25 years of insuring progress

Quando il “cervellone” perde la memoria

panorama sul trasferimento dei rischi informatici dalle aziende al mondo assicurativo

Club degli assicuratori

2012

Riccardo Scalici

SOMMARIO ARGOMENTI : Prima Parte / Seconda parte.

INTRODUZIONE

- **Dai sinistri informatici alla ricerca di una protezione assicurativa**

PRIMA PARTE

- **Un abaco dei rischi e delle coperture informatiche.**
- **L'analisi di rischio.**

SECONDA PARTE

- **I capitali da assicurare e le condizioni particolari nei diversi settori.**

Panorama sul trasferimento dei rischi informatici dalle aziende al mondo assicurativo

- prima parte -

INTRODUZIONE

- **Dai sinistri informatici alla ricerca di una protezione assicurativa**

Esempi di eventi dannosi subiti dalle aziende esempio 1 (fonte : ACE) – **PERDITA di DATA – da MALWARE -**

Tipologia di azienda:	**metalmeccanica (ITALIA).**
Tipologia di danno:	**perdita dei data.**
Area colpita:	**controllo produzione.**
Causa:	**rottura disco principale e successiva rottura disco di back-up dovuto a malware.**
Effetti:	**arresto totale attività di 4 giorni.**
Danno diretto:	**costo di ricostruzione data 50.000 €.**
Danno indiretto:	**perdita ordinativi (stima 600.000€) + lavori straordinari,notturni e festivi per recupero produzione (60.000€).**
Indennizzo:	**assenza di copertura assicurativa sotto la polizza All Risks Incendio (esclusi i danni immateriali).**
Recupero:	**nessuno – gli ordinativi persi sono stati acquisiti dalla concorrenza.**

Esempi di eventi dannosi subiti dalle aziende esempio 2 (fonte : ACE) – MALWARE -

Tipo di azienda:	**Ente pubblico (Italia)**
Tipologia di danno:	**Malware vari**
Area colpita:	**network pc/server**
Parte a rischio:	**riservatezza e integrità sistema**
Effetti:	**3 giorni circa di fermo/rallentamento per 10.000pc**
Danno diretto stimato:	**diretto 0,5 milioni € per spese di disinfestazione**
Danno indiretto?:	**solo per stipendi dipendenti inattivi 1,5 milioni €**
Causa:	**assenza di una politica centralizzata del sistema e della sicurezza**
Indennizzo:	**Nessuno, la polizza incendio AR non copre i danni informatici.**

25 years of insuring progress

Esempi di eventi dannosi subiti dalle aziende esempio 3 (fonte : ACE) – **ERRORE UMANO** -

Tipo di azienda:	**Operatore telefonia mobile (Italia)**
Tipologia di danno:	**Errore operativo del personale addetto**
Area colpita:	**Capacità del sistema a gestire il volume delle connessioni telefoniche**
Effetti:	**24 ore di malfunzionamento delle telecomunicazioni**
Danno indiretto?:	**8 milioni € (stima)**
Causa:	**la riallocazione del set up delle "HLRutomatic additional memory" ad una soglia che eccedeva le capacità del sistema.**
Indennizzo :	**nessuno , la polizza elettronica non può essere estesa alla fattispecie di rischio.**

25 years of insuring progress

Esempi di eventi dannosi subiti dalle aziende esempio 4 (fonte : ACE) – **ERRORE UMANO** -

Tipo di azienda:	**servizi informatici Bancari (Italia).**
Tipologia di danno:	**errore umano (imp.nuova piattaforma).**
Area colpita:	**il sistema principale.**
Funzione:	**Gestione conti correnti.**
Parte a rischio:	**elaborazione di 3,5 milioni CC.**
Danno subito:	**fermo totale di 0,5 giorni + 0,5 giorni ricarico vecchia piattaforma revisione errori e ricarico nuova piattaforma 1,5 giorni (+ 70-80 giorni di lavoro per riallineamento, controlli,ripristino agenzie).**
Sinistro:	**2,5 milioni di sole spese extra ,**
Indennizzo:	**assente (assenza di assicurazione per la fattispecie)la polizza BBB nella sezione elettronica non può essere estesa a questo rischio.**

25 years of insuring progress

- Un abaco dei rischi e delle coperture informatiche.
- L’analisi di rischio.

Prima parte

Riccardo Scalici

Dai sinistri informatici alla ricerca di una protezione assicurativa

1

Cos'è un incidente informatico ?

Un evento dannoso accaduto nella parte non materiale dei sistemi informatici, i macchinari e impianti non sono colpiti da nessun accidente, ma programmi e dati non sono utilizzabili , le operazioni che dipendono dal processo elaborativo sono rallentate o fermate o danno risultati non conformi.

Le spese di ripristino dell'attività e le perdite economiche conseguenti al malfunzionamento o fermo dell'attività non sono assicurate sotto le polizze incendio.

La richiesta di copertura assicurativa sopra gli incidenti informatici ha avuto come risposta le polizze informatiche.

L'Italia è un paese a rischio ?

Crescita degli attacchi malevoli in Italia , nel 2011 pari a + 81% alla ricerca di dati sensibili vendibili sul mercato nero.

Nel mirino aziende con meno di 250 dipendenti (18% degli attacchi), anche le ns PMI sono nel mirino dei criminali.

L'Italia è al primo posto in EMEA per il numero di PC infettati controllati da remoto (bot) , quarto paese a livello mondiale.

Le principali motivazioni di attacco informatico (EMEA) :

55% ……frodi informatiche

47%……..vandalismo (seppur di tipo informatico)

42%……..sabotaggio e

27%……..spionaggio

23%……..l'azione dimostrativa

15%……..ricatti

05%……..terrorismo

Le nostre aziende in un Paese a Rischio (1)

Rank	World Rank	Target Country	Percentage of Attacks	World Percentage of Attacks
1	7	Italy	29%	4%
2	1	United States	10%	24%
3	9	Japan	8%	3%
4	8	Russia	7%	3%
5	5	France	6%	4%
6	2	Germany	4%	7%
7	17	Poland	4%	2%
8	4	China	3%	5%
9	3	United Kingdom	3%	6%
10	14	Taiwan	2%	2%

Fonte Symantec ISTR XVI. Origin of Attacks targeting Italy

Rank				Percentage		
2010 EMEA	2009 EMEA	2010 Global	Country	2010 EMEA	2009 EMEA	2010 Global
1	1	2	Germany	20%	14%	12%
2	2	4	Italy	15%	12%	9%
3	8	7	United Kingdom	11%	5%	7%
4	4	8	Poland	8%	12%	5%
5	3	10	Spain	7%	12%	4%
6	9	11	Hungary	6%	4%	4%
7	6	12	France	6%	7%	4%
8	7	14	Portugal	3%	5%	2%
9	5	15	Turkey	3%	7%	2%
10	10	17	Israel	3%	3%	2%

Fonte Symantec ISTR XVI. Bot-infected computers by country, EMEA

ACE 25 years of insuring progress

Le nostre aziende in un Paese a Rischio (2)

Country Rank	World Rank	City	Country Percentage of Bots	World Percentage of Bots
1	5	Roma	65%	2%
2	25	Milano	21%	1%
3	75	Cagliari	6%	< 1%
4	281	Arezzo	1%	< 1%
5	562	Torino	< 1%	< 1%
6	576	Venezia	< 1%	< 1%
7	695	Bologna	< 1%	< 1%
8	721	Perugia	< 1%	< 1%
9	764	Firenze	< 1%	< 1%
10	778	Bolzano	< 1%	< 1%

