OCSE

129 Raccomandazione del Consiglio Ocse relativa alle linee-guida per la sicurezza dei sistemi informativi e delle reti: verso una cultura della sicurezza

(adottata dal Consiglio nel corso della sua 1037ma riunione, il 25 luglio 2002)

OCSE
Organizzazione per la cooperazione e lo sviluppo economico

C(2002)131/FINAL

RACCOMANDAZIONE DEL CONSIGLIO OCSE RELATIVA ALLE LINEE-GUIDA PER LA SICUREZZA DEI SISTEMI INFORMATIVI E DELLE RETI: VERSO UNA CULTURA DELLA SICUREZZA

IL CONSIGLIO

Vista la Convenzione sull'Organizzazione per la cooperazione e lo sviluppo economici del 14 dicembre 1960, ed in particolare gli articoli 1 b), 1 c), 3 a) e 5 b) della stessa,

Vista la Raccomandazione del Consiglio relativa alle Linee-guida sulla protezione della vita privata e sui flussi transfrontalieri di dati personali, del 23 settembre 1980 [C(80)58(Final)],

Vista la Dichiarazione sui flussi transfrontalieri di dati personali, adottata dai governi dei Paesi membri dell'OCSE l'11 aprile 1985 [Allegata a C(85)139],

Vista la Raccomandazione del Consiglio relativa alle Linee-guida per le politiche crittografiche, del 27 marzo 1997 [C(97)62/FINAL],

Vista la Dichiarazione ministeriale relativa alla tutela della privacy sulle reti globali, del 7-9 dicembre 1998 [Allegata a C(98)177/FINAL],

Vista la Dichiarazione ministeriale relativa all'autenticazione per il commercio elettronico, del 7-9 dicembre 1998 [Allegata a C(98)177/FINAL],

Riconoscendo che le reti ed i sistemi di informazione trovano impiego crescente, e rivestono sempre maggiore importanza, per quanto concerne governi, imprese, altri enti e singoli utenti,

Riconoscendo che il ruolo sempre più significativo dei sistemi informativi e delle reti e la loro crescente rilevanza ai fini della stabilità e dell'efficienza delle economie nazionali e del commercio internazionale nonché nella vita sociale, culturale e politica richiedono un impegno particolare al fine di tutelare e promuovere la fiducia nei loro confronti,

Riconoscendo che i sistemi informativi e le reti e la loro proliferazione a livello mondiale sono stati accompagnati da nuovi e crescenti rischi,

Riconoscendo che i dati e le informazioni conservati e trasmessi attraverso i sistemi informativi e le reti sono esposti a rischi legati a varie modalità di accesso e utilizzazione indebiti, alla loro sottrazione o

alterazione, alla trasmissione impropria di codici, ad attacchi tipo DoS [Denial of Service] o alla loro distruzione, e necessitano di opportune garanzie,

Riconoscendo la necessità di sensibilizzare rispetto ai rischi per i sistemi informativi e le reti ed alle politiche, prassi, misure e procedure disponibili per fare fronte a tali rischi, e di promuovere un comportamento corretto quale presupposto essenziale ai fini dello sviluppo di una cultura della sicurezza,

Riconoscendo l'esigenza di rivedere le politiche, prassi, misure e procedure correnti in modo da contribuire ad assicurarne l'adeguatezza rispetto alle sfide in continua evoluzione derivanti dalle minacce ai sistemi informativi ed alle reti,

Riconoscendo l'esistenza di un interesse comune a promuovere la sicurezza dei sistemi informativi e delle reti attraverso una cultura della sicurezza che favorisca il coordinamento e la cooperazione internazionali per fare fronte alle sfide derivanti dai danni che deficit di sicurezza possono causare alle economie nazionali, al commercio internazionale ed alla partecipazione alla vita sociale, culturale e politica,

Riconoscendo, inoltre, che le Linee-guida per la sicurezza dei sistemi informativi e delle reti: verso una cultura della sicurezza definite nell'Allegato alla presente Raccomandazione hanno natura volontaria e non incidono sui diritti sovrani delle nazioni,

Riconoscendo che le presenti Linee-guida non intendono indicare l'esistenza di una soluzione univoca per garantire la sicurezza, né quali politiche, prassi, misure e procedure siano adeguate in rapporto a specifiche situazioni, bensì intendono fornire un quadro di principi finalizzati a promuovere una migliore comprensione del modo in cui le parti in causa possono trarre vantaggio dallo sviluppo di una cultura della sicurezza e, al contempo, contribuire a tale sviluppo,

