ace europe

Fiera di Milano – 11,12 e 13 Febbraio 2004

Riccardo Scalici – ACE Technical Lines
Andrea Marega – ACE Financial Lines

ace europe

AGENDA

1. **DATA FLOW, la copertura per i Rischi informatici**

2. **Le coperture RC per gli operatori della sicurezza informatica**

3. **L'assicurazione come trasferimento del rischio residuo: una soluzione sia tecnica che economica, in sintonia con le disposizioni di Basilea II**

ace europe

AGENDA

1. **DATA FLOW, la copertura per i Rischi informatici**
   - DATA FLOW, un abito su misura
   - Organigramma del rischio I.T.
   - Tipi di rischi I.T.
   - Key risk
   - Trasferimento del rischio
   - Procedura di trasferimento
   - La stima
   - Le valutazioni
   - La convenienza
   - Un esempio di variazione del costo assicurativo in funzione del livello di protezione
   - Esempi di sinistri

ace europe

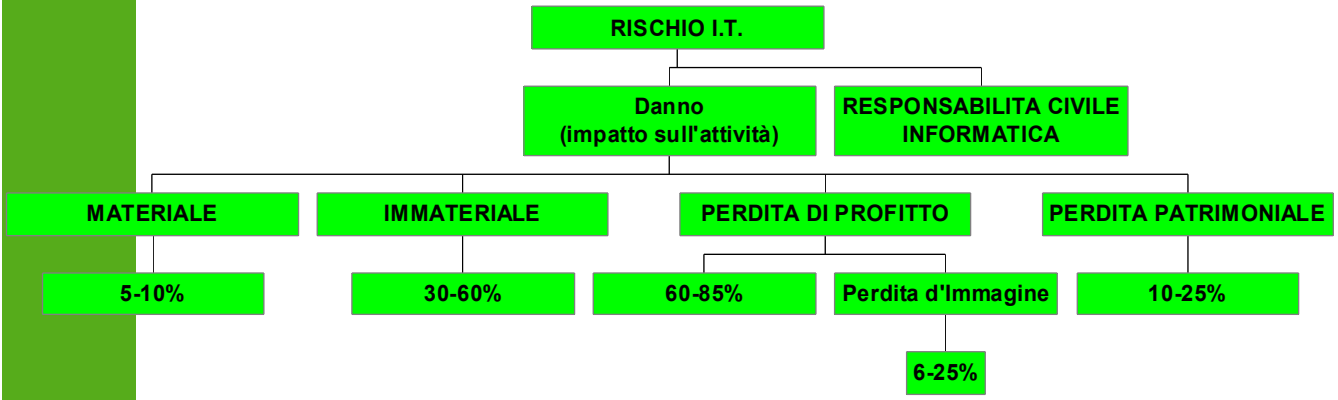
DATA FLOW
Un *"ABITO"* su misura

- Studio delle aree di rischio
- Partnership per costruire polizze su misura
- Collaborazione e aiuto durante le emergenze
- Partecipazione al crescere delle esigenze dei Clienti

- Copertura ALL RISKS per: Hacker, cracker, atti di pirateria informatica
- Errori, virus, bombe logiche
- Frodi informatiche (infedeltà dipendenti)
- Perdite di profitto e spese extra
- Spese straordinarie per ricostruzione immagine sul mercato
- Responsabilità civili informatiche per società di servizio

ace europe

ORGANIGRAMMA DEL RISCHIO I.T.



ace europe

TIPI DI RISCHI I.T.

USUALI

(Mercato Tradizionale I.T.)

