

Lo scenario e le norme internazionali per la Certificazione della Sicurezza delle Informazioni

Luigi PAVANI

Head of ICT Certification Services Department

RINA SpA

<http://itservices.rina.org>



RINA

Il contesto competitivo e la Certificazione

Pressioni interne

- Ritorno degli investimenti
- Riduzione dei costi
- Responsabilità finanziarie
 - Massimo profitto
- Qualità del prodotto
- Tutela del Know-how
- Minacce interne

**COMPANY
MANAGEMENT**

Pressioni esterne

- Minacce in rete
- tam-tam di internet
- Responsabilità segreti industriali
- Direttive europee (31/2000)
- Consenso sociale e legislazione
 - Obblighi legali
- Sicurezza dei dati
- Enti Autorizzatori (Basilea 2,
• Banca d'Italia CAI)

SOLUZIONI GESTIONALI

- | | | |
|---------------|-----------|----------------------------------|
| - ISO 9000 | Qualità | - EMAS |
| - ISO 14001 | Ambiente | - ISO 17799 e BS 7799 |
| - OHSAS 18001 | Sicurezza | - Qweb (certificazione dei siti) |
| - SA 8000 | Etica | |



Aziende

- Requisiti dei clienti
 - aziende che trattano informazioni in outsourcing
 - centri di ricerca, di design, di progettazione, ad elevato know-how, che operano per più clienti tra loro concorrenti
 - aziende che trattano grandi quantità di dati personali (es. utility)
 - aziende con processi produttivi o di erogazione servizio governati da sistemi informativi
- Requisiti interni
 - miglioramento processi, ROI su investimenti informatici
 - tutela know-how
- Requisiti normativi
 - complesso normativo sulla Privacy e Data Protection - Nuovo Codice



RINA

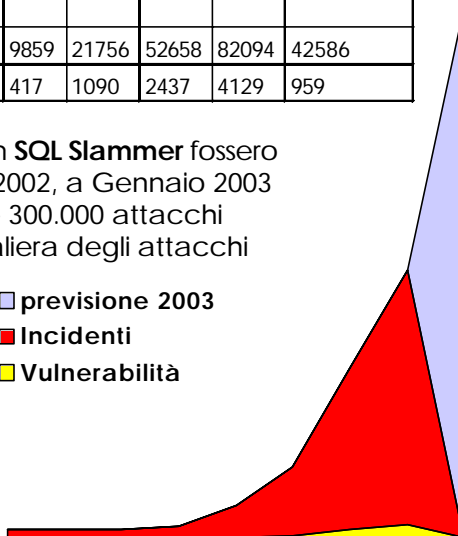
INTERNET SECURITY

Fonte:	1995	1996	1997	1998	1999	2000	2001	2002	Q1 2003
www.cert.org									
Incidenti	2412	2573	2134	3734	9859	21756	52658	82094	42586
Vulnerabilità	171	345	311	262	417	1090	2437	4129	959

- Sebbene le patch per il worm **SQL Slammer** fossero disponibili almeno dal Luglio 2002, a Gennaio 2003 si sono registrati tra 200.000 e 300.000 attacchi all'ora, pari alla media giornaliera degli attacchi

NIMDA.

- previsione 2003
- Incidenti
- Vulnerabilità



RINA

MINACCE DA INSIDER

installazione/uso di sw non autorizzato	78%
uso di risorse aziendali per comunicazioni /attività illegali o illecite	60%
uso di risorse aziendali per profitto personale (scommesse, spam, gestione di personal e-commerce site, investimenti online)	60%
abuso di computer control access	56%
furto fisico, sabotaggio o distruzione intenzionale di computer equipment	49%
installazione/uso di hw/periferiche non autorizzate	47%
furto elettronico, sabotaggio o intenzionale distruzione/diffusione di dati/informazioni proprietari	22%
frode	9%



RINA

Fonte: True Secure - Predictive Systems
% aziende con risposta affermativa

MINACCE DA OUTSIDER

viruses/trojan/worms	89%
attacchi su bug di web server	48%
Denial of Service (Dos)	39%
buffer overflow attacks	32%
exploits dovuti a scripting/mobile code (acitveX, Java, javaScript, VBS)	28%
attacchi dovuti a protocol weakness	23%
attacchi dovuti a password non sicure	21%



RINA

Fonte: True Secure - Predictive Systems
% aziende con risposta affermativa

LE RISPOSTE DELLE AZIENDE

rafforzamento del perimetro di rete per prevenire intrusioni dall'esterno	4.31
sicurezza e disponibilità per siti web e/o operazioni di e-commerce	4.01
sicurezza di messaggi/e-mail	3.99
mettere in sicurezza gli accessi remoti per impiegati/telecommuters/utenti remoti	3.89
gestione centralizzata/correlazione di security policy/contromisure/alert data	3.79
prevenzione di abuso di accesso da parte di impiegati/insiders	3.66
altro	2.72



