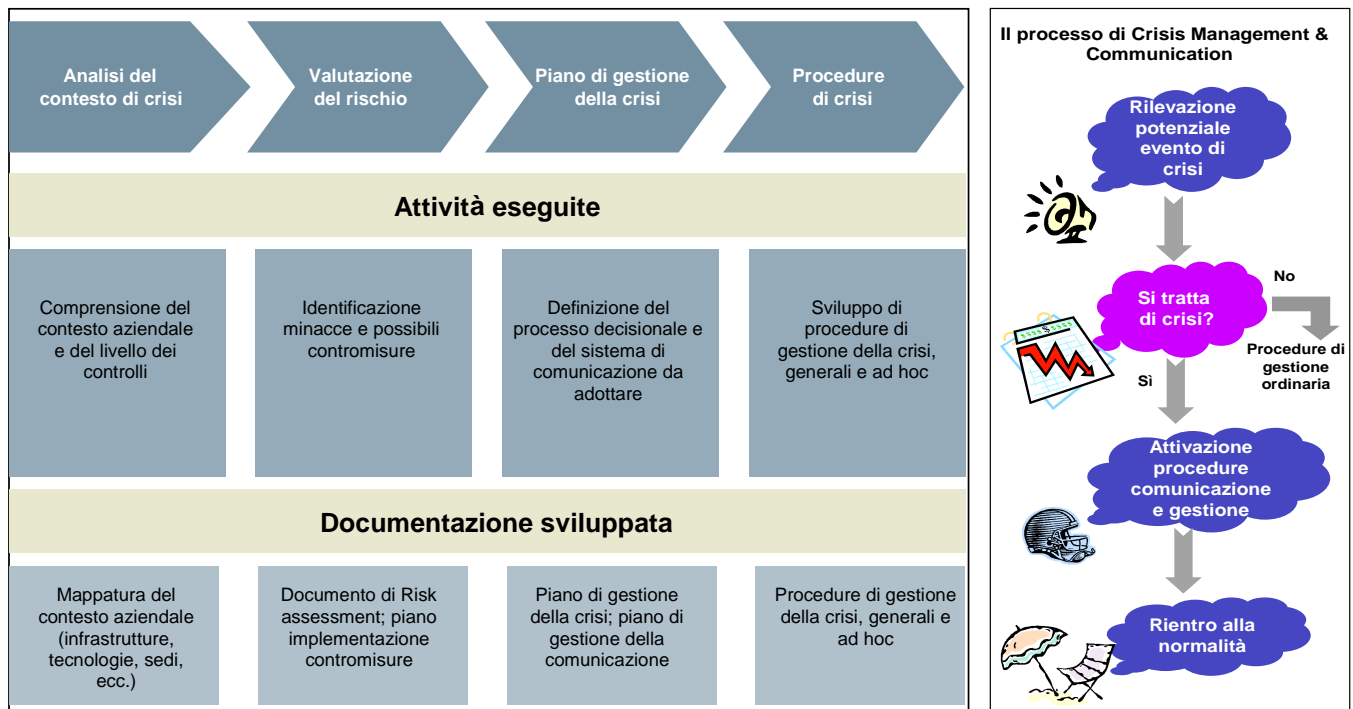
Una metodologia efficace di gestione della crisi deve prevedere un approccio integrato, che non ne isoli singole componenti per implementare contromisure discontinue, ma che concepisca la gestione della crisi come un processo, i cui elementi interagiscono strettamente e contribuiscono alla sopravvivenza e continuità dell’azienda.

L'approccio al Crisis Management & Communication

L'obiettivo primario di una soluzione di Crisis Management & Communication è la definizione e lo sviluppo dei meccanismi per affrontare e governare il contesto di crisi e, in particolar modo, identificare e ridurre i potenziali impatti negativi sul business e prevenire o limitare i danni a persone e beni.