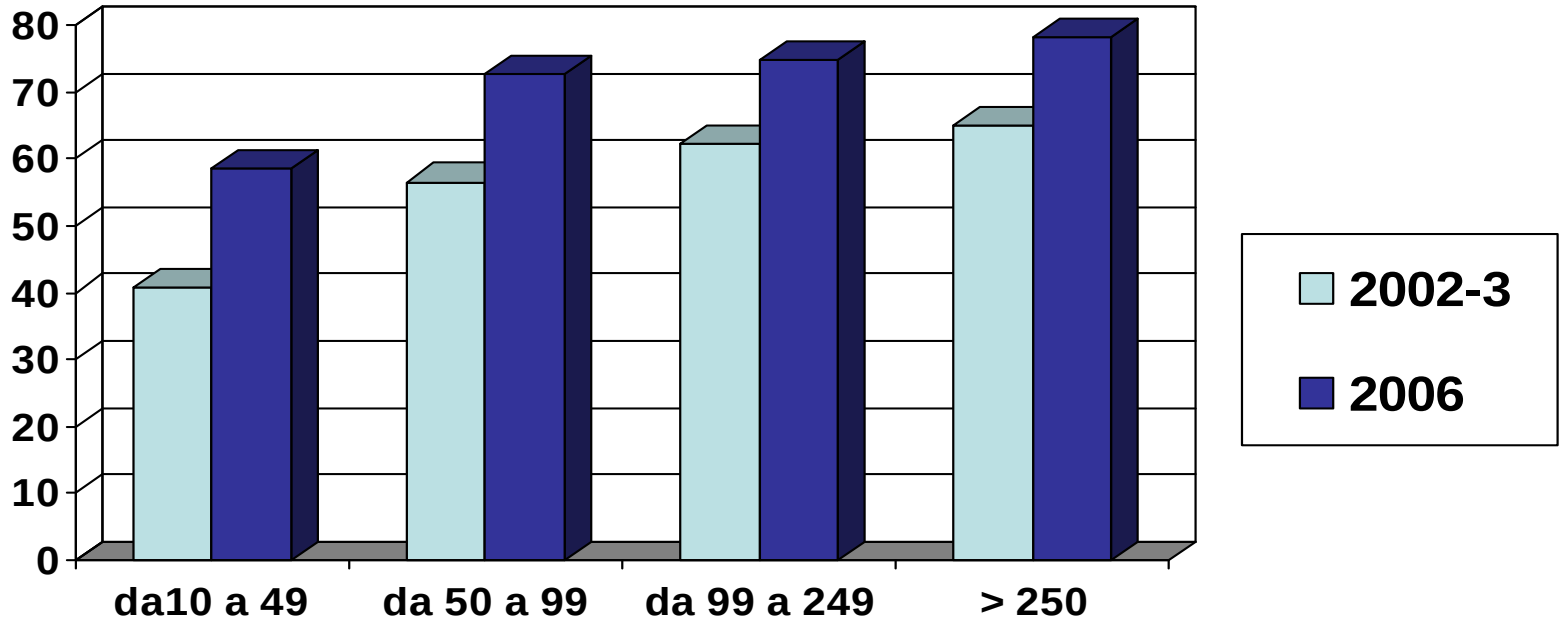
Fonte Symantec ISTR XVI. Bots by City – Italy

Rank			Country	Percentage			Top Sector Targeted in Country	Percentage of URLs Targeting Sector
2010 EMEA	2009 EMEA	2010 Global		2010 EMEA	2009 EMEA	2010 Global		
1	10	2	Netherlands	26%	4%	8%	Financial	89%
2	6	4	Germany	13%	8%	4%	Financial	73%
3	5	5	United Kingdom	12%	9%	4%	Financial	84%
4	8	6	Italy	10%	5%	3%	Financial	89%
5	7	7	France	9%	6%	3%	Financial	84%
6	4	9	Russia	6%	9%	2%	Financial	70%
7	17	13	Bulgaria	3%	1%	1%	Insurance	62%
8	2	14	Poland	3%	11%	1%	Financial	86%
9	1	5	Spain	3%	11%	1%	Financial	79%
10	14	16	Ukraine	2%	2%	1%	Financial	69%

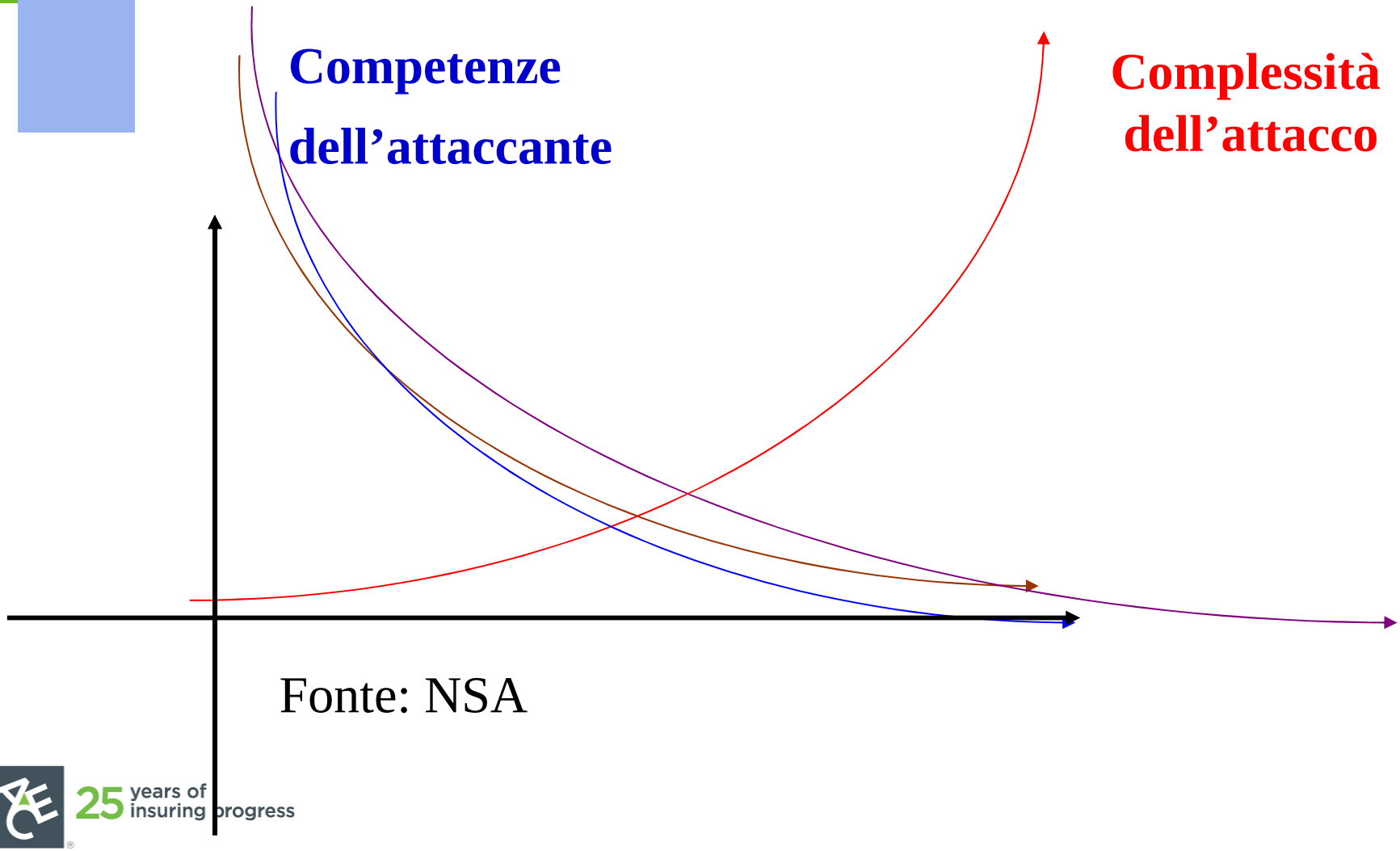
Fonte Symantec ISTR XVI. Top countries hosting phishing URLs and top targeted sectors, EMEA

