



Associazione Italiana
Information Systems Auditors



Si avvicina il 2009.....

e con esso il calendario degli eventi AIEA. La messa a punto del calendario e, soprattutto, del contenuto dei singoli eventi (Sessioni di studio, Convegno, Corsi...) è una fase importante. Ed è anche importante che, in questa fase, collaborino i soci, con i loro suggerimenti, con le loro disponibilità a supportare le attività, con le indicazioni di possibili argomenti di interesse.

Ricordiamo, anche, che entro il 31 dicembre 2008 deve essere rinnovata l'iscrizione all'Associazione. Sul sito sono disponibili le informazioni per il rinnovo che, da quest'anno ed in accordo a quanto ci ha chiesto ISACA, dovrà essere fatto direttamente ad ISACA

Riceviamo da E&Y

Ricerca internazionale Ernst & Young Global Information Security Survey 2008

Potenziali danni al brand e alla reputazione aziendale favoriscono gli investimenti in Information Security

Ernst & Young, leader mondiale nei servizi professionali, ha annunciato i risultati dell'undicesima edizione annuale del Global Information Security Survey, che ha coinvolto circa 1.400 senior executive di aziende appartenenti a tutti i principali settori economici operanti in oltre 50 paesi, tra cui una trentina a livello italiano, per esaminare come la sicurezza informatica sia attualmente affrontata e gestita.

L'indagine, intitolata "Moving beyond compliance", ha rilevato che sempre più organizzazioni riconoscono l'esistenza di una relazione fra la sicurezza delle informazioni e la reputazione e solidità del proprio marchio. La maggior parte dei soggetti coinvolti ritiene che un incidente legato alla sicurezza produrrebbe un impatto sulla reputazione e sul marchio dell'azienda di gran lunga maggiore che non sul fatturato. Tale risultato è ampiamente confermato anche a livello italiano, con ben il 90% degli intervistati che è preoccupato dalla potenziale perdita di immagine derivante da problemi collegati alla sicurezza delle informazioni.

Nonostante un momento particolarmente difficile per alcune delle maggiori economie mondiali, è emerso come le aziende prevedano un incremento degli investimenti dedicati alle soluzioni per la sicurezza e come sempre più organizzazioni stiano adottando standard di sicurezza internazionali.

Il 50% degli intervistati ha asserito infatti di prevedere un incremento degli investimenti nell'ambito Information Security nel prossimo futuro, mentre solo il 5%, diminuirà i budget attuali. Particolarmente positivo è il dato italiano con solo il 3% degli intervistati che prevede una riduzione del budget dedicato alla sicurezza informatica.

Inoltre il ricorso all'utilizzo di terze parti e all'outsourcing è in aumento, e le aziende si stanno muovendo in questo senso per adottare alcune misure focalizzate alla salvaguardia delle informazioni, anche se molto resta ancora da fare. Solo il 45% delle imprese intervistate prevede specifici requisiti per la sicurezza delle informazioni nei contratti stipulati con terze parti, mentre quasi un terzo non verifica o non valuta il modo in cui i contraenti tutelano le proprie informazioni. La situazione italiana



Associazione Italiana
Information Systems Auditors



è simile a quella mondiale, con solo il 42% degli intervistati che adotta adeguate misure contrattuali per la protezione dei dati.

Lo studio completo è disponibile su richiesta all'indirizzo e-mail EY.InformationSecurity@it.ey.com

La survey è stata presentata e distribuita in cartaceo durante la sessione di Roma dell'11 novembre u.s.

Riceviamo da CNIPA

CNIPA annuncia la pubblicazione sul sito www.cnipa.it, della versione definitiva dell'ottavo manuale delle Linee Guida "Analisi di Fattibilità per l'acquisizione delle forniture ICT".