In tale ambito anche la comunicazione riveste un ruolo importante ed è necessario definire i protocolli più efficaci per comunicare a tutti gli stakeholder coinvolti, con l'obiettivo di fornire istruzioni o rassicurazioni e proteggere gli asset e la reputazione dell'azienda.

Una soluzione di Crisis Management & Communication deve fare i conti con contesti dinamici, in cui gli scenari possono sovrapporsi e di conseguenza moltiplicare reciprocamente i possibili effetti. Da ciò consegue la necessità di un approccio che non consideri in modo isolato il singolo episodio, ma che affronti in modo organico tutti i fenomeni, prima in un'ottica di contenimento e quindi di miglioramento continuo. Un approccio metodologico coerente con questa esigenza prevede gli elementi sotto riportati:



Nel dettaglio:

Analisi del contesto di crisi

Comprensione del contesto aziendale: organizzazione, processi, infrastrutture, tecnologie e livello dei controlli in essere (ad esempio, il grado di sicurezza fisica).

Valutazione del rischio e identificazione delle contromisure

Identificazione delle minacce rispetto alla continuità dei processi aziendali, valutate in termini di probabilità di accadimento e gravità dell'impatto. Attraverso l'identificazione delle contromisure, per ogni rischio sono definite le azioni preventive e correttive e il relativo effetto di mitigazione. E' fondamentale in questa fase identificare tutte le misure che possono essere messe in atto per prevenire il verificarsi di situazioni di crisi, o contenerne preventivamente l'estensione e gli effetti.

Piano di gestione della crisi

Definizione del processo decisionale e del sistema di comunicazione da adottare nel corso della crisi. Il piano si basa sull'identificazione di una serie di scenari rispetto ai quali si sviluppano le procedure di gestione e comunicazione. In particolare, nel piano sono definiti:

- il comitato di gestione della crisi (Crisis Management Team - CMT), ossia il gruppo di persone dotate di potere decisionale e di coordinamento. Il gruppo è generalmente costituito da alcuni componenti permanenti, più altri designati ad hoc, a seconda del fenomeno in corso. Al fine di conseguire agilità e autonomia decisionale, il CMT dovrebbe essere costituito da un numero limitato di rappresentanti del Top Management;
- il sistema di governo del processo di Crisis Management & Communication, in termini di gestione del processo decisionale e di comunicazione, di identificazione degli eventi critici e delle corrispondenti linee guida per la gestione. In altri termini, per ogni evento identificato, sono specificati ruoli, responsabilità, azioni ed eventuali raccomandazioni;
- la gestione della comunicazione, che mira a governare il processo comunicativo durante la crisi. Ne sono componenti centrali, ad esempio, le procedure per la comunicazione, i template di comunicati e le Domande & Risposte per gestire i rapporti con i media, le autorità, i sindacati e le linee guida per il press monitoring.

Procedure di crisi

Sviluppo di procedure, generali e ad hoc, per gestire gli eventi di crisi e le relative contromisure, come, ad esempio, la gestione della produzione o l'erogazione dei servizi in situazione di emergenza o di controllo degli accessi del personale agli impianti o alle sedi. Le procedure sono richiamate all'interno del piano di gestione della crisi.

Data l'estensione degli impatti che una crisi può determinare, essa deve essere gestita attraverso competenze trasversali e un approccio multidisciplinare.

Le competenze richieste, finalizzate all'individuazione delle opportune contromisure, sono di varia natura e riguardano competenze specifiche della soluzione di Crisis Management & Communication quali:

- **gestione del rischio;**
- **gestione della continuità operativa;**
- **sicurezza fisica e degli accessi;**
- **sicurezza logica;**
- **gestione della comunicazione e coaching.**

Accanto a queste specifiche competenze, vanno annoverate anche quelle riguardanti aspetti generali, di business o di altra natura, che possono essere richieste a seconda dei contesti di crisi che si analizzano:

- **processi di business dell'azienda;**
- **gestione del personale;**
- **sicurezza sul lavoro;**
- **competenze legali.**

Il Crisis Management & Communication è una delle componenti del Business Continuity Management, ovvero dell'insieme di soluzioni per proteggere i processi critici di un'azienda da eventi che ne

potrebbero interrompere l'operatività, esponendola di conseguenza a danni rilevanti.