Information technology
in ITALIA : frequenza eventi (fonte istat)

Problemi sicurezza : attacco malware ,le %
(suddivisione dimensione aziende x nr di dipendenti)

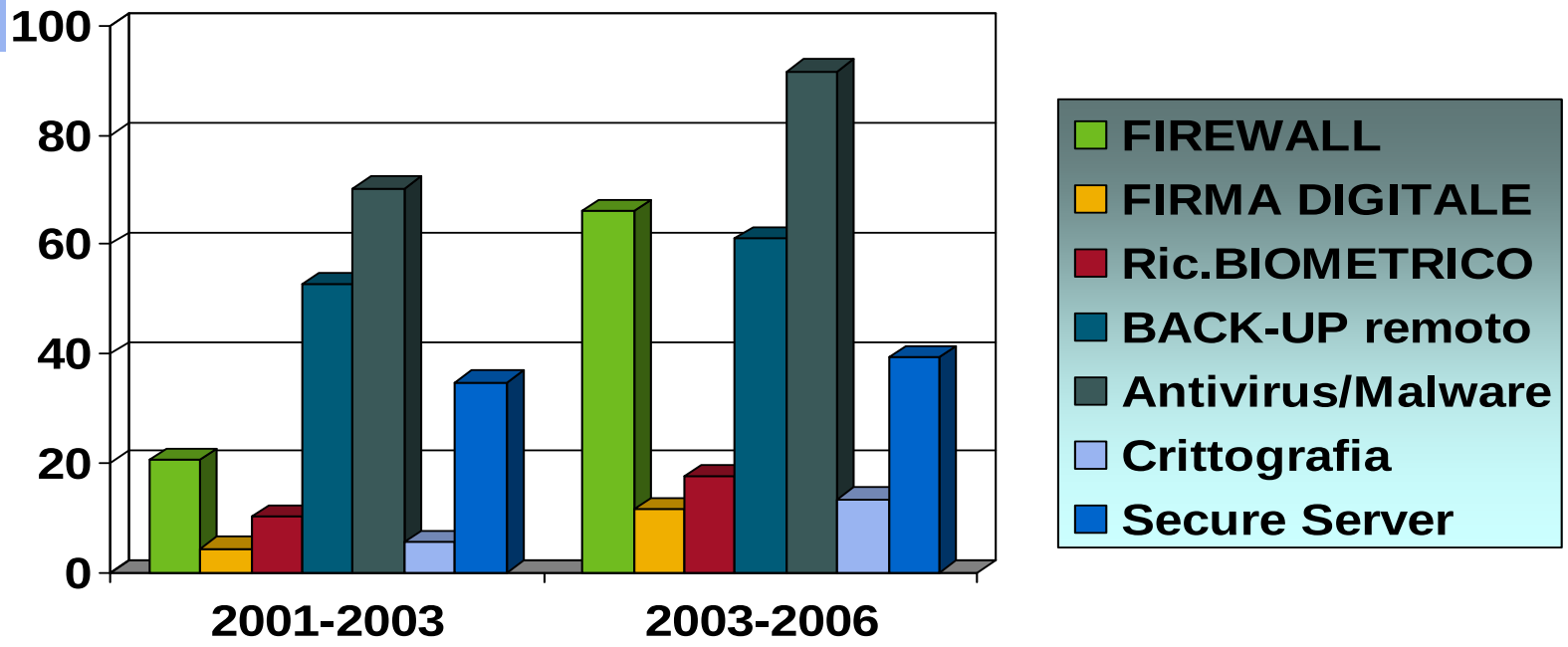


Protezioni I.T. e attacchi
ai sistemi



Fonte: NSA

Le aziende italiane si attrezzano nelle migliori difese e protezioni (elab.dati Istat)

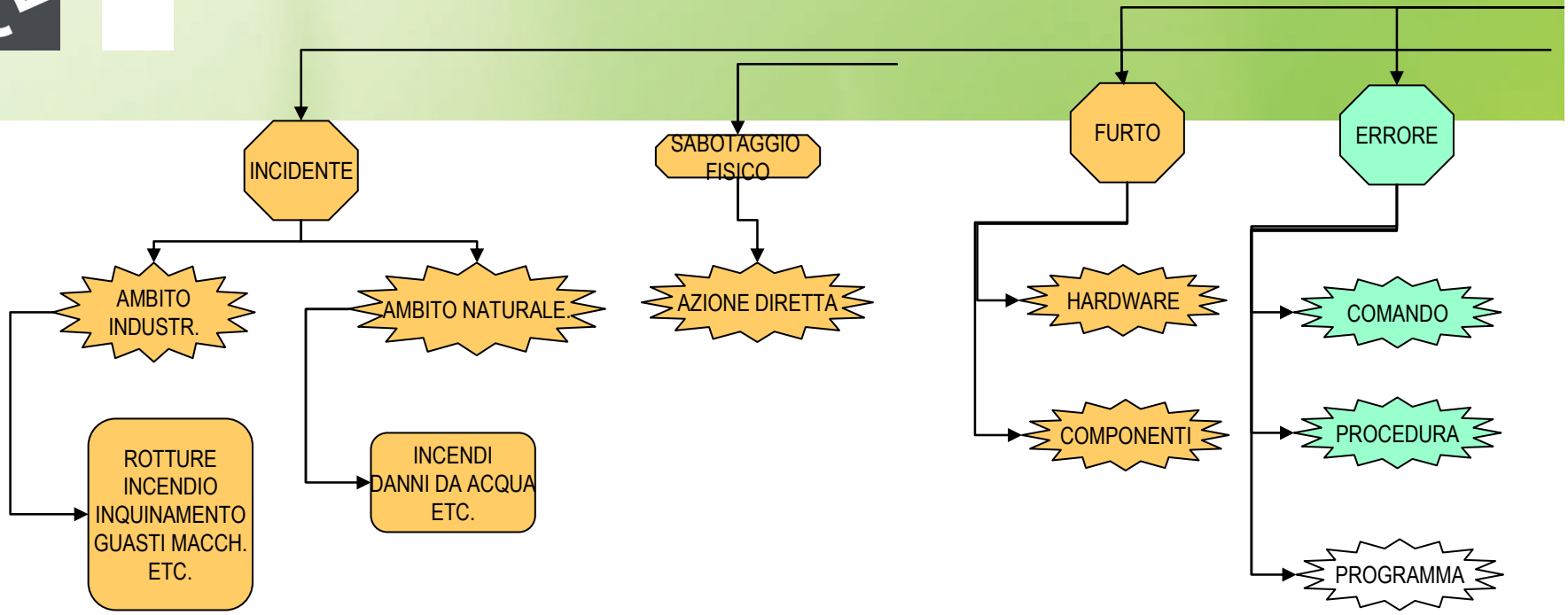


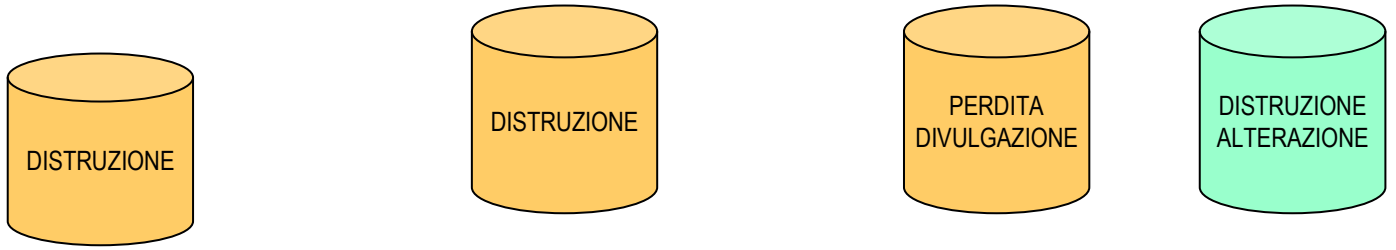
La sicurezza informatica non è diversa da quella di altri campi

Rimane sempre un rischio residuo !