Il documento è disponibile su
http://www.cnipa.gov.it/site/it-IT/Attivit%c3%a0/Qualit%c3%a0_delle_forniture_ICT/Manuali/Analisi_fattibilit%c3%a0_forniture_ICT/

E' stata, inoltre, pubblicata, con lievi modifiche rispetto la bozza precedente, la versione definitiva dell'VIII Manuale delle Linee guida sulla la qualità dei beni e servizi ICT: "Analisi di fattibilità per l'acquisizione delle forniture ICT". Il manuale si concentra sulla chiarificazione degli obiettivi, delle caratteristiche e delle modalità di realizzazione di uno studio di fattibilità. Nel manuale sono identificate e commentate specificatamente le varie fasi lungo le quali uno Studio di Fattibilità dovrebbe svolgersi, secondo la struttura di seguito riportata: dall'esame della situazione attuale al progetto di massima della soluzione; dall'analisi del rischio alla valutazione del rapporto costi-benefici; dalla gestione del cambiamento alle raccomandazioni per le fasi realizzative.

AIEA partecipa

Nell'ambito del Security Summit che sarà organizzato a marzo, a Milano, dal CLUSIT, AIEA organizzerà una propria Sessione di Studio. Dal 2009 Security Summit sostituirà Infosecurity Forum. Sempre in tale manifestazione il nostro Presidente parteciperà ad una sessione del percorso formativo "Gestione della sicurezza informatica". Il tema della sessione sarà "Quali requisiti professionali sono necessari per chi si occupa di sicurezza ICT in azienda". L'intervento di AIEA sarà focalizzato sulle certificazioni ISACA

Esame CISA e CISM 13 dicembre 2008

Stanno proseguendo i corsi, organizzati da AIEA, sia a Roma che a Milano. Ai soci che affronteranno l'esame, i nostri migliori auguri.

Gruppi di ricerca

Gruppo di Lavoro "Business Continuity"

Manca ancora un capitolo da terminare, ma che è quasi completato. L'elaborato finale sarà il 5° volume delle Guide AIEA, dopo che saranno presi gli opportuni accordi con le associazioni che hanno collaborato (Aused – Anssaif)



Gruppo di Lavoro "COBIT-Legge 262"

Il primo ed il quarto sottogruppi stanno lavorando. Il terzo sta iniziando e la nuova data prevista per il termine dei lavori è il 31/3/2009

Gruppo di Lavoro "Traduzione COBIT 4.1"

COBIT 4.1 – sono stati tradotti e resi disponibili nell'area Downloading del sito i seguenti moduli: ME1, ME2, Me3, ME4DS1, DS2, DS3, DS4, DS5, DS6.

A breve saranno finalizzati l'Introduzione ed i moduli DS7-DS13.

Per la fine dell'anno saranno completati i moduli: PO e AI.

AIEA , TUV e HP

Aiea ha stipulato un accordo, con TUV in base al quale i soci AIEA hanno diritto ad uno sconto del 20% per l'iscrizione a corsi a calendario sul tema "IT&Security" organizzati da TUV.

Un accordo simile è in fase di finalizzazione con HP per i corsi ITIL v.3

I prossimi eventi di AIEA

Calendario Eventi AIEA

Novembre

27Torino - Sessione di Studio

DICEMBRE

11Roma - Sessione di Studio

16.....Milano - Sessione di Studio

Ricordiamo i prossimi eventi ISACA:

Calendar of Events

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

November

18 November **e-Symposium**

20 November Articles due for consideration for publication in volume 2, 2009, of *ISACA Journal*

December

4-5 December... **IT Controls for Sarbanes-Oxley: The Symposium, Dallas, Texas, USA**