Nell'ambito del Business Continuity Management, il Crisis Management & Communication costituisce il primo passo per il ripristino dell'operatività aziendale. Accanto ad esso troviamo:

- **Business Resumption Planning, mirato al ripristino delle funzioni e dei processi critici per l'operatività del business;**
- **IT Disaster Recovery Planning, mirato al ripristino degli asset critici ICT (applicazioni, sistemi, reti di telecomunicazioni).**

Data la complessità della tematica e gli impatti sull'organizzazione, non è possibile fronteggiare una crisi attraverso interventi puntuali e discontinui. L'assenza di una strategia in questo senso rappresenta una limitazione che costituisce una delle principali fonti di rischio.

L'analisi degli scenari e la determinazione delle procedure per gestirli deve essere effettuata in modo preventivo, poiché al momento della crisi spesso non si possiedono la necessaria lucidità e il tempo richiesto per affrontare coerentemente gli eventi.

Una compagnia statunitense su 4 ha dichiarato di avere attraversato un “disastro” negli ultimi 5 anni.

Su 5 aziende colpite da un disastro esteso, 2 non sono in grado di riavviare l'attività; 1 riesce a riavviare l'attività, ma fallisce entro due anni.

(fonte: Contingency Planning & Management Magazine)

Dopo l'attacco dell'11 settembre, il 70% delle aziende coinvolte e prive di piani di gestione della continuità operativa è fallito.

(fonte: SEC – Security Exchange Commission)

Un caso reale

A causa di spinte congiunturali e difficoltà legate al mercato, un'azienda manifatturiera ha rivisto le proprie strategie, decidendo di chiudere uno dei siti produttivi e riassorbire la capacità produttiva nei restanti.

Tale ristrutturazione avrebbe potuto configurarsi come contesto di crisi qualora le reazioni da parte dei dipendenti e delle aziende collegate avessero minacciato la continuità del business o l'immagine dell'azienda.

I dipendenti dell'azienda (e delle aziende ad essa collegate) costituivano la principale fonte di rischio, in quanto avrebbero potuto organizzare scioperi e dimostrazioni tali da bloccare la produzione o la distribuzione, con conseguenti ripercussioni economiche (nel caso peggiore, la perdita di clienti).

Ancora, avrebbero potuto verificarsi episodi di danneggiamento verso cose o persone, o incidenti dovuti alla negligenza nella manutenzione dei macchinari, nonché ad atti di sabotaggio.

Ci si potevano attendere reazioni da terze parti (da un lato clienti e fornitori, dall'altro sindacati, istituzioni locali, clienti, media, etc.), che miravano a scendere in campo per influenzare la decisione presa dall'azienda ed evitare la chiusura dell'impianto.

Un'ulteriore fonte di rischio era legata alla possibilità di danneggiamento o furto della documentazione relativa ai contratti con i clienti, che avrebbe potuto

fornire ai competitor importanti informazioni commerciali.

Senza la definizione e implementazione di adeguati presidi, l'escalation di questi eventi avrebbe potuto essere ingovernabile. Si veda in merito la figura sottostante, che mostra con un esempio di come lo scenario di crisi possa generare nuovi elementi di crisi, se non sono predisposti adeguati interventi.