RINA

Fonte: True Secure - Predictive Systems
Scala da 1 a 5 per livello di importanza

GLI OSTACOLI

budget	3.55
mancaanza di training per gli utenti/consapevolezza per gli end-user	3.55
mancaanza di supporto della direzione	3.17
mancaanza di personale competente di sicurezza	3.08
mancaanza di policy di sicurezza interna	3.07
responsabilità poco chiare	3.04
technical challenges/complessità dei prodotti	3.00



RINA

Fonte: True Secure - Predictive Systems
Scala da 1 a 5 per livello di importanza

LE BAD PRACTICES

"La sicurezza si misura nel suo anello più debole"

- utilizzo di post-it per ricordarsi le password
- aggirare le misure di sicurezza (es. Disattivazione antivirus)
- lasciare i sistemi/documenti "unattended"
- aprire e-mail attachment
- utilizzo di password banali
- discorsi riservati in aree/locali pubblici
- applicazione poco rigorosa delle policy
- sottovalutazione dello staff (insider attacks)
- lentezza nell'update dei sistemi (patch)



RINA

Elementi della sicurezza

- Gli elementi che interagiscono nella sicurezza di una organizzazione sono:
 - il management
 - gli addetti ai sistemi (interni/esterni)
 - gli utenti (interni/esterni)
 - le informazioni
 - le apparecchiature Hardware/Software
 - le minacce in continuo divenire
 - l'evoluzione tecnologica



RINA

LA RISPOSTA GESTIONALE

Una risposta di tipo solamente tecnologico
(controllo accessi, protezione da virus/dos,..)
penalizza l'intero sistema di sicurezza
(tralascia "l'anello più debole")

La risposta delle BS7799, ISO/IEC 17799 parte da una visione globale della sicurezza

- **Global Security Management**
- componenti fisica, logica, operativa, legislativa ..,

focalizzandosi sugli aspetti **gestionali**.



RINA

Le norme internazionali

• **British Standard**

- 1995: emissione delle norme
 - BS 7799-1 contiene indicazioni e raccomandazioni
 - BS 7799-2 contiene requisiti obbligatori, è una norma certificativa
- 1999: pubblicata revisione
- 2002: pubblicata revisione parte 2: BS 7799-2:2002

• **ISO**

- 2000: emissione dello standard
 - ISO 17799, che recepisce la BS 7799-1



RINA

I requisiti della BS 7799

BUSINESS CONTINUITY MANAGEMENT

112	4.9.1.1	Business continuity management process	
113	4.9.1.2	Business continuity and impact analysis	<i>A strategy plan, based on appropriate risk assessment, shall be developed for the overall approach to business continuity</i>
114	4.9.1.3	Writing and implementing continuity plans	
115	4.9.1.4	Business continuity planning framework	<i>A single framework of business continuity plans shall be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance</i>
116	4.9.1.5	testing, maintaining and re-assessing business continuity plans	



RINA

I requisiti della ISO 17799

ISO/IEC 17799

SECTION 11 – BUSINESS CONTINUITY PLANNING

11.1	Aspects of Business Continuity Planning
P	Contingency plans should be developed and implemented to ensure business processes can be restored within the required time-scale. Such plans should be maintained and practised to become integral part of all other management processes
O	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.
S	A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. The consequences of disasters, security failures and loss of service should be analyzed. Business continuity planning should include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure speedy resumption of essential operations.



RINA

I principi

I principi di base di un SGSI sono:

- information security policy (volontà e supporto della direzione)
- allocazione delle responsabilità
- educazione, sensibilizzazione e training
- report degli incidenti
- business continuity management
- controlli necessari per assicurare che gli obiettivi posti sulla sicurezza siano raggiunti



Efficienza ed efficacia

- **Risk Analysis:** identificazione delle risorse da proteggere, dello scenario di minacce e vulnerabilità (interne all'impresa o esterne), calcolo del rischio, della probabilità del suo concretizzarsi, e dell'impatto sul business.
- **Risk Management:** definizione strategica del livello di rischio accettabile e conseguenti decisioni operative sulla gestione del rischio (riduzione, trasferimento, accettazione).

Ogni fase di questo processo richiede responsabilità definite e criteri di conduzione sistematici per assicurarne il controllo periodico, la ripetitività e la tracciabilità nel tempo.