- Materiali su Hardware
- Materiali su supporto dati e programmi
- Spese Extra

NUOVI

(Caratteristici *"Data Flow"*)

- Immateriali su programmi e dati, su reti e flussi di dati
- Perdite patrimoniali (frodi)
- Perdite di profitti
- RC Informatica

ace europe

KEY RISK

DANNI IMMATERIALI E DI PROFITTO

- La prima caratteristica di questi nuovi tipi di danno è quella di subire una perdita (pecuniaria, di funzionalità, di profitto, di aumento dei costi, ecc.) senza che un evento fisico sia rilevabile sulla materialità dei cespiti
- La seconda caratteristica consiste nell'estrema varietà della casistica

ace europe

TRASFERIMENTO DEL RISCHIO

SI POSSONO ASSICURARE?

SI!

"*Data Flow*" è presente sul mercato assicurativo Nazionale

"*Data Guard*"su quello Internazionale

proprio per soddisfare queste esigenze

ace europe

PROCEDURA DI TRASFERIMENTO

COME ASSICURARLI

- ANALISI DEL RISCHIO
- STIMA DEL MASSIMO DANNO PROBABILE
- VALUTAZIONE GRADO DI ASSORBIMENTO DELLA FRANCHIGIA
- CALCOLO COSTI ASSICURATIVI

ace europe

ANALISI DEL RISCHIO

Per poter effettuare una corretta analisi del rischio che si intende assicurare bisogna tener conto:

- **Del tipo di attività**
- **Del grado di protezione informatica sia fisica che logica**
- **Della Gestione del Rischio-Risk Management**

ace europe

LE VALUTAZIONI

STIMA DEL MASSIMO DANNO PROBABILE

- Elementi Tecnici
- Fattori Economici
- Fattore Tempo

ace europe

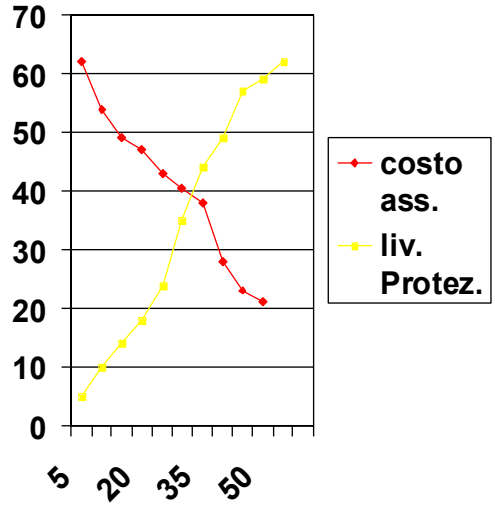
CALCOLO DEL PREMIO

- **In base alla propria esperienza, ogni assicuratore calcola il proprio premio**
- **Non ci sono sufficienti elementi statistici che consentano di poter stimare il rischio nell'ambito dei grandi numeri**

ace europe

Un esempio di variazione del costo assicurativo in funzione del livello di protezione

- La valutazione dell'insieme della gestione della sicurezza determina la valutazione del rischio residuo (quantificato in costi assicurativi)



ace europe

ESEMPIO DI SINISTRO

Ditta:	Impresa per servizi finanziari
Impianti:	pochi PC in rete
Somma assicurata:	assicurato solo hardware
Cause del sinistro:	Cortocircuito nel server (danneggiato durante l'evento). Il back-up non è entrato subito in funzione
Indennizzo:	inferiore alle aspettative perché non risultavano assicurati : programmi,dati,danni indiretti,spese extra costituenti il 1900 % delle perdite

ace europe

ESEMPIO DI SINISTRO

Ditta:	Impresa metallurgica
Impianti:	PC in rete
Somma assicurata:	troppo bassa
Causa del sinistro:	Virus (parity B virus, “AIDS”)
Danno:	molto superiore al capitale ass.to Guasto del sistema di sicurezza, impresa d’assistenza inesperta in questo tipo di virus. Ha aggravato il danno resettando un disco rigido del server
Indennizzo :	nessuno ,non erano assicurati su rischi IT