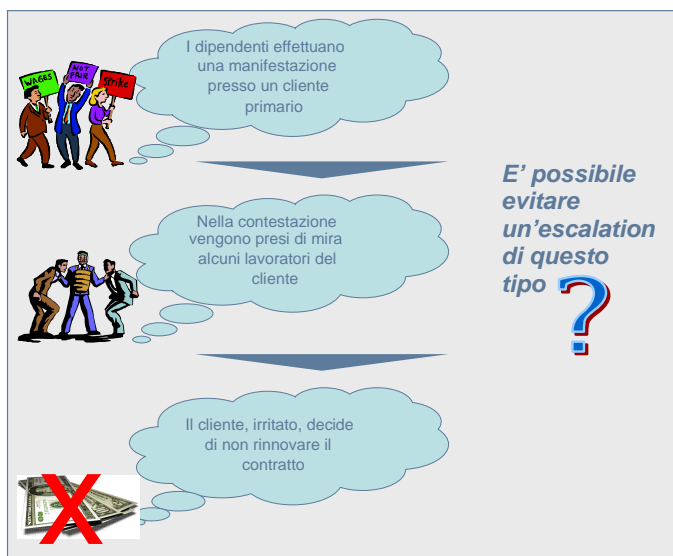
Il team Protiviti specializzato sulla tematica Crisis Management & Communication è stato coinvolto per analizzare la situazione e disegnare possibili interventi. Poiché al momento dell'avvio delle attività la decisione aziendale non era stata ancora annunciata, Protiviti ha adottato tutte le misure necessarie a garantire la totale segretezza circa gli obiettivi e l'ambito del mandato.

Il team coniugava competenze metodologiche sulle tematiche di Crisis Management & Communication, quali:

- **framework di Risk Assessment e Crisis Management**
- **Business Continuity Management**
- **comunicazione**

con competenze più specialistiche, quali

- **sicurezza fisica in impianti industriali**
- **supporto legale.**



Come si può comunicare durante la crisi senza far salire la tensione?

Come si dovrebbe affrontare un'occupazione dei dipendenti?

Qual è il modo migliore per rispondere alle provocazioni di un giornalista?

Come si può evitare la diffusione di informazioni riservate?

Come si possono limitare i danni all'immagine aziendale?

L'intervento consulenziale ha previsto innanzitutto la definizione del contesto di crisi e delle sue possibili conseguenze, attraverso una serie di interviste e riunioni con il management.

A seguire, sono state svolte alcune visite ai siti produttivi e ai centri direzionali, per valutare i rischi e il livello dei controlli esistenti.

Sulla base di questa analisi, Protiviti ha sviluppato il Piano di Gestione della Crisi indirizzando i seguenti elementi:

- l'identificazione delle **contromisure preventive** per mitigare i rischi rilevati (accordi con fornitori e partner commerciali per gestire discontinuità nella produzione e nella logistica, identificazione delle potenziali integrazioni ai sistemi di sorveglianza degli impianti, modalità di gestione della manutenzione degli impianti per prevenire sabotaggi, etc.);
- la definizione del **Crisis Management Team**;
- la determinazione del **flusso informativo** per la gestione della crisi;

- la definizione delle linee guida per la **gestione della comunicazione** (identificazione dei Key Message e delle principali Question & Answer, definizione dei template per i comunicati, predisposizione di press release);
- l'identificazione dei **potenziali eventi di crisi** e, per ciascuno di essi, le linee guida da seguire (modalità per gestire la produzione e la logistica, requisiti per il servizio di vigilanza ed identificazione del fornitore, gestione del customer service);
- le **procedure operative** (in particolare, la procedura per la vigilanza ed il controllo degli accessi) e la procedura per la protezione della documentazione commerciale.

In chiusura dell'intervento, Protiviti ha erogato una sessione di **formazione per il Management** del cliente, mirata allo sviluppo e all'affinamento delle tecniche e modalità di comunicazione.

* * *

Per maggiori informazioni, rivolgetevi all'ufficio Protiviti più vicino o a Enrico Ferretti (enrico.ferretti@protiviti.it – 06 42049801) e Giuseppe Blasi (giuseppe.blasi@protiviti.it - 02 65506301).