8-12 December **ISACA Training Week, New Orleans, Louisiana, USA**

10 December Early-bird registration deadline for the Asia-Pacific CACS conference, Kyoto, Japan

13 December CISA, CISM and CGEIT exams held worldwide

17 December Early-bird registration deadline for the ISACA Training Week, Houston, Texas, USA

31 December Deadline for submission of CGEIT grandfathering application

January

14 January Early-bird registration deadline for the Information Security Conference Latin America

20 November Articles due for consideration for publication in volume 3, 2009, of *ISACA Journal*

28 January Early-bird registration deadline for the ISACA Training Week, Nashville, Tennessee, USA



Associazione Italiana
Information Systems Auditors



Member benefit of the month



Member Benefit of the Month: Academic Research Area of ISACA Web Site

ISACA has added an area to its web site dedicated to providing ISACA and its members an opportunity to support potentially groundbreaking research. Each research project will also result in the addition of professional content to the site, via resulting white papers, articles, etc. ISACA encourages its members and chapters to participate in those projects they find of special interest or pertinence. Please visit www.isaca.org/academicresearch to learn more. !

Riceviamo da ISACA

Siamo lieti di farvi partecipi del riconoscimento che ISACA ha fatto nei confronti di AIEA, capitolo di Milano. Ecco la mail che è arrivata al nostro Presidente

Dear Silvano,

One of the primary purposes of an ISACA chapter board is to maintain good governance at the local level. ISACA International requires that the following three items be submitted to International Headquarters within 30 days of your Annual General Meeting (AGM):

- 1) Chapter Annual Report;*
- 2) Chapter Balanced Scorecard (CBSC) rating grid; and*
- 3) An audit/verification letter.*

Completion and submission of these reports is meant to ensure that good governance is in place, that your chapter supports and protects the ISACA brands and that your chapter continuously aligns itself with the ISACA strategy.

Effective 12 November 2008, ISACA International will post at www.isaca.org/chapterportal a list of all chapters and their compliance in returning all three of the items above. The list, which will be updated on a weekly basis, will display all chapters who held AGMs this year and have submitted all three of these items to ISACA International as being fully compliant. Chapters who have not yet submitted all three of the items listed above will display as non-compliant until all items are received.

The current compliance status for the Milano Chapter is:

Chapter Annual Report: Compliant

Chapter Balanced Scorecard Rating Grid: Compliant



Audit/Verification Letter: Compliant

.Sincerely,

.....

Avviso ai soci 1

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo, azienda di appartenenza o altro...) di comunicare i nuovi dati in segreteria aiea@aiea.it. La mancanza di tali comunicazioni potrebbero impedire, al socio, la ricezione delle comunicazioni.

Avviso ai soci 2

Per completare alcuni dati mancanti sul DB associativo, AIEA invierà, a breve, una comunicazione ai soci.

Avviso ai soci 3

Stiamo preparando il calendario degli eventi AIEA.

Rinnoviamo l'invito ai soci di fornire le proprie indicazioni su argomenti o temi che desiderano vengano trattati nel corso del 2009 sia nelle Sessioni di Studio sia in Workshop.

Chi volesse dare il proprio contributo, è pregato inviare una mail a aiea@aiea.it, specificando, nell'oggetto "ARGOMENTI DI INTERESSE"

In una successiva newsletter provvederemo ad elencare tutti i temi proposti.

Partecipazione di soci ad eventi

Tutti i soci possono segnalare eventi, fatti e informazioni di possibile interesse comune da segnalare ad esempio nella newsletter.

In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o chairman, valutate la possibilità di partecipare a nome AIEA. La partecipazione dell'Associazione ad un evento "deve" però essere decisa dal Consiglio Direttivo: siete quindi pregati di contattare il CD con ragionevole anticipo!

In caso non fosse possibile la partecipazione a nome AIEA, vi invitiamo ad indicare, nel profilo professionale la vostra appartenenza ad AIEA, Capitolo di ISACA

Bibliografia

E' on line il nuovo numero di InterLex (<http://www.interlex.it>)

Vi informiamo che sul sito www.cnipa.it sono disponibili molti documenti di interesse per i nostri soci. Ricordiamo che alla stesura di numerosi documenti hanno partecipato diversi nostri soci e che inoltre CNIPA organizza incontri o seminari aperti anche ai soci AIEA.