ace europe

ESEMPIO DI SINISTRO

Ditta:	Impresa di produzione
Impianti:	AS/400 (capacità bassa in Gbyte)
Somma assicurata:	insufficente (per programmi e dati)
Causa del sinistro:	Inondazione locali aziendali
Costi: :	Guasto del sistema di back-up, + adattamento dei dati al nuovo sistema di back-up
Indennizzo :	danni molto superiori agli importi assicurati

ace europe

ESEMPIO DI SINISTRO

Ditta:	Ufficio tecnico di progettazione
Impianti:	PC in rete con server, scanner dati numerici e soprattutto grafici
Somma assicurata:	insufficiente (programmi dati),assente la copertura danni indiretti.
Cause del sinistro:	Guasto del sistema, caduta della testina del disco.
Indennizzo:	500 h di input manuale per i dati numerici, 3500 h x quelli grafici , zero per danni indiretti (non assicurati).
Maggiori perdite :	perdita di clienti dovuti all'impossibilità di rispettare gli impegni presi ,incremento delle spese (stipendi) perdita dell'utile dell'anno.

ace europe

ESEMPIO DI SINISTRO

Ditta:	Attività per conto terzi
Cause del sinistro:	Intrusione CYBERCRIME . Danni provocati dall'impossibilità di verificare la bontà di funzionamento dei sistemi. Nonostante l'ottima collaborazione fra la Ditta Assicurata e tutte le parti interessate (utenti, fornitori, ecc.) il sinistro provocò 4 settimane di interruzione di attività.
Costi:	per la ricostruzione del back-up di n . settimane di funzionamento "anomalo" con ripulizia controllo di tutti i files. Per sostenere cause di responsabilità per danni a terzi (clienti e non)
Indennizzo :	nessuno non erano assicurati su rischi IT

ace europe

ESEMPIO DI SINISTRO

Ditta:	Settore del Credito
Cause del Sinistro:	Negligenza. Nel sostenere un forte afflusso di acquisti sul mercato borsistico gli operatori effettuarono operazioni fuori standard (forzature)rendendo inefficienti i controlli standard. La successiva ondata di vendite non trovò conferma su ordini di acquisto in stand by (non definitivi) dalla quale emerse una differenza (perdita) sostenuta .
Costi:	l'intero importo del totale delle differenze dovette essere caricato sui conti dei clienti per evitare lo scandalo.
Indennizzo :	nessuno non erano assicurati contro gli errori umani.

ace europe

ESEMPIO DI SINISTRO

Ditta:	Ufficio di amministrazione immobiliare
Cause del Sinistro:	Impianto di aria condizionata erroneamente installato sul soffitto e mancanza di svuotamento della vasca di raccolta dell'acqua di condensa. Colaggio dell'acqua sui cavi dei server causando numerosi corto circuiti a seguito dei quali andarono persi banche dati non correttamente salvate in luogo sicuro .
Danno:	notevole in proporzione alla dimensione dell'azienda
Indennizzo :	non significativo perché il grosso del danno non era assicurato (danni indiretti).

ace europe

ESEMPIO DI SINISTRO

Tipo di sinistro:	Perdita (crollo) del valore delle azioni sul mercato borsistico
Tipo di azienda:	Software Engineering
Caratteristiche del Sinistro:	Attacco al sito Web dell'azienda + modifica di messaggi per altri siti
Costi Totali:	Elevati 7/8 giorni lavorativi per la società di consulenza 10 giorni lavorativi per le risorse interne
Indennizzo:	sufficiente ma non esaustivo in quanto una parte del rischio era stata coperta.

ace europe

ESEMPIO SI SINISTRO

Tipo di Azienda: Settore I.T.

Caratteristiche del Sinistro: Perdita apparente di posta nelle caselle e-mail (in entrata e in uscita). Perdita dell'intera posta elettronica aziendale (per un periodo di ore limitate).