RACCOMANDA le presenti Linee-guida per la sicurezza dei sistemi informativi e delle reti: verso una cultura della sicurezza a governi, imprese, altri enti e singoli utenti che sviluppino, possiedano, forniscano, gestiscano, mantengano e utilizzino reti e sistemi di informazione,

RACCOMANDA agli Stati membri:

di definire nuove politiche, prassi, misure e procedure, ovvero di modificare quelle esistenti, in modo da riflettere e tenere conto delle Linee-guida per la sicurezza dei sistemi informativi e delle reti: verso una cultura della sicurezza adottando e promuovendo una cultura della sicurezza secondo le indicazioni fornite nella Linee-guida,

di consultarsi, coordinarsi e collaborare a livello nazionale e internazionale al fine di dare attuazione alle Linee-guida,

di diffondere la conoscenza delle Linee-guida nei settori pubblico e privato, compresi governi, imprese, altri enti e singoli utenti, in modo da promuovere una cultura della sicurezza, e

di invitare tutte le parti interessate ad un comportamento responsabile e all'adozione delle misure necessarie per dare attuazione alle Linee-guida secondo modalità consone ai rispettivi ruoli,

di mettere le Linee-guida a disposizione degli Stati che non sono membri OCSE, tempestivamente e nei modi opportuni,

di rivedere le Linee-guida ad intervalli quinquennali al fine di promuovere la cooperazione internazionale su temi attinenti alla sicurezza dei sistemi informativi e delle reti,

DA' MANDATO al Comitato OCSE per le politiche dell'informazione, dell'informatica e della comunicazione di promuovere l'attuazione delle Linee-guida.

La presente Raccomandazione sostituisce la Raccomandazione del Consiglio relativa alle Lineegui da per la sicurezza dei sistemi informativi del 26 novembre 1992 [C(92)188/FINAL].

ALLEGATO

LINEE-GUIDA PER LA SICUREZZA DEI SISTEMI INFORMATIVI E DELLE RETI VERSO UNA CULTURA DELLA SICUREZZA PREFAZIONE

1. L'impiego di sistemi informativi e di reti e l'intero settore delle tecnologie dell'informazione sono considerevolmente diversi rispetto al 1992, quando l'OCSE pubblicò le Linee-guida per la sicurezza dei sistemi informativi. Questa continua evoluzione comporta significativi benefici, ma richiede anche un'attenzione alla sicurezza molto più consistente da parte di governi, imprese, altri enti e singoli utenti che sviluppino, possiedano, forniscano, gestiscano, mantengano e utilizzino sistemi informativi e reti ("parti in causa").

2. Personal computer sempre più potenti, la convergenza di tecnologie diverse e l'impiego diffuso di Internet hanno fatto scomparire i sistemi isolati e più modesti, situati all'interno di reti prevalentemente chiuse. Oggi l'interconnessione di tutte le parti in causa è sempre più accentuata, e le connessioni travalicano i confini nazionali. Inoltre, Internet supporta infrastrutture critiche come energia, trasporti e finanze e svolge un ruolo essenziale nell'attività delle imprese, nella fornitura di servizi a cittadini e imprese da parte dei governi, e nelle comunicazioni e nello scambio di informazioni fra i singoli cittadini. Anche la natura e la tipologia delle tecnologie che formano l'infrastruttura comunicativa e informativa si sono modificate significativamente. Numero e natura dei dispositivi per l'accesso a tale infrastruttura si sono moltiplicati fino a comprendere dispositivi fissi, wireless e mobili, e l'accesso avviene in misura crescente attraverso connessioni "sempre attive". Pertanto, sono aumentati in misura sostanziale la natura, il volume e la delicatezza delle informazioni trasmesse.

3. A seguito della crescente interconnettività, i sistemi informativi e le reti sono esposti attualmente a minacce e rischi sempre più numerosi e di più varia tipologia. Tutto ciò solleva nuove problematiche di sicurezza. Per tali motivi, le presenti Linee-guida sono rivolte a tutte le parti in causa nella nuova società dell'informazione, e indicano l'esigenza di una maggiore consapevolezza e comprensione delle problematiche attinenti la sicurezza oltre che la necessità di sviluppare una "cultura della sicurezza".