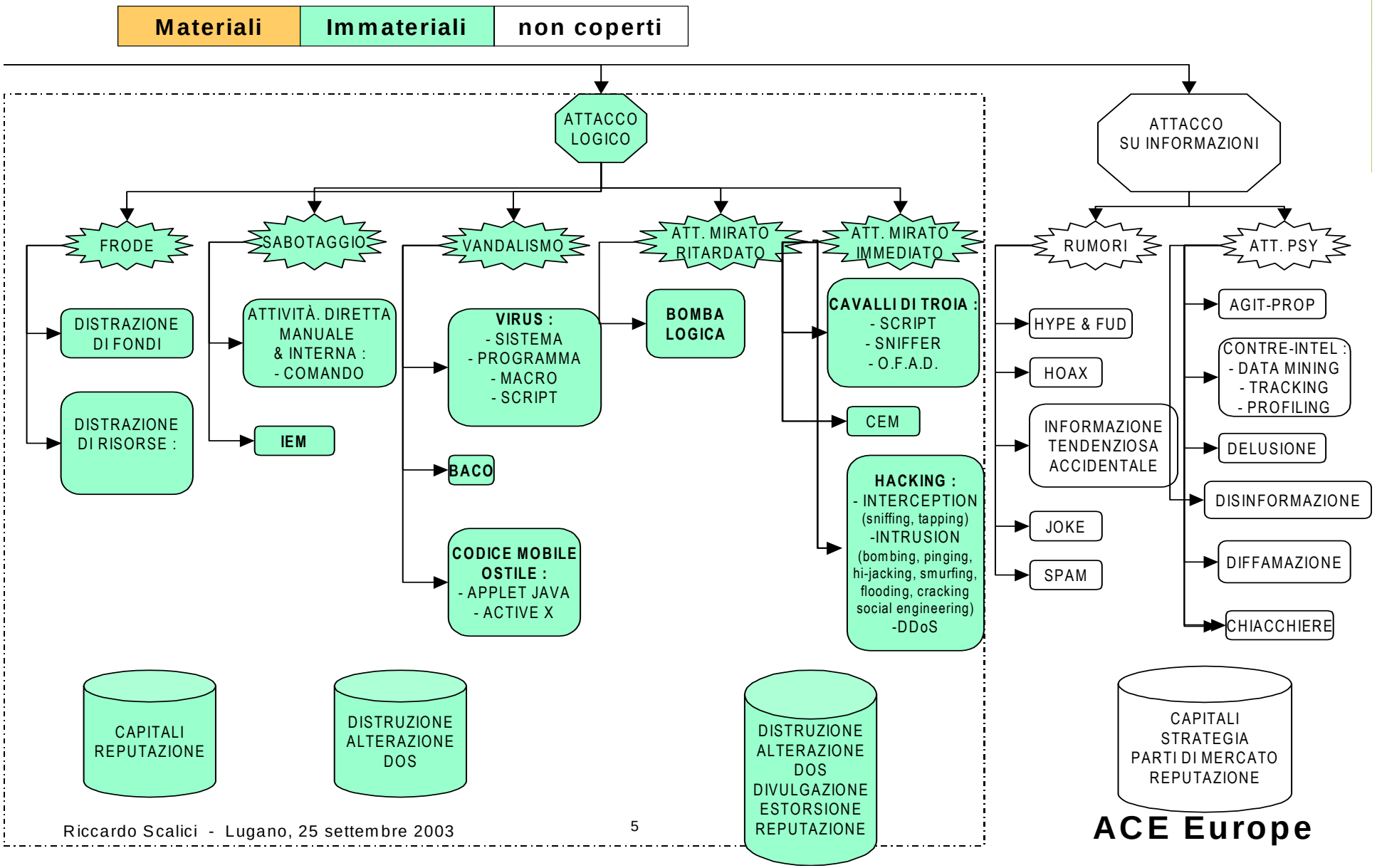
Materiali | Immateriali | Non coperti

Rischi Informatici 1/2

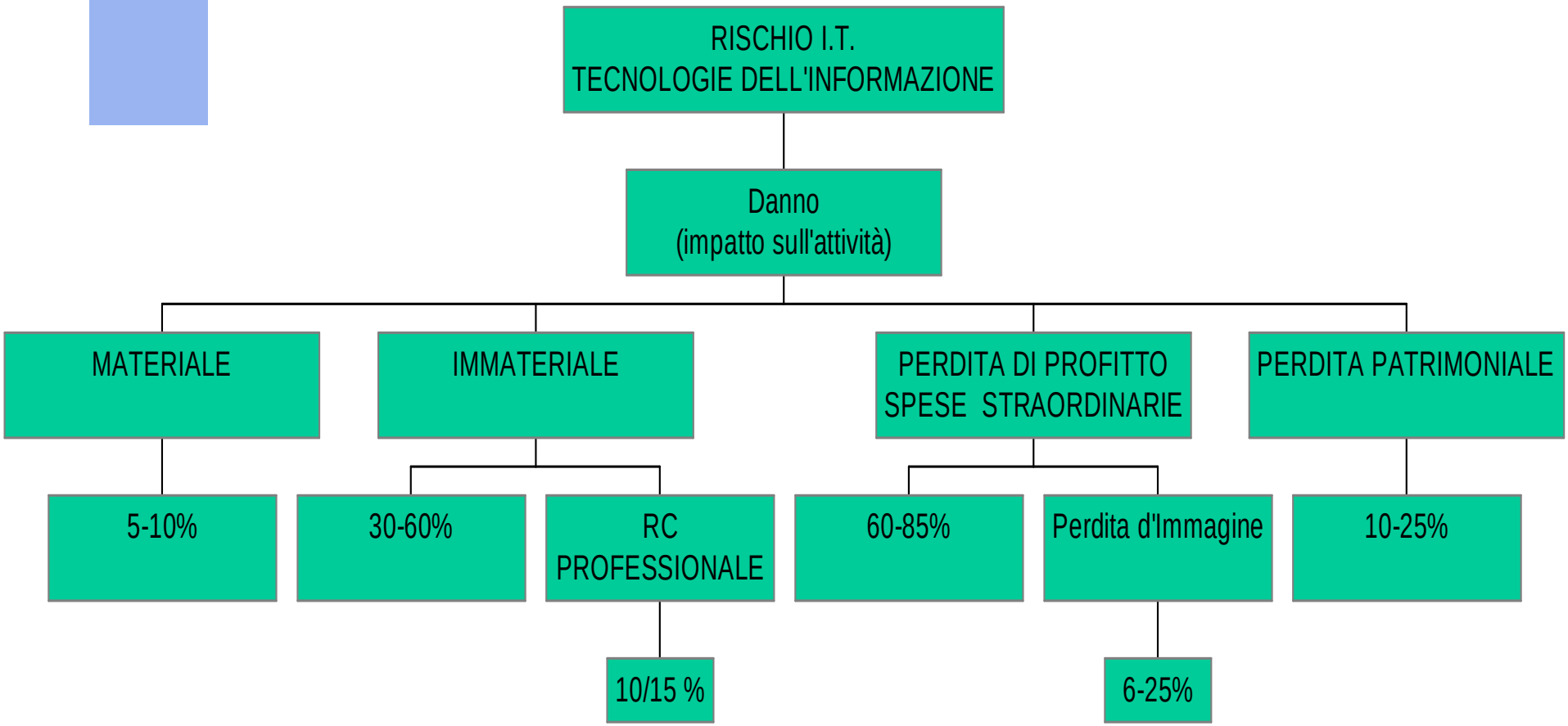




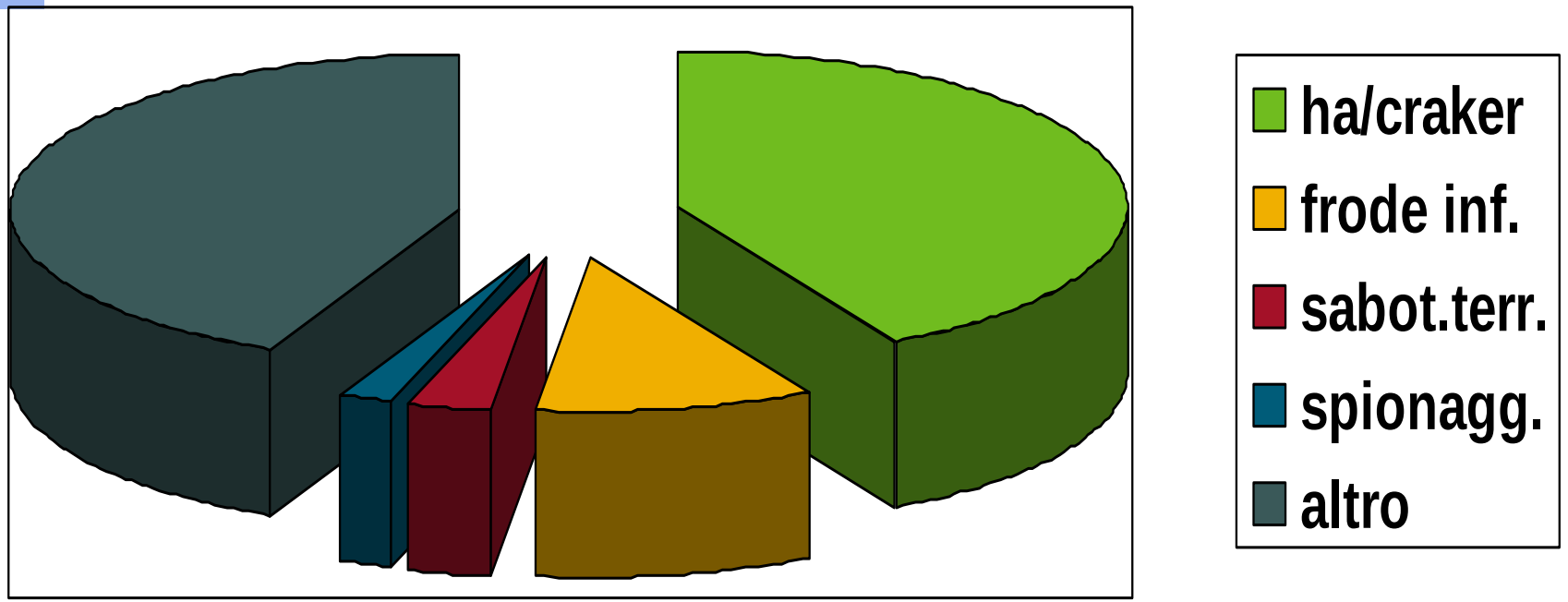
Rischi informatici 2/2



ABACO dei rischi IT



Information technology
in EUROPA : frequenza eventi



Introduzione alle protezioni assicurative dei rischi Information technology

Più che il solito contratto di assicurazione, necessita un prodotto studiato per la protezione finanziaria di tutte attività fortemente dipendenti dalle tecnologie dell'informazione .

L'analisi di rischio : metodologia

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

Gli standard di riferimento

Danni materiali : NFPA (USA)

Danni informatici : BS17799 / ISO equiv.

Danni economici : Basilea 2 (e succ.)

Danni al Brand : Fair value

Responsabilità : Sarbane O./ISO equiv.

STIMA DEL MASSIMO DANNO PROBABILE

Dal punti di vista assicurativo la stima del massimo danno probabile riveste storicamente una grande importanza.