Le Newsletter delle altre Associazioni



- E' disponibile on line, la **Newsletter CLUSIT** del 31 ottobre 2008 (disponibile in PDF all'indirizzo www.clusit.IT/newsletter_31_10_08.pdf)

Tra i vari, interessanti articoli, segnaliamo:

SECURITY SUMMIT 2009

=====

L'organizzazione del Security Summit, a cui stanno contribuendo con molto impegno oltre ad alcuni membri del direttivo e del CTS anche diversi soci, prende proporzioni sempre più significative. Abbiamo invitato 3 keynote di fama internazionale, che saranno per la prima volta in Italia e apriranno le tre giornate di Milano (24-26 marzo). Per le sessioni formative, i seminari tecnici e gli atelier tecnologici (momenti di approfondimento sulle tecnologie più significative per la sicurezza ICT, con case studies e sessioni dimostrative), abbiamo coinvolto oltre 50 docenti: professionisti, ricercatori e docenti universitari. Alle tavole rotonde ed ai convegni verticali parteciperanno oltre 70 relatori: esperti del settore, rappresentanti di aziende, rappresentanti di associazioni, rappresentanti delle istituzioni.

Sono state fissate anche le date del Security Summit di Roma, che si terrà nei giorni 10 e 11 giugno. Tra le più importanti novità del Summit, confermiamo che tutti potranno seguirne sul web i momenti più significativi, sia in diretta che in differita, aprendo così, per la prima volta, una manifestazione specialistica alla comunità online.

Segnaliamo infine che, nell'ambito del Security Summit, si terrà la prima edizione dell'hacking Film Festival, con la proiezione di film di gran successo ma anche di film indipendenti/underground, seguiti da dibattiti a cui parteciperanno, oltre agli esperti del Security Summit, critici cinematografici e giornalisti di settore.

Il Festival si svilupperà su tre serate, sia a Milano che a Roma, e la direzione scientifica sarà affidata ai professori Giovanni Ziccardi e Danilo Bruschi dell'Università degli Studi di Milano.

DUE GUIDE DAL NIST

=====

Con l'arrivo di ottobre, il National Institute of Standards and Technology (NIST) ha aggiornato ben quattro documenti "speciali", alcuni dei quali passati da semplici "draft" a documentazione ufficiale. Gli argomenti trattati sono tutti molto interessanti, ma di particolare interesse per i soci del Clusit troviamo: "Technical Guide to Information Security Testing and Assessment" e la "Guide to Bluetooth Security".

.....

Sul sito Clusit sono anche elencati i prossimi **EVENTI SICUREZZA**

E' disponibile on line la **Newsletter ANSSAIF** del 30/10/2008 (www.anssaif.it)

E' disponibile, ed è qui allegata, la Newsletter n.ro 325 del Garante Privacy



- PAZIENTE PUÒ AVERE FOTO INTERVENTI CHIRURGIA PLASTICA
- MULTA A GESTORE TELEFONICO CHE NON RISPONDE AL GARANTE
- GARANTITO L'ACCESSO AI DATI PERSONALI NEI PROCEDIMENTI A CARICO DI TERZI
- L'UE APRE LA STRADA ALL'USO DELLE "ETICHETTE INTELLIGENTI"

Paziente può avere foto interventi chirurgia plastica

Anche le foto scattate prima e dopo gli interventi di chirurgia plastica contengono dati personali e i pazienti hanno il diritto di accedervi.

Lo ha chiarito il Garante nell'accogliere il ricorso di una donna che si era vista negare da due medici l'accesso alle fotografie scattate prima e dopo alcuni interventi di liposuzione cui si era sottoposta. La signora, prima di rivolgersi all'Autorità, aveva chiesto più volte copia delle fotografie degli interventi ai due medici che gliel'avevano negate sostenendo che la paziente non aveva mai chiarito di quale materiale volesse entrare in possesso e soprattutto affermavano che, trattandosi di dati sanitari, doveva motivare la richiesta.