La certificazione BS7799

- La certificazione del proprio sistema di gestione della sicurezza delle informazioni consente di:
 - dimostrare l'aderenza alle best practice riconosciute internazionalmente
 - adottare uno strumento di monitoraggio e miglioramento continuo del livello di sicurezza
- e costituisce
 - un forte asset competitivo in termini di autorevolezza (valutazione di una terza parte indipendente)
 - il naturale ed autorevole coronamento di un percorso di crescita organizzativa e tecnologica
- Viene percepita e compresa dal mercato come uno strumento utile al business



RINA

ACCREDITAMENTO

- RINA è il **primo** Organismo di Certificazione accreditato in ITALIA per la BS 7799 dal Sincert, a garanzia delle competenze, dell'esperienza e della indipendenza
- RINA è in grado di supportare le aziende con un team qualificato, competente sulle tematiche di security, di BS 7799 e di legislazione italiana
- RINA opera nel campo della Information Security da diversi anni, dall'origine delle norme BS 7799 (prima versione del 1995, revisioni del 1999, ISO dal 2000)
- RINA ha sviluppato competenze ed esperienza in tutti i settori merceologici, industriali e di servizi
- RINA opera dal 1861 come Organismo di Certificazione

Certificazione BS 7799 (1/5)

- **Programma Operativo**

- Coinvolgimento e Commitment del Vertice Aziendale
- Risk Assessment: valutazione del livello di esposizione al rischio, individuazione delle aree di criticità, identificazione delle contromisure
- Preparazione del Sistema di Gestione della Sicurezza delle Informazioni
- Audit di Certificazione BS 7799



RINA

Certificazione BS 7799 (2/5)

- **Coinvolgimento del Management**

- Stesura e sottoscrizione della Policy di Sicurezza
- Istituzione dell'Information Security Manager
- Costituzione del Forum per la Sicurezza
 - A.D. o D.G. (o delegato)
 - Resp. Sistemi Informativi
 - Resp. Personale
 - Resp. Affari Legali
 - Information Security Manager
 - Resp. Sicurezza Fisica



RINA

Certificazione BS 7799 (3/5)

- **Risk Assessment**

- Censimento e valorizzazione degli Asset
- Valutazione documentazione (architettura del sistema, descrizione applicativi, procedure o istruzioni in uso, ...)
- Interviste con il personale interessato
- Identificazione minacce e vulnerabilità
- Identificazione Aree di Criticità
- Identificazione Contromisure tecnologiche, organizzative, gestionali, procedurali



RINA

Certificazione BS 7799 (4/5)

- **Preparazione** del Sistema di Gestione della Sicurezza delle Informazioni

- Definizione Responsabilità e ruoli, trasversali a tutta l'organizzazione (IT, personale, legale, servizi generali, ...)
- Stesura Statement of Applicability (selezione motivata dei controlli e dei requisiti della BS 7799 applicati)
- Redazione procedure per la descrizione delle attività correlate alla Security (configurazione, gestione password, backup, amministrazione server e rete, business continuity, ...)
- Sensibilizzazione e formazione personale (IT, guardiania, utenti sistemi informativi, ...)
- Applicazione giornaliera nella routine operativa



RINA

Certificazione BS 7799 (5/5)

- **Certificazione**

- Richiesta di offerta, offerta, accettazione offerta
- Pre-audit (raccomandato)
- Esame Documentale
- Stage 1
 - esame della documentazione (politica, sintesi analisi rischi, statement of applicability, procedure) e verifica dell'applicazione effettiva
 - Rapportazione e sistemazione delle osservazioni
- Stage 2
 - visita di audit (riunione iniziale, suddivisione del team, riunione finale)
 - Rapportazione da parte del team
- Esame del rapporto
- Rilascio del Certificato

I benefici diretti

- **valorizzazione degli investimenti**
- **rafforzamento dell'immagine aziendale**
- **segnale forte verso un mercato sempre più sensibile alla problematica sicurezza**
- **fattore di vitalità per il sistema di gestione stesso, assicurandone efficienza/efficacia e rispondenza ai requisiti legali e contrattuali**
- **strumento di supporto verso enti regolamentatori ed autorizzatori**



RINA

I benefici indiretti

- ♦ influenza positiva sul prestigio aziendale, sull'immagine, sui parametri di goodwill esterna fino ad una possibile incidenza sulla valutazione patrimoniale
- ♦ valenza dello strumento nella gestione delle informazioni, in termini di risk management tramite la definizione di modalità operative anche rispetto ai parametri di legge
- ♦ riduzione dei costi di gestione della sicurezza miglioramento dell'efficienza dei processi
- ♦ sistema di misurazione per valutare le performance nella sicurezza e suggerire aggiunte, miglioramenti
- ♦ miglioramento del ROI sugli investimenti informatici dovuto ad una focalizzazione mirata alla luce dell'analisi e della valutazione dei rischi



RINA

CONCLUSIONI

La ricerca scientifica e tecnologica hanno messo a punto una serie di strumenti e metodologie che consentono di ridurre al minimo le minacce alla sicurezza delle informazioni

Tecnologie, sistemi, infrastrutture, applicativi devono essere gestiti, aggiornati, mantenuti adeguati per far fronte a minacce accidentali o intenzionali che evolvono nel tempo, provenienti dall'interno o dall'esterno dell'azienda.

La norma BS7799 propone gli step operativi per un buon risk management, con il vantaggio della standardizzazione.

GRAZIE PER L'ATTENZIONE

luigi.pavani@rina.org
<http://it.services.rina.org>



RINA