Il principio sul quale si basa è certamente nuovo rispetto a stime di altri settori (ivi comprese quelle degli addetti alla sicurezza e alla pratica di molti Risk Manager aziendali) .

Esso nasce dall'esperienza dei sinistri reali e non di quelli teoricamente "prevedibili" , e si sostanzia nel prevedere *l'impatto economico massimo prevedibile in assenza di un corretto funzionamento delle protezioni antidanno attive.*

25 years of insuring progress

I capitali da assicurare e le condizioni particolari nei diversi settori.

Seconda parte

Riccardo Scalici

Il Contratto

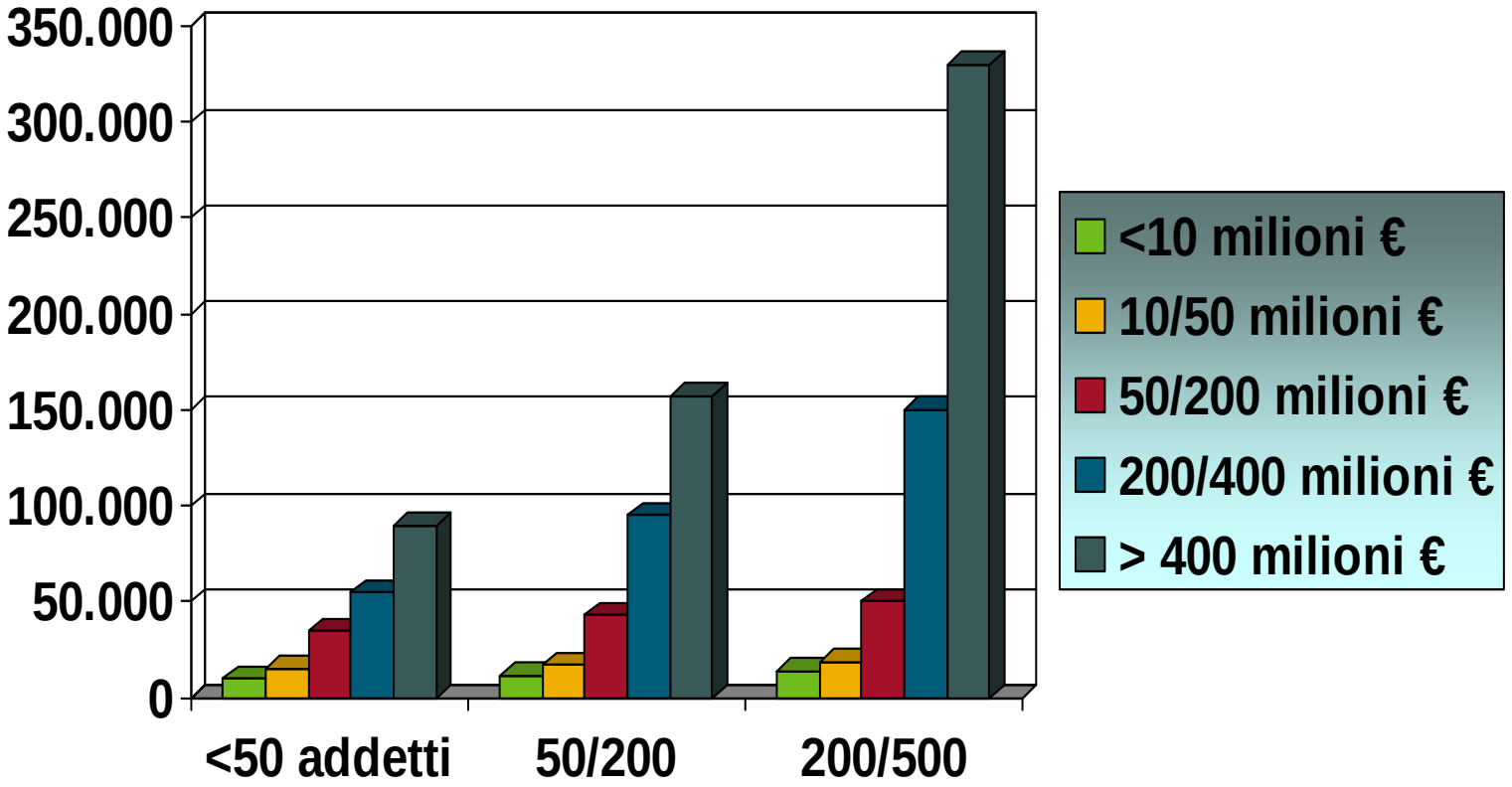
L’esperienza ha insegnato che il rapporto tra costi e benefici determina la concentrazione della protezione assicurativa nell’area del massimo danno probabile *(appena sopra i rischi di frequenza,e non tenendo in considerazione i rischi di distruzione totale).*

Ottenendo così economie nei costi assicurativi ,e ampio spettro di copertura sui rischi emergenti.