L'Autorità, con un provvedimento di cui è stato relatore Mauro Paissan, nell'accogliere il ricorso ha ordinato ai due medici di comunicare alla paziente i dati personali che la riguardano, in particolare le fotografie realizzate prima e dopo gli interventi chirurgici, dando conferma, entro un termine, dell'avvenuto adempimento.

Nel provvedimento il Garante evidenzia che l'interessato ha diritto di accedere a tutti i dati personali che lo riguardano, in qualunque documento, supporto anche visivo o archivio essi siano contenuti, senza dover fornire giustificazioni della necessità di ottenere tali informazioni. La motivazione, erroneamente richiesta dai medici in questo caso, è necessaria invece quando l'accesso ai dati contenuti nelle cartelle cliniche è effettuato da parte di terzi diversi dall'interessato.

Ai sensi del Codice Privacy, infatti, l'esercizio del diritto d'accesso ai dati conservati dal titolare del trattamento consente all'interessato di ottenere la comunicazione in forma intelligibile dei dati o, quando la loro estrazione risulti particolarmente difficoltosa, la consegna in copia dei documenti che li contengono, comprese le informazioni sullo stato di salute riportate su fotografie, filmati, radiografie, ecc.

Le spese sostenute per il procedimento dovranno essere liquidate dai due medici direttamente a favore della signora.

Multa a gestore telefonico che non risponde al Garante

Chi non fornisce all'Autorità informazioni o documenti che gli sono stati richiesti è soggetto al pagamento di una sanzione pecuniaria. È quanto accaduto a un gestore telefonico al quale il Garante ha ordinato di pagare una multa di 20.000 euro per violazione della norma del Codice privacy che stabilisce, appunto, l'obbligo di fornire informazioni richieste dall'Autorità. Il provvedimento è stato adottato a seguito della segnalazione di una signora che lamentava di ricevere telefonate indesiderate da parte di un sistema automatizzato di chiamata senza operatore, senza che fosse stato preventivamente chiesto e ottenuto il consenso. In questi casi la normativa stabilisce che per effettuare telefonate attraverso l'uso di sistemi automatizzati di chiamata è necessario aver acquisito prima il consenso degli interessati.

Il Garante, che aveva già invitato la società a fornire ogni informazione in merito all'utilizzo del sistema, non avendo ricevuto risposta ha contestato la violazione. Trascorsi i termini che il gestore telefonico aveva per presentare scritti difensivi e documenti o per effettuare il pagamento previsto in misura ridotta, l'Autorità ha applicato la sanzione pecuniaria prevista dal Codice privacy tenendo conto della gravità della violazione.

Garantito l'accesso ai dati personali nei procedimenti disciplinari a carico di terzi

Le persone citate specificamente nell'ambito di procedimenti disciplinari hanno diritto di accedere ai dati personali che li riguardano riportati all'interno dei verbali.

E' quanto ha chiarito il Garante accogliendo il ricorso di due impiegati bancari esplicitamente menzionati negli atti