Tipo di sinistro:
- spese per individuare i malfunzionamenti del sistema e il colpevole
- perdita di tempo e malfunzionamenti nella messaggistica
- altri danni evitati dalla velocità di reazione del responsabile della sicurezza

Costi totali: Elevati

Indennizzo: Elevato

ace europe

ESEMPIO DI SINISTRO

Tipo di Azienda:	Commercio al Dettaglio
Tipo di Sinistro:	Intrusione on-line (“war driving”)
Caratteristiche del Sinistro:	Spese per l’individuazione del responsabile del Cyber Crime. Pronta reazione del personale della sicurezza informatica
Spese sostenute:	Notevoli – Si parla di 15 giorni di lavoro della società di consulenza specializzata
Indennizzo :	nessuno non avevano una copertura IT

ace europe

ESEMPIO DI SINISTRO

Tipo di Azienda:	Società di Software Engineering
Tipo di sinistro:	Cyber Crime (attacco Back-door)
Danni subiti:	Limitati poiché l'intrusione è stata subito scoperta dal responsabile della sicurezza rilevando immediatamente un'anomalia nel server DNS tramite un programma di controllo auto-progettato per bloccare subito l'effetto dell'intrusione. Circa 2 giorni lavorativi di cui 1 di azienda esterna specializzata per rilevare il meccanismo dell'intrusione.
Indennizzo:	notevole

ace europe

ESEMPIO DI SINISTRO

Tipo di azienda:	Società di Engineering
Tipo di attacco:	Penetrazione nel sistema tramite intercettazione di corrispondenza inviata via radio diffusione non criptata
Danni subiti:	Nonostante l'intrusione sia stata rilevata fin dalle prime fasi, è servita una prima settimana di lavoro per capire qual era effettivamente il problema e una seconda per effettuare controlli e contromisure.
Indennizzo:	nessuno,non c'era un copertura IT

ace europe

ESEMPIO DI SINISTRO

Tipo di azienda:	Società specializzata nella ricerca genetica
Tipo di attacco:	Infedeltà dipendenti combinata con penetrazione nel sistema informatico
Danni subiti:	Non quantificabili in quanto il risultato della ricerca aziendale avrebbe consentito di acquisire importanti contratti con committenti di livello nazionale ed internazionale. Tutt'ora in corso procedimento legale con i concorrenti con procedimento penale nei confronti dell'ex-ricercatore
Indennizzo :	nessuno non esisteva nessuna copertura.

ace europe

ESEMPIO DI SINISTRO

Tipo di azienda:	Azienda di servizi finanziari (consulenza per investimenti e altri servizi connessi)
Tipo di attacco:	Unicode Attack
Danni subiti:	Fortunatamente, il responsabile dell'azienda aveva prontamente individuato e iniziato la reazione, ed è solo per questo motivo che le diverse centinaia di aziende colpite non hanno fatto causa alla sorgente dell'infezione (la macchina *Solaris* da cui è partito l'attacco) .
Indennizzo:	sufficiente a coprire tutte le spese (esisteva copertura completa).

ace europe

ESEMPIO DI SINISTRO

Tipo di azienda:	Banca on-line (Virtual Banking)
Obiettivo:	Furto di informazioni sensibili e critiche e successiva azione di estorsione informatica
Danni subiti:	Sostituzione integrale del server con un altro sano e ricostruzione completa del sistema a partire da versioni originali. Spese legali per depositare copie speculari del sistema effettuate dalle autorità. Spese per agenzia investigativa privata specializzata (con l'obiettivo di scoprire l'autore dell'intrusione)

ace europe

ESEMPIO DI SINISTRO

Tipo di azienda: Commercio on-line

Tipo di attacco: Attacco da parte di Cracker che è riuscito ad accedere al sistema inserendosi come “Administrator” .