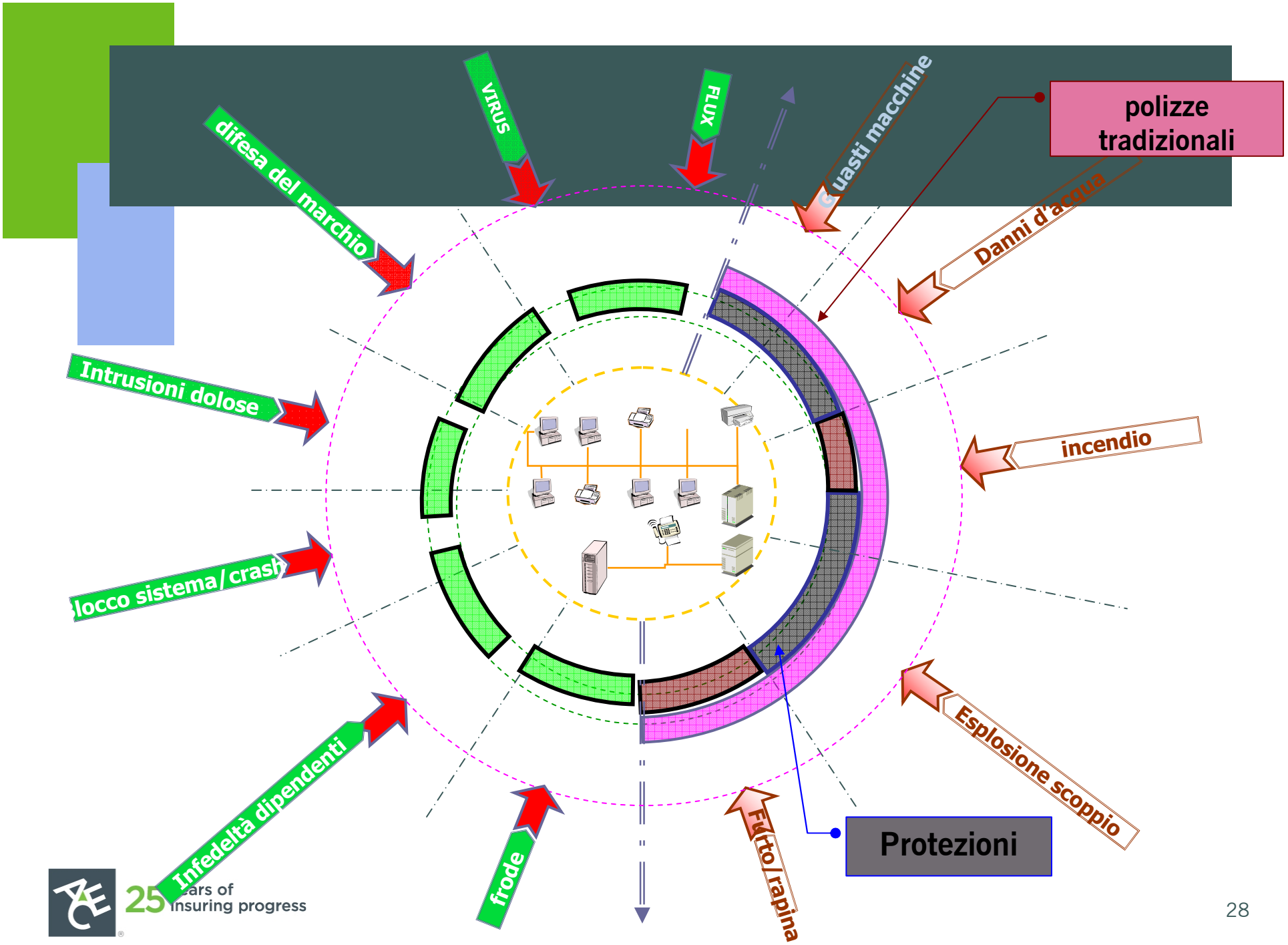
Le somme assicurate non saranno vincolate all’effettivo costo di ricostruzione di tutti i dati potenzialmente registrabili nella capacità di memoria del sistema, così come per le perdite economiche saranno assicurate per l’importo massimo corrispondente alle perdite di uno o più mesi .

Massimo danno economico medio giornaliero in migliaia € per classe di fatturato/nr di addetti

proiezioni PML su campioni di clienti
- fonte ACE IT -



25 years of insuring progress


difesa del marchio
VIRUS
FLUX
Guasti macchine
polizze tradizionali
Danni d'acqua
Intrusioni dolose
incendio
Blocco sistema/crash
Esplosione scoppio
Infedeltà dipendenti
frode
Furto/rapina
Protezioni

Gli eventi generatori

Gli <u>eventi generatori</u> sono chiaramente identificabili :

- **Un Virus ,un'istruzione o un programma dannosi.**
- **Un'azione dolosa da parte di un dipendente ,di un terzo,di un cracker.**
- **Un'azione informatica che costituisca violazione della privacy .**
- **Un evento naturale come l'effetto indiretto del fulmine, la scarica elettrostratica.**
- **L'infedeltà dei dipendenti che generi perdita di funzionalità ,aumento di spese,distrazione di fondi ,utilizzo indebito di fondi di clienti.**
- **L'intervento di Cybercriminal nei sistemi con forzatura delle protezioni.**
- **La deficienza in una procedura di controllo generata da un'alterazione casuale o dolosa.**
- **DoS:l'Impossibilità per l'Assicurato di utilizzare i sistemi di posta, in assenza di danni materiali,e l'utilizzo di sistemi alternativi in emergenza.**
- **Un errore umano dei tecnici addetti alle gestioni informatiche.**
- **la copia di dati sensibili ai fini di vendita a concorrenti con cancellazione dei files**
- **L'utilizzo indebito di beni di terzi ai fini di guadagno .**
- **La distruzione dolosa di dati per cancellare le tracce di un crimine.**

Le Garanzie base

Le conseguenze coperte si presentano come la messa a disposizione di un capitale finanziario per indennizzare i diversi tipi di pregiudizio sofferti :

- **Spese per Ricostituzione dei dati (di proprietà o di terzi)**
- **I costi di riacquisto a nuovo di macchinari ed impianti**
- **Spese extra,supplementari,straordinarie (e Disaster Recovery)**
- **Perdite patrimoniali da Frode informatica (€,merci,etc..)**
- **Spese di difesa del Brand(marchio)**
- **Mancato Profitto (spese fisse,stipendi dip.,utili,ammortamenti)**
- **Gli indennizzi a terzi per responsabilità professionali**

Le Esclusioni di base

=> terrorismo informatico (Alkaeda per es.).

=> errori di programmazione.

=> radiazione elettromagnetica/atomica.

=> perdite di profitto da errori umani.

=> costi di manutenzione hd/sw.

=> costi di miglioria dopo un sinistro.

=> Mancata fornitura di energia.

Le condizioni particolari
(estensioni principali)

=>Frode informatica (distrazione di fondi,merci,servizi).

=>Responsabilità Civile (professionale) Informatica.

=>Danni a beni immobili.

=>Guasti meccanici.

=>Terrorismo (solo per danni a hw).