I. VERSO UNA CULTURA DELLA SICUREZZA

4. Le presenti Linee-guida intendono fornire una risposta alla continua evoluzione del settore della sicurezza promuovendo lo sviluppo di una cultura della sicurezza – ossia, un'attenzione particolare alla sicurezza nello sviluppo di sistemi informativi e reti e l'adozione di nuovi approcci mentali e comportamentali nell'utilizzazione di sistemi informativi e reti e nelle interazioni che avvengono al loro interno. Le Linee-guida segnano una netta soluzione di continuità con l'epoca in cui la progettazione e l'utilizzazione di reti e sistemi secondo criteri di sicurezza rappresentavano troppo di frequente una valutazione a posteriori. Cresce di continuo la dipendenza delle parti in causa da sistemi informativi e reti e dai relativi servizi, che devono essere affidabili e sicuri. Solo un approccio che tenga nel debito conto gli interessi di tutte le parti in causa e la natura dei sistemi, delle reti e dei relativi servizi, può garantire un'efficace sicurezza.

5. Ciascuna parte in causa rappresenta un soggetto importante ai fini della sicurezza. Le parti in causa, ciascuna secondo il rispettivo ruolo, dovrebbero essere consapevoli dei rischi per la sicurezza che le riguardano e delle corrispondenti misure preventive, assumersi proprie responsabilità ed agire al fine di potenziare la sicurezza di sistemi informativi e reti.

6. Per promuovere una cultura della sicurezza saranno necessarie una visione ispiratrice e un'ampia partecipazione, con l'obiettivo di conferire maggiore priorità alla pianificazione e gestione della sicurezza, nonché la comprensione diffusa fra tutte le parti in causa della necessità di garantire la sicurezza. Le questioni attinenti la sicurezza dovrebbero essere oggetto di attenzione responsabile a tutti i livelli governativi e imprenditoriali ad opera di tutte le parti in causa. Le presenti Linee-guida costituiscono le fondamenta di un'attività mirante a diffondere una cultura della sicurezza in tutti settori sociali. In tal modo le parti in causa potranno inserire la sicurezza come parte integrante della progettazione e utiliz-

zazione di tutti i sistemi informativi e tutte le reti. Con le presenti Linee-guida si propone a tutte le parti in causa di adottare e promuovere una cultura della sicurezza nel considerare, valutare e intervenire sul funzionamento di sistemi informativi e reti.

II. OBIETTIVI

7. Le presenti Linee-guida intendono

- promuovere una cultura della sicurezza fra tutte le parti in causa come strumento per tutelare i sistemi informativi e le reti,
- sensibilizzare rispetto ai rischi per i sistemi informativi e le reti, alle politiche, prassi, misure e procedure disponibili per affrontare tali rischi, e all'esigenza che esse siano adottate e messe in pratica,
- stimolare la fiducia fra tutte le parti in causa rispetto ai sistemi informativi ed alle reti ed alle modalità della loro fornitura e utilizzazione,
- creare un quadro generale di riferimento che aiuti le parti in causa a comprendere le tematiche della sicurezza ed a rispettare valori etici nello sviluppo e nell'applicazione di politiche, prassi, misure e procedure coerenti per la sicurezza di sistemi informativi e reti,
- promuovere fra tutte le parti in causa la cooperazione e lo scambio di informazioni, nei modi opportuni, rispetto allo sviluppo e all'attuazione di politiche, prassi, misure e procedure di sicurezza,
- promuovere l'inserimento delle tematiche di sicurezza fra gli obiettivi importanti per tutte le parti in causa che siano impegnate nella definizione o nell'attuazione di standard.

III. PRINCIPI

8. I nove principi indicati di seguito sono complementari e dovrebbero essere letti come un insieme unitario. Essi riguardano le parti in causa a tutti i livelli, fra cui il livello politico e quello operativo. Secondo le presenti Linee-guida, la responsabilità delle parti in causa varia in rapporto al ruolo rispettivamente svolto. Per tutte le parti in causa saranno utili la conoscenza, l'educazione, lo scambio di informazioni e la formazione in quanto seguite dall'adozione di migliori prassi e da una migliore comprensione delle tematiche di sicurezza. L'impegno mirante a potenziare la sicurezza di sistemi informativi e reti dovrebbe essere coerente con i valori di una società democratica, in particolare con l'esigenza della libera circolazione delle informazioni, e con l'attenzione fondamentale alla privacy dell'individuo.