Effetti: Arresto dell’attività per consentire la sostituzione completa di tute le macchine collegate a quella colpita (dato la situazione della funzione di Administrator effettuata dal cracker). Spese e costi ingenti e possibili danni a terzi (ancora in fase di definizione) .

ace europe

ESEMPIO DI SINISTRO

Tipo di azienda:	Stabilimento di produzione semiconduttori
Evento:	Intrusione accidentale in rete wireless aziendale
Tipo di danno:	fortunatamente non c'è stata nessuna denuncia alle autorità ed è stato possibile dimostrare la buona fede dei dipendenti e la casualità dell'intrusione e procedere in 2 giorni a controllare tutta la rete.
Indennizzo:	nessuno .

ace europe

ESEMPIO DI SINISTRO

Attività:	Servizi di elaborazione dati per conto terzi
Tipo di danno:	Malfunzionamento del servizio di condizionamento della sala principale
Danni subiti:	Arresto di elaborazione (4 ore) e, in seguito all'intervento del manutentore dell'impianto, rallentamento nell'elaborazione dei dati (sette giorni). Danneggiamento dell'attività di qualche centinaia di punti vendita (clienti) e relativo ricorso per svariate centinaia di migliaia di Euro.
Indennizzo :	cause civili in corso .

ace europe

ESEMPIO DI SINISTRO

Attività:	Servizi di elaborazione dati per conto terzi
Tipo di danno:	Dolo / infedeltà dipendenti .
Danni subiti:	Furto di database , alterazione di SW di controllo e vendita illegale di database contenenti dati sensibili di terzi. Costi per disinfestazione dei sistemi ,sostituzione di intere macchine (in emergenza per non arrestare totalmente le attività di servizio. Costi per recuperare le informazioni e per evitare che le medesime potessero essere utilizzate per scopi illeciti.Perdite di profitto dovute a sconti e special agreement con clienti per evitare denunce e cause ,spese legali e di marketing.
Indennizzo :	nessuno,non erano assicurati sopra l'evento.

ace europe

AGENDA

2. **La copertura RC per gli operatori della sicurezza informatica:**
   - **Sicurezza informatica**
   - **Fonti di responsabilità**
   - **Quali protezioni adottare?**
   - **Perché una copertura RC "infomatica" e non "contrattuale" per le società di servizi?**

ace europe

Sicurezza informatica

Non esiste un sistema informatico sicuro ed inattaccabile

La sicurezza informatica ha l'obiettivo di garantire un adeguato grado di protezione dei dati e delle informazioni (Security Management), riducendo i "rischi informatici":

- ✓ **virus e bugs**
- ✓ **violazione privacy**
- ✓ **interruzione trasmissioni**
- ✓ **hacking**
- ✓ **frode informatica**
- ✓ **errori nella elaborazione dei risultati nei prodotti software**

ace europe

Fonti di responsabilità

Responsabilità penale:

- **art. 169 del Nuovo T.U. Privacy (d.l. 27/06/2003): omessa adozione di misure necessarie alla sicurezza dei dati**

Responsabilità civile:

- **art. 2050 c.c.: in base all'art. 15 del Nuovo T.U. Privacy il trattamento dei dati personali rappresenta esercizio di attività pericolosa e quindi l'operatore deve fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire la sicurezza dei dati**
- **art. 2049 c.c.: responsabilità del datore di lavoro per fatti illeciti del proprio dipendente**
- **art. 2043 c.c.: qualunque atto illecito che crea un danno ingiusto a terzi**

ace europe

Quali protezioni adottare?

Quali soluzioni adottare per ridurre la possibilità che si verifichi un danno al sistema informatico e garantire la tranquillità operativa?

Soluzioni fisiche e logiche (a titolo esemplificativo):

- ✓ **procedure di back-up**
- ✓ **piani di recovery per garantire business continuity**
- ✓ **antivirus**
- ✓ **sicurezza degli accessi**

Soluzioni giuridiche:

- ✓ **contratti**
- ✓ **polizze assicurative**

ace europe

Perché una copertura RC "informatica" e non "contrattuale" per le società di servizi?