=>Danni da violazione della riservatezza/segretezza dei dati.

Le condizioni particolari
(altre estensioni)

>Danni a dati di macchinari speciali (portatili, medicali,etc..).

>Danni avvenuti durante i trasporti di Hardware/software.

>La copertura di hd/sw portatili/mobili – truck attrezzati.

>Danni avvenuti durante l'operatività (in acqua/aria/strada).

>Il maggior costo dopo una interruzione delle trasmissioni di dati.

>Spese conseguenti all'interruzione della fornitura di energia.

>Il maggior costo delle relazioni pubbliche a seguito di sinistro.

>l'estensione della copertura all'estero.

>i maggiori costi per il trasferimento di pazienti tra strutture osp.

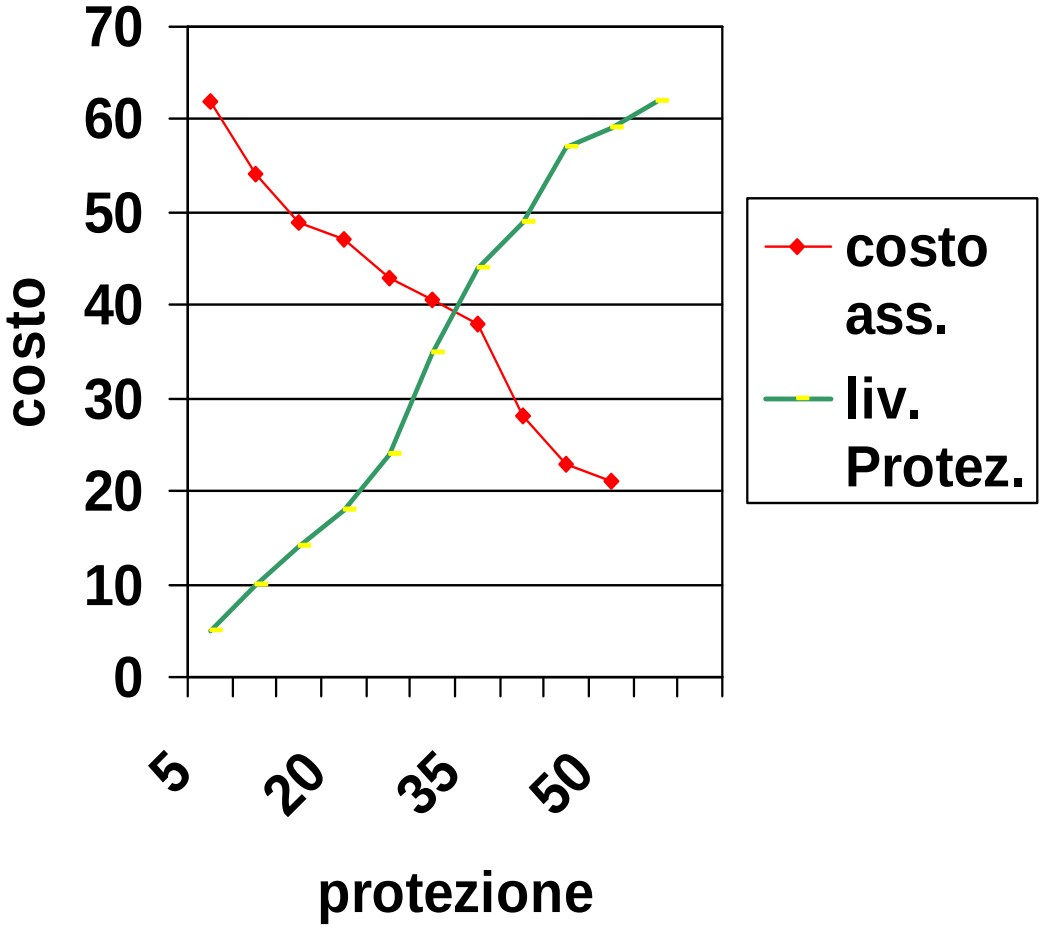
>riacquisto mezzi di estinzione a seguito di attivazione errata di scarica.

>eventi fieristici,dimostrazioni,convention.

>etc..etc…

La variazione del costo assicurativo è in funzione del livello di protezione in rapporto al rischio

- *valutazione gestione della sicurezza*
- *valutazione del rischio*
- *rischio operativo residuo*
- *costi assicurativi*



Grazie per la vostra attenzione

25 years of insuring progress

ANCORA ESEMPI DI SINISTRO

ADDENDUM SINISTRI => e per chi vuole ricevere il Bollettino di aggiornamento sui rischi informatici

Inviare la propria e.m. all'indirizzo :

carlo.delisio@acegroup.com

riccardo.scalici@acegroup.com

Riceverete asap gli aggiornamenti mensili o bimestrali via e.m.direttamente al vs indirizzo.

Segnalateci ogni sinistro o danno informatico avvenuto presso i vostri clienti anche se non risarcito da alcuna polizza. L'informazione sarà opportunatamente mascherata in modo da non poter risalire al danneggiato ed inserita nel nostro database di esempi di sinistro.

Visitate il sito www.clusit.it troverete la parte assicurativa ed informazioni su eventi inerenti la sicurezza informatica in Italia e all'estero , oltre che a corsi, seminari, conferenze e materiale aggiornato.

Esempi di eventi dannosi subiti dalle aziende esempio 4 (fonte : ACE) – **VIRUS** -

Tipo di azienda:	**servizi finanziari (Irlanda)**
Tipologia di danno:	**contaminazione da Virus**
Area colpita:	**il network pc principale**
Funzione:	**gestione posta, interfaccia mainframe**
Parte a rischio:	**28.000 pc del network**
Danno subito:	**fermo totale di 5 giorni + decontaminazione in laboratorio di 15.000pc altri 13.000pc**
Causa:	**software installation matrix contamination**
Danno complessivo:	**spese 2,3 mil. + 16 mil. perdite finanziarie per un totale di = 28,3 milioni (stima).**
Indennizzo:	**nessuno , nè la BBB, nè All Risks incendio coprivano la fattispecie di evento dannoso.**

25 years of insuring progress

Esempi di eventi dannosi subiti dalle aziende esempio 2 (fonte : ACE) – **ERRORE UMANO** -

Tipo di azienda:	**servizi informatici per conto terzi (catena franchising ITALIA)**
Tipologia di danno:	**errore umano (errata implementazione applicativo gestionale).**
Area colpita:	**controllo automatico impianto di condizionamento.**
Funzione:	**mantenimento parametri climatici sala centrale CED.**
Parte a rischio:	**elaborazione (da 4,5 a 25 milioni) di operazioni settimanali.**
Danno subito:	**fermo totale di 1,5 giorni + rallentamenti del sistema per 48 giorni.**
Sinistro:	**4.500 punti vendita al dettaglio con problemi di funzionamento.**
Perdite stimate:	**punti vendita c.ca 15 milioni € e soc.servizi informatici 2,5 milioni €**
Indennizzo:	**punti vendita : zero (non assicurati),soc.servizi informatici : 0,5 M€ (sottoassicurati su spese extra).**
Meccanismo:	**l'incapacità di elaborare giusto risettaggio del software di controllo di un impianto di climatizzazione del centro elaborazione dati principale ha provocato un funzionamento a singhiozzo per 45 giorni delle macchine principali ,con rallentamenti e fermi di attività di 4.500 punti vendita**
Brand defence:	**ai punti vendita che hanno promosso azione legale contro la società di servizi sono state proposte condizioni di servizio compensative del danno subito (spesa = 0,5 milioni €).**

Esempi di eventi dannosi subiti dalle aziende esempio 8 (fonte : ACE) – **CRACKER** -