Global COMMUNIQUÉ



ISACA Unveils Evolved Strategy

All members and certification holders will receive a brochure outlining the strategy, resulting from the recent market study undertaken. Members can immediately access the brochure at www.isaca.org/strategy. The research was undertaken while recognizing ISACA's strengths and its challenges within a shifting marketplace and evolving constituency base. The study and strategy initiative were prompted by a desire to stay ahead of the curve.

As noted by International President Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, "...in today's world, events and the environment are always changing, and if the organization does not change as well, it can quickly find itself behind the times.

The strategy was designed to address a vision and mission built on the following basic tenets: **5. RESEARCHERS AND ORGANIZATIONS** must realize value from information systems, and they must realize value from them. Trust and value are the outcomes of members' endeavors.

3. #! HAS A GLOBAL LEADERSHIP POSITION TO BUILD ON that reputation for knowledge, certifications, community, advocacy and education.

3. #! FOCUSES ON CERTAIN SPACES—information systems assurance and security, enterprise governance of IT, and IT-related risk and compliance.

Although the specific wording of the vision and mission may still be in draft stage, the concepts are clear. The initiatives outlined in the strategy reinforce each other and support the mission and

vision, and are grouped within five major strategic themes:

1. Realize full potential of COBIT®. COBIT is widely known and adopted, giving it a leadership position and favorable reputation. ISACA will create new intellectual property and incorporate existing IP under the COBIT umbrella through an open source model. Volunteers will drive development of COBIT levels 3 and 4 controls material.

2. Enhance commitment to the core constituency of IT audit and controls. To address constituents' evolving need for

Continued on page 3

Inside This Issue

MAY 2009, VOLUME 5

- ISACA Unveils Evolved StrategyPage 1
- New Web Site Features Help Members Stand Out in a Tough EconomyPage 1
- President's Message.....Page 2
- Distance Learning.....Page 2
- Chapter Spotlight: Milan Chapter Academic RelationsPage 3
- Notice of the 2009 Annual Meeting of ISACAPage 4
- Report of the Nominating CommitteePage 4
- Global Events.....Page 5
- ISACA Looks Back: 1983-1986Page 6
- What's New at the BookstorePage 6
- Certification Update.....Page 7
- Highlights of March 2009 Board MeetingsPage 7
- Conference Q&A: 2009 International ConferencePage 8
- Conference and Education Update.....Page 9
- Using Technology to Cut In-house Fraud Off at the PassPage 10
- Research Q&A: COBIT and Application Controls.....Page 11
- Research News.....Page 11
- 2009 ISACA Calendar of Events.....Page 12

New Web Site Features Help Members Stand Out in a Tough Economy

In April 2009, ISACA launched a new web section called Stay Competitive—Stand Out for Your Enterprise is a quick summary sheet of the top five reasons to invest in employees. As part of ISACA's response to the global economy, five new member services have been developed to help members succeed in challenging times:

sNEW COBIT discounts—Members get COBIT® Quickstart free as part of their membership and 75 percent off the full subscription to COBIT Online—a US \$150 value.

sNEW e-Library—For instant, self-directed learning, reference and support, members will soon be able to access an on-demand, customized collection of ISACA and third-party books, videos and other resources in a fully searchable, web-based environment powered by Books24x7.

sNEW Career Centre enhancements—The Career Centre will include more jobs, including those posted on other job boards, and more robust tools for job seekers. Coming soon, a free job board for freelancers will be available. Members will be able to post freelance/contract positions free of charge for other members to view and pursue.

sNEW employer handout—Ensure Success for Your Enterprise is a quick summary sheet of the top five reasons to invest in employees. As part of ISACA's response to the global economy, five new member services have been developed to help members succeed in challenging times:

sNEW free CPE table—This handy new reference itemizes 52 free continuing professional education (CPE) credits available from ISACA for certified members.

ISACA International President Lynn Lawton offers three reasons for this new web section: to help members keep a competitive edge in their current market, to help members take their next professional steps while in transition and to help members ensure the success of their enterprises. The new web section can be accessed from the ISACA web site home page or at www.isaca.org/standout. Take a look today!