1) Sensibilizzazione

Le parti in causa dovrebbero essere consapevoli dell'esigenza di garantire la sicurezza di sistemi informativi e reti e delle misure alle quali ricorrere per potenziare la sicurezza. La sensibilizzazione rispetto ai rischi ed alle tutele disponibili costituisce la prima linea di difesa per la sicurezza di sistemi informativi e reti. I sistemi informativi e le reti possono essere soggetti a rischi sia esterni sia interni. Le parti in causa dovrebbero comprendere che deficit di sicurezza possono danneggiare in misura significativa reti e sistemi soggetti al loro controllo. Dovrebbero inoltre essere consapevoli dei pregiudizi potenzialmente arrecabili a terzi per effetto dell'interconnettività e dell'interdipendenza. Le parti in causa dovrebbero essere a conoscenza della configurazione e degli aggiornamenti disponibili in rapporto al proprio sistema, della collocazione di quest'ultimo nelle reti, delle buone prassi da esse applicabili per potenziare la sicurezza, e delle esigenze di altre parti in causa.

2) Responsabilità

Tutte le parti in causa sono responsabili della sicurezza di sistemi informativi e reti Tutte le parti in causa fanno riferimento a sistemi informativi e reti interconnessi a livello locale e globale, e dovrebbero essere consapevoli delle rispettive responsabilità per quanto concerne la sicurezza di tali reti e sistemi. Dovrebbero risponderne ciascuna nei modi opportuni in rapporto alla funzione rispettivamente svolta. Le parti in causa dovrebbero riesaminare periodicamente le proprie politiche, prassi, misure e procedure valutando se siano adeguate al rispettivo contesto. I soggetti responsabili dello sviluppo, della progettazione e della fornitura di prodotti e servizi dovrebbero prendere in considerazione le tematiche della sicurezza di reti e sistemi e diffondere tempestivamente le informazioni opportune – ivi compresi eventuali aggiornamenti – in modo che gli utenti possano più facilmente comprendere le funzioni di sicu-

rezza dei prodotti e servizi in questione e le rispettive responsabilità in termini di sicurezza.

3) Reazione

Le parti in causa dovrebbero agire tempestivamente ed in modo cooperativo per prevenire, individuare e rispondere a problemi di sicurezza In ragione dell'interconnettività dei sistemi informativi e delle reti e dei rischi potenziali di danni rapidi e diffusi, le parti in causa dovrebbero agire tempestivamente ed in modo cooperativo per affrontare problemi di sicurezza. Dovrebbero scambiarsi informazioni su rischi e vulnerabilità, nei modi opportuni, e mettere in atto procedure finalizzate ad una rapida ed efficace collaborazione in modo da prevenire, individuare e rispondere a problemi di sicurezza. Quando ammissibile, ciò può comportare uno scambio di informazioni e attività di cooperazione transfrontalieri.

4) Etica

Le parti in causa dovrebbero rispettare i legittimi interessi di terzi. In considerazione della pervasività dei sistemi informativi e delle reti nelle nostre società, le parti in causa devono comprendere che le loro azioni o omissioni possono danneggiare soggetti terzi. Pertanto, è fondamentale adottare comportamenti eticamente corretti, e le parti in causa dovrebbero mirare alla definizione e all'adozione di prassi esemplari e promuovere comportamenti che tengano conto delle esigenze di sicurezza e rispettino i legittimi interessi di terzi.

5) Democrazia

La sicurezza dei sistemi informativi e delle reti dovrebbe essere compatibile con valori fondamentali di una società democratica La sicurezza dovrebbe essere garantita in modi compatibili con i valori riconosciuti dalle società democratiche e, in particolare, con la libertà di manifestazione del pensiero, la libera circolazione delle informazioni, la riservatezza delle informazioni e delle comunicazioni, la protezione adeguata dei dati personali, l'apertura e la trasparenza.

6) Analisi dei rischi

Le parti in causa dovrebbero effettuare un'analisi dei rischi L'analisi dei rischi permette di evidenziare rischi e vulnerabilità e dovrebbe essere sufficientemente ampia da tenere conto di fattori fondamentali sia interni sia esterni, come le componenti tecnologiche, i fattori fisici e umani, le politiche ed i servizi gestiti da terzi che abbiano implicazioni in termini di sicurezza. L'analisi dei rischi permetterà di definire la soglia accettabile di rischio e faciliterà l'individuazione di controlli adeguati per gestire il rischio di danni potenziali ai sistemi informativi ed alle reti, tenendo conto della natura e dell'importanza delle informazioni da tutelare. A causa della crescente interconnettività dei sistemi informativi, l'analisi dei rischi dovrebbe prendere in considerazione i pregiudizi potenzialmente derivanti da terzi o arrecabili a terzi.