Tipo di azienda:	**Operatore trasporti gas (est UE)**
Tipologia di danno:	**Craker instrusion in IT system – (1999)**
Area colpita:	**sistema di regolazione flussi di gas**
Effetti:	**8 e più ore di continui malfunzionamenti nelle regolazioni flussi gas**
Danno diretto?:	**sconosciuto**
Danno indiretto?:	**sconosciuto**
Brand protection:	**l'informazione è stata bloccata a più livelli, è trapelata durante un convegno di Haker in Germania. E' stata commentata durante il G8 durante il meeting sul Cybercrime nell'Ottobre del 2000**
Indennizzo:	**danno non assicurato**

25 years of insuring progress

Esempi di eventi dannosi subiti dalle aziende esempio 9 (fonte : ACE) – **ERRORE UMANO** -

Tipo di azienda:	**Mobil phone operator (USA)**
Tipologia di danno:	**Improper parameter setting**
Area colpita:	**HLR Automatic additional memory reallocation set up at a threshold exceeding the equipment capacity.**
Effetti:	**Users connection stopped during more than 24 hours.**
Danno diretto?:	**sconosciuto**
Danno indiretto?:	**Loss of revenue and associated cost estimated € 8,000,000**

25 years of insuring progress

Esempi di eventi dannosi subiti dalle aziende esempio 10 (fonte : ACE) – **ERRORE UMANO** -

Tipo di azienda:	**Bank group (markets study division) (UK).**
Tipologia di danno:	**Wrong indexation procedure.**
Area colpita:	**Client marketing main project.**
Effetti:	**error in plan marketing projects because loss discovered after 6 months**
Danno diretto?:	**pure restoration costs estimated in 820.000€**
Danno indiretto?:	**Loss of revenue associated to the marketing action plan delay (1 year delay): unknown (difficult estimation of market loss due delay), in any case over 3 million lst.**

25 years of insuring progress

Esempi di eventi dannosi subiti dalle aziende esempio 1 (fonte : ACE) – **BACK-UP**

Tipo di azienda:	**azienda a proprietà pubblica (Francia)**
Tipologia di danno:	**malfunzionamento back-up**
Area colpita:	**dati contabili e fatturazione a utenti del servizio pubblico**
Funzione:	**comunicazione rendiconti mensili**
File a rischio:	**45 milioni di utenti**
Danno subito:	**persi 2 giorni di dati - impossibilità di rispettare la scadenza mensile con il rendiconto del mese**
Sinistro:	**maggiori spese postali per 3.000.000 € + altre perdite.**
Indennizzo:	**complessivamente 5.700.000 € (90% ca del massimale assicurato allo scopo)**
Brand defence:	**ai cittadini è stato inviato un rendiconto per ciascuna voce di spesa giustificato da "ragioni tecniche", con lettera di scuse (maggiori spese per 1.000.000 € non rimborsate perchè non assicurate, ai giornalisti non è stata data alcuna nota informativa).**

Esempi di eventi dannosi subiti dalle aziende esempio 11 (fonte : ACE) – **CYBERCRIME** -

Tipo di azienda:	**80.000 aziende sul web con siti di e.commerce (danno WW)**
Tipologia di danno:	**pirataggio a sito protetto da tecnologia ScanAlert**
1°sito colpito:	**Geeks.com – è stata oggetto cybercrime.**
Effetti:	**furto di carte di crédito Visa dei clienti**
Danno diretto?:	**costi di di ricerca e indagine non stimati**
Danno indiretto?:	**perdita di fiducia di consumatori , riduzione delle vendite , perdite di profitto sconosciute.**
Causa?:	**incremento delle capacità della malavita che ora comincia ad agire anche sul Web direttamente.**
	Si sono attivati gli organi di polizia del paese, i servizi segreti USA,FBI,etc.

Esempi di eventi dannosi subiti dalle aziende esempio 13 (fonte : ACE) – **SITI WEB OSCURATI** -

Tipologia di azienda:	**distributori via WEB (piattaforme) (USA)**
Tipologia di danno:	**oscuramento di due maggiori siti Web**
Area colpita:	**vendita/distribuzione on-line(7,8 bilion$ Yr)**
Causa:	**attacco Cybercrime (con estorsione)**
Effetti:	**arresto totale attività di 15 giorni**
Danno diretto:	**costo di ricostruzione siti 500.000 € (stima)**
Danno indiretto:	**perdita vendite > di 6 milion $ (stima)**
Indennizzo:	**assenza di copertura assicurativa**
Recupero:	**nessuno – gli ordinativi persi sono stati acquisiti dalla concorrenza**
Brand Protection:	**spese di pubblicità dei nuovi siti stimate in 1,5 million $**

Esempi di eventi dannosi subiti dalle aziende esempio 15 (fonte : ACE) – **ERRORE** -

Tipologia di azienda: **fornitore globale di servizi IT (UE)**

Tipologia di danno: **problemi di DNS**

Area colpita: **150.000 siti Internet**

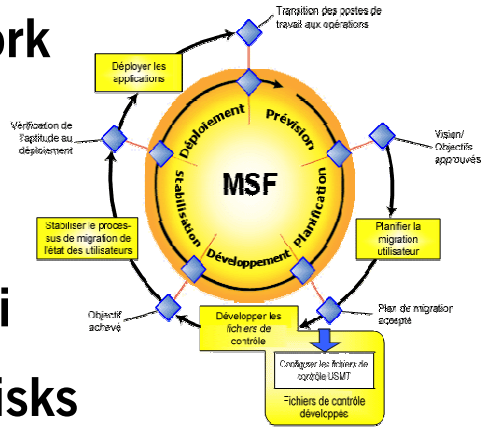
Causa: **migrazione di un centinaio di servers da sito A a sito B**

Effetti: **fuori servizio intero network**

Danno diretto: **350.000€**

Danno indiretto: **stimato 20 milioni**

Indennizzo : **nessuno : erano assicurati solo polizza incendio all risks**



25 years of insuring progress

Esempi di eventi dannosi subiti dalle aziende esempio 14 (fonte : ACE) – **ERRORE + VIRUS** -

Tipologia di azienda:	**compagnia di assicurazione (UK)**
Tipologia di danno:	**contaminazione virus.**
Area colpita:	**l'intero network (circa 1000 pc/server)**
Causa:	**chiave usb utilizzata da membro CED**
Effetti:	**infezione totale network.**
Danno diretto:	**costo decontaminazione 450.000€**
Danno indiretto:	**milioni di € rischio non assicurato**
Brand protection:	**maggiori costi telefonici (non stimato)**

25 years of insuring progress

Esempi di eventi dannosi subiti dalle aziende esempio 16 (fonte : ACE) – sparizione DATA -

Tipologia di azienda:	**Banche (gruppo) (USA).**
Tipologia di danno:	**parte del database totale copiato e reso inaffidabile.**
Area colpita:	**1,5 milioni di conti.**
Effetti:	**perdita riservatezza di milioni di informazioni,codici,password,etc**
Danno diretto/indiretto:	**(stima)>15 milioni $**
Brand Protection:	**i clienti non sono stati avvertiti.**
Indennizzo:	**nessuno non erano assicurati.**

25 years of insuring progress

Esempi di eventi dannosi subiti dalle aziende esempio 5 (fonte : ACE) – **DOLO DIPENDENTE** -

Tipo di azienda:	**finanziaria (NY - USA)**
Tipologia di danno:	**Dolo di dipendente (programmatore)**
Area colpita:	**sistema principale e banche dati**
Parte a rischio:	**l'intera attività**
Causa:	bomba logica nel sistema che ha cancellato tutti i files compresi quelli di back-up dell'ultimo anno.
Danno:	**2,5 m$ data restoration costs + 15 m$ loss of profit = 17,5 m$ total estimated**
Brand defence:	l'operazione di salvataggio e ripristino è stata condotta con la supervisione di società specializzata in servizi riservati per evitare fuga di notizie e il panico in borsa (sovracosto c.ca 1 milione $)

25 years of insuring progress