

Seminario di studio tenutosi a Roma il 13 novembre 2007.

Sintesi degli interventi.

Sommario

Seminario di studio tenutosi a Roma il 13 novembre 2007.....	1
Sintesi degli interventi.....	1
Introduzione.....	1
1.Relazione CIPA.....	1
2.Relazione di Wright.....	4
3.Relazione Escape.....	5
4.Relazione IBM.....	7
5.Conclusione.....	9

Introduzione

L'Ing. Anthony Cecil Wright, Presidente ANSSAIF apre il Seminario con un breve saluto e ringraziamento ai partecipanti e, in particolare, alla ICCREA Banca ospitante. Ricorda quindi, brevemente, gli scopi dell'associazione ANSSAIF e gli aspetti organizzativi dei Seminari, facendo cenno all'obiettivo posto di coinvolgere il mondo studentesco alle non semplici problematiche relative alla Sicurezza. In questa ottica si inquadrano i recenti contatti con alcune Università, ed il progetto con la Università Cattolica del Sacro Cuore di Milano.

Cede quindi la parola al Sig. Salvatore Fratejacci della Banca d'Italia, che presenta un'anticipazione del rapporto CIPA sulla Sicurezza in banca, rapporto che verrà pubblicato a dicembre.

1.Relazione CIPA

L'intervento del sig. Salvatore Fratejacci (Segreteria CIPA) si apre con una breve storia e finalità relative alla Convenzione Interbancaria per i Problemi dell'Automazione.

Passa, quindi a descrivere il documento "Rilevazione sullo stato di automazione del Sistema Creditizio" pubblicata dalla CIPA, con specifico riferimento alla sicurezza informatica.

Tale rilevazione è molto apprezzata non solo dalle Banche ma anche da consulenti e dalle stesse Università per l'attendibilità dei dati che fornisce ed inoltre non esiste eguale in nessun altro paese europeo.

Il documento è l'elaborazione di un questionario fornito ad un campione di Banche (circa l'80% dell'intero Sistema Bancario in termini di fondi intermediati) commentato con indici ed informazioni atte ad analizzare

la situazione di ciascuna Banca in termini di spesa/produttività dell'ICT in rapporto all'intero Sistema Creditizio.

Nell'ambito dell'indagine si pone l'attenzione sulla Sicurezza Informatica e in particolare sugli aspetti relativi a:

- Costi
- Continuità di servizio
- Prevenzioni delle frodi informatiche

Per il 2007 si prevede di allargare l'indagine sul contenuto delle policy di sicurezza.

Per quanto riguarda i Costi della Sicurezza Informatica : essi variano dal 2,70% del 2004, al 3,12% del 2006 con una previsione per il 2007 del 3,44% sul totale della spesa per l'ICT.

Fratejacci osserva che la spesa per la sicurezza si mantiene entro un certo livello anche quando la spesa complessiva per ICT è bassa.

Passando alla tematica relativa alla Continuità di Servizio, dall'indagine risulta che l'89,2% delle Banche hanno un piano formalizzato e che per il 2007 si prevede che diventino il 99,3% sul totale del campione. L'aspetto tecnologico (piano di D.R.) è presente sull'intero campione.

Il passo successivo del documento descritto dal sig. Fratejacci riguarda la frequenza e la tipologia delle prove e la qualità dei risultati. Le risposte ai quesiti indicano che una volta l'anno è la frequenza maggiormente dichiarata, mentre per quanto riguarda la tipologia delle prove risulta dalle risposte dei questionari che le prove con l'utilizzo di dati a perdere sono quelle maggiormente dichiarate (62% del campione) e quelle con dati veri sono il 26% (attivazione del D.R. e ripristino sull'ordinario ossia doppio test). La qualità dei risultati appare dalle risposte per il 50% eccellente.

Infine il relatore affronta il problema relativo alla Prevenzione delle frodi informatiche e del furto d'identità. I dati statistici presentati fanno riferimento alle iniziative intraprese dagli Istituti Bancari: risulta che le maggiori Banche sono più sensibili rispetto a quelle meno importanti in relazione alle informazioni alla clientela, agli strumenti tecnologici utilizzati, alle misure organizzative ed alle attività di analisi e monitoraggio statiche per individuare siti clone, mentre le attività di collaborazione sistematiche a fini preventivi risultano maggiormente intraprese dalle Banche minori.

Interviene il Presidente ANSSAIF, Ing. Wright, facendo alcune riflessioni sui costi relativi alla continuità del business: si può fare Business Continuity anche spendendo poco, utilizzando quello che già esiste. Lo dimostra anche un dato relativo all'incidenza della spesa per DR e BCP, ove quest'ultima ha rappresentato per molte banche circa il 2% del totale.

Ha poi accennato alla legge sulla privacy, che ci fa riflettere sulla ridondanza dei dati e sull'esistenza di una normativa per sollecitare le banche ad attuare anche politiche di ottimizzazione degli stessi.

Si apre successivamente la discussione su alcuni quesiti proposti dai partecipanti al Seminario :

I) Domanda (Dott.P.Serafini): La percentuale di spesa per la Sicurezza sull'ammontare totale dell'ICT è andata aumentando, tenendo in considerazione anche i risparmi indotti dalla multicanalità?

Risposta: La spesa in termini assoluti per l'IT negli ultimi anni dopo una leggera flessione nel 2006 è tornata a crescere lentamente, mentre la spesa per la Sicurezza cresce gradatamente; la fusione di Banche alla lunga portano risparmi ma non immediatamente; la multicanalità all'