7) Progettare e realizzare in un'ottica di sicurezza

Le parti in causa dovrebbero fare della sicurezza una componente fondamentale di sistemi informativi e reti. E' necessario progettare, realizzare e coordinare in modo corretto sistemi, reti e politiche al fine di ottimizzare la sicurezza. Un fattore importante, ma non esclusivo, in tale contesto è rappresentato dalla progettazione e dall'adozione di garanzie e soluzioni adeguate in modo da evitare o limitare il pregiudizio potenzialmente derivante dai rischi e dalle vulnerabilità già individuate. Occorrono garanzie e soluzioni di natura tecnica e non tecnica, che devono essere proporzionate al valore delle informazioni presenti sui sistemi e sulle reti del singolo organismo. La sicurezza dovrebbe rappresentare una componente fondamentale di tutti i prodotti, i sistemi, i servizi e le reti, nonché costituire parte integrante della progettazione e dell'architettura di sistema. Per quanto riguarda gli utenti finali, progettare e realizzare in un'ottica di sicurezza significa soprattutto individuare e configurare prodotti e servizi per i rispettivi sistemi.

8) Gestione della sicurezza

Le parti in causa dovrebbero adottare un approccio globale alla gestione della sicurezza La gestione della sicurezza dovrebbe basarsi sulla valutazione dei rischi ed essere di tipo dinamico, abbracciando le attività delle parti in causa a tutti i livelli e tutti gli aspetti delle rispettive operazioni. Dovrebbe prevedere una risposta lungimirante rispetto ai rischi emergenti e comprendere la prevenzione, l'individuazione e la reazione a possibili incidenti, il ripristino dei sistemi, la manutenzione permanente, attività di

verifica e di controllo indipendente. Le politiche di sicurezza relative a sistemi informativi e reti, nonché le prassi, misure e procedure connesse, dovrebbero essere coordinate e integrate in modo da creare un sistema di sicurezza coerente. Le esigenze gestionali dipendono dal livello di partecipazione, dal ruolo del singolo soggetto parte in causa, dai rischi associati e dai requisiti di sistema.

9) Riesame

Le parti in causa dovrebbero sottoporre a riesame e ad una nuova valutazione la sicurezza di sistemi informativi e reti, e modificare nei modi opportuni politiche, prassi, misure e procedure di sicurezza Rischi e vulnerabilità sempre nuovi e mutevoli vengono incessantemente alla luce. Le parti in causa dovrebbero costantemente riesaminare, rivedere e modificare tutti gli aspetti di sicurezza per fare fronte all'evolversi delle situazioni di rischio.

Consiglio dell'Unione europea

130 Risoluzione del Consiglio dell'Unione europea del 18 febbraio 2003 su un approccio europeo per una cultura della sicurezza delle reti e dell'informazione (2003/C 48/01)(*)

IL CONSIGLIO DELL'UNIONE EUROPEA,

RICORDANDO

1. la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni, sulla sicurezza delle reti e sicurezza dell'informazione: Proposta di un approccio strategico europeo;

2. la risoluzione del Consiglio del 30 maggio 2001 concernente un "Piano d'azione eEurope: sicurezza dell'informazione e delle reti";

3. la risoluzione del Consiglio del 28 gennaio 2002 relativa ad un approccio comune e ad azioni specifiche nel settore della sicurezza delle reti e dell'informazione (1);

4. il Piano d'azione eEurope 2005 confermato dal Consiglio europeo di Siviglia del giugno 2002;

5. il parere del Parlamento europeo circa la comunicazione della Commissione europea sulla sicurezza dell'informazione e delle reti: proposta di un approccio strategico europeo;

SOTTOLINEA PERTANTO CHE:

1. con lo sviluppo dei servizi della società dell'informazione, la sicurezza delle reti e delle informazioni assume sempre maggiore importanza per la vita quotidiana dei cittadini, così come per gli operatori economici e le amministrazioni pubbliche, contribuendo al corretto funzionamento del mercato interno;
2. gli Stati membri e le Istituzioni europee devono sviluppare ulteriormente una strategia europea globale per la sicurezza delle reti e delle informazioni e adoperarsi per conseguire una "cultura della sicurezza" tenendo conto dell'importanza della cooperazione internazionale;
3. gli orientamenti dell'OCSE per la sicurezza dei sistemi e delle reti di informazione sono considerati un modello valido per lo sviluppo delle politiche che perseguono una cultura della sicurezza, nel rispetto dei valori democratici e dell'importanza della protezione dei dati personali;
4. occorre rispettare il diritto alla vita privata. I cittadini e le imprese devono poter confidare che l'informazione è trattata con accuratezza, riservatezza e affidabilità;
5. nello sviluppare una cultura della sicurezza, uno dei compiti fondamentali sarà la precisazione della responsabilità della sicurezza delle reti e dei sistemi di informazione per tutti gli interessati;
6. all'Europa occorre garantire l'elaborazione e lo sviluppo dell'appropriata qualificazione nel settore della sicurezza delle reti e delle informazioni;
7. occorrono maggiori trasparenza, scambio di informazioni e cooperazione tra gli Stati membri, le Istituzioni europee e il settore privato;
8. l'elaborazione di una politica coerente in materia di sicurezza a livello europeo richiede trasparenza e cooperazione interpilastri;
9. devono essere proseguiti i lavori in corso per adempiere l'impegno preso nella risoluzione del

(*) G.U.C.E. n. C 48/2, del 28.2.2003
(1) GU C 43 del 16.2.2002, pag. 2.

Consiglio del 28 gennaio 2002 sull'approccio comune e le azioni specifiche nel settore delle reti e della sicurezza dell'informazione.

INVITA PERTANTO GLI STATI MEMBRI A:

1. promuovere la sicurezza quale componente essenziale del governo pubblico e privato, in particolare incoraggiando l'assegnazione delle responsabilità;
2. prevedere un'appropriata istruzione e formazione professionale, nonché l'aumento della consapevolezza, in particolare tra i giovani, nei confronti dei problemi della sicurezza;
3. adottare provvedimenti adeguati per impedire e reagire agli incidenti in materia di sicurezza, soprattutto tramite:

a) il costante miglioramento del processo di identificazione e di valutazione dei problemi di sicurezza e l'applicazione di controlli adeguati;

b) la creazione di mezzi efficaci per comunicare la necessità di agire a tutti gli interessati mediante il rafforzamento del dialogo a livelli sia europeo che nazionale e, ove opportuno, internazionale in particolare con i fornitori di tecnologia e servizi della società dell'informazione;

c) la presa in considerazione di un adeguato scambio di informazioni rispondente all'esigenza della società di essere tenuta al corrente delle buone prassi connesse alla sicurezza.

4. incoraggiare la cooperazione e il partenariato tra le università e le imprese in modo da fornire servizi e tecnologie sicure e favorire lo sviluppo di norme riconosciute.

ACCOGLIE CON FAVORE L'INTENZIONE DELLA COMMISSIONE DI:

1. applicare il metodo aperto di coordinamento per quanto riguarda le attuali azioni degli Stati membri e valutare il relativo impatto sulla sicurezza;

2. istituire un gruppo interdisciplinare provvisorio in stretta collaborazione con gli Stati membri e composto di loro rappresentanti, incaricato dei lavori preparatori in vista della creazione di una "Cyber-Security Task Force", come previsto dalla risoluzione del Consiglio del 28 gennaio 2002;

3. avviare uno studio come base della prevista relazione sulle applicazioni dei sistemi di autenticazione biometrica;

4. sviluppare ulteriormente, in collaborazione con gli Stati membri, un dialogo con l'industria del settore per migliorare la sicurezza nell'elaborazione dei prodotti hardware e software e garantire la disponibilità dei servizi e dei dati;

5. istituire la "Cyber-Security Task Force" di cui sopra.

INVITA:

1. l'industria del settore a far sì che la gestione dei rischi in materia di sicurezza sia integrata nel pensiero manageriale e nell'ingegneria economica;

2. tutti gli utenti ad avere una visione olistica dei rischi associati ai sistemi di informazione e valutare le minacce conseguenti ad eventi materiali, carenze umane, nonché a vulnerabilità tecnologiche e ad aggressioni deliberate.

3. l'industria e tutti gli utenti a dialogare coi governi per sviluppare una cultura della sicurezza.