Le soluzioni utili e necessarie per affrontare la sicurezza informatica sono fornite nell'ambito delle moderne competenze professionali dalle cosiddette "società di servizi".

L'attività aziendale delle società che forniscono servizi informatici è variegata e comporta una pluralità di rischi che necessitano coperture assicurative adeguate, innovative e personalizzate.

Le aziende clienti/utenti, infatti, si tutelano da eventuali problemi di fornitura e gestione del servizio dato in outsourcing definendo obblighi contrattuali e responsabilità.

La società di servizi non può sostenere da sola tutte le potenziali lamentele dei clienti/utenti.

ace europe

AGENDA

3. **L'assicurazione come trasferimento del rischio residuo: Basilea II**
   - **Basilea II: nuove regole sulla gestione del rischio**
   - **Basilea II: azioni da intraprendere**
   - **Basilea II: difficoltà di attuazione**
   - **Quale alternativa?**
   - **Rischi trasferibili all'assicurazione**

ace europe

Basilea II: nuove regole sulla gestione del rischio

Definizione di indicatori per il calcolo della quota di riserva capitale correlati al rischio operativo.

Rischio operativo → **rischio di perdite risultanti da inadeguatezza o fallimento di:**

- **processi interni**
- **persone o sistemi**
- **eventi esterni**

Le Istituzioni Finanziarie devono identificare le fonti del rischio operativo per calcolare la riserva capitale richiesta e valutare l'opportunità di trasferire all'assicurazione il rischio residuo.

ace europe

Basilea II: Azioni da intraprendere

Le Istituzioni Finanziarie devono:

- ✓ **Creare il responsabile della sicurezza I.T.**
- ✓ **Assegnare ruoli e responsabilità per la gestione del rischio I.T.**
- ✓ **Sviluppare soluzioni per la gestione real time del rischio**
- ✓ **Attivare processi di gestione degli incidenti transazionali**
- ✓ **Misurare e testare i livelli di sicurezza**

ace europe

Basilea II: Difficoltà di attuazione

Perchè le Istituzioni Finanziarie hanno difficoltà ad attuare le azioni richieste ?

- ✓ **Mancanza di skills adeguate**
- ✓ **Minacce nuove, non prevedibili e non identificabili**
- ✓ **Sistemi di sicurezza informatica (firewall, antivirus, …) non "totalmente sicuri"**

ace europe

Basilea II: quale alternativa?

Non tutti i rischi possono essere identificati e adeguatamente coperti con una riserva di capitale

Valutare l'opportunità di trasferire all'assicurazione il rischio residuo per coprire:

- ✓ **perdite di dati e programmi**
- ✓ **spese extra in caso di disaster recovery**
- ✓ **perdita di profitto**
- ✓ **responsabilità civile per servizi di informatica errati o inadeguati**
- ✓ **spese di ricostruzione dell'immagine**

ace europe

Rischi trasferibili all'assicurazione

Copertura assicurativa per:

- **Aziende la cui attività si svolge sul web**
- **Aziende che utilizzano il web e sistemi informatici per lo svolgimento della propria attività**

Rischi trasferibili:

- **Violazione proprietà intellettuale e privacy**
- **Perdite finanziarie causate a terzi per malfunzionamento del proprio sistema informatico**
- **Richieste di risarcimento per danni causati da virus informatici**
- **Errori/omissioni/negligenze nell'utilizzo di prodotti software**

ace europe

Come è strutturata la copertura assicurativa RC?

A. **Responsabilità Civile Professionale per negligenza, errori od omissioni nella fornitura o mancata fornitura di servizi professionali**

B. **Responsabilità Civile per creazione di programmi software**

C. **Responsabilità Civile per negligenza, errori od omissioni nella fornitura di servizi telematici o informatici (diffamazione, violazione della privacy, frode informatica, virus informatici, mancato accesso al servizio, accesso non autorizzato, violazione di copyright,…)**