di un giudizio disciplinare a carico di un collega, accusato di sottrazione di denaro dalle casse dell'istituto di credito presso il quale lavorava. Interpellati in proposito dalla banca, i due avevano chiesto, ai sensi del Codice in materia di tutela dei dati personali, di conoscere quanto li riguardava all'interno della documentazione relativa al procedimento. La banca si era però inizialmente opposta alla richiesta, affermando di non poterli fare accedere alla documentazione di un procedimento disciplinare nei confronti di un terzo senza consenso di questi. Insoddisfatti, i due dipendenti avevano presentato ricorso al Garante Privacy, ribadendo la richiesta di accesso anche in relazione all'eventualità di dover tutelare i propri diritti nei confronti di quanto affermato, secondo loro falsamente, dal collega. Sollecitata dal Garante ad accogliere le richieste dei due dipendenti, la banca aveva continuato ad opporsi sostenendo questa volta che la richiesta originaria era in realtà finalizzata ad ottenere copia della documentazione relativa al procedimento disciplinare riguardante esclusivamente un terzo, anziché la semplice comunicazione dei dati personali relativi ai due impiegati. La decisione del Garante ha considerato legittima la rivendicazione dei due: la richiesta, infatti, formulata ai sensi del Codice Privacy, doveva essere intesa dalla banca come finalizzata alla sola comunicazione dei dati personali che li riguardano direttamente e che a tale richiesta l'istituto avrebbe dovuto adeguarsi nei tempi e nei modi stabiliti dalla normativa.

L'Ue apre la strada all'uso delle "etichette intelligenti"

La presidenza francese dell'Ue ha organizzato a Nizza nelle scorse settimane una conferenza ad alto livello dedicata alla costruzione di quello che viene definito "l'Internet degli oggetti". La conferenza fa parte di una serie di iniziative della Commissione europea, che si appresta a presentare un pacchetto di misure finalizzate a superare i timori per la privacy connessi all'impiego dei microprocessori (o "tag") Rfid che si ritiene faranno da apripista della nuova rivoluzione tecnologica. Le etichette Rfid sono microcircuiti dai costi relativamente contenuti, in grado di comunicare con un dispositivo fisso o portatile, il lettore. Le etichette si compongono di un'antenna e di un microprocessore al silicio e possono essere applicate ad articoli di consumo, imballaggi ed altri oggetti, ovvero impiantate in animali o nell'uomo. Bruxelles considera la creazione dell' "Internet degli oggetti" una priorità fondamentale, poiché potrebbe offrire soluzione ad un'ampia gamma di problemi sociali quali l'invecchiamento della popolazione. La Commissione ritiene che, in un futuro in cui etichette e sensori omnipervasivi sarebbero applicati ad ogni oggetto di uso quotidiano, compresi gli articoli di vestiario, si

apriranno enormi occasioni di progresso ed avanzamento. Tanto da potersi spingere ad affermare che "chi è non vedente potrebbe vedere", grazie ad una rete di sensori Rfid che potrebbero indicare la posizione di tutti gli oggetti circostanti.

Tuttavia, l'impiego dei tag Rfid solleva anche una serie di preoccupazioni rispetto alla privacy ed alla sicurezza delle informazioni che essi veicolano. I tag Rfid possono contenere, infatti, informazioni personali potenzialmente utilizzabili da chiunque sia munito di un lettore, anche all'insaputa dell'interessato.

La Commissione europea sta lavorando ad un progetto di raccomandazione in materia che fa seguito agli esiti di una consultazione pubblica lanciata all'inizio del 2008. Numerose proposte contenute in tale raccomandazione derivano dalle indicazioni formulate nel documento di lavoro sull'Rfid adottato dal Gruppo che riunisce le Autorità per la privacy europee nel 2005: adeguata informativa agli utenti, misure di sicurezza idonee per evitare intrusioni, disattivazione automatica dei tag Rfid all'uscita dagli esercizi commerciali.

Le etichette Rfid sono utilizzate soprattutto negli Usa, in Giappone, in Cina e nella Corea del Sud. In Europa il mercato è in fase iniziale. Secondo IDTechEX, una società di consulenza specializzata, attualmente sono già 2 miliardi le etichette utilizzate a livello mondiale. Fra dieci anni si ritiene che il numero dei dispositivi Rfid sarà aumentato di 300 volte.

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

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

Cooperazione giudiziaria in Ue: Pizzetti incontra Barrot - Comunicato del 9.10.2008

Garanti privacy mondiali su Social network: raccomandazioni a utenti e fornitori di servizi - Comunicato del 20.10.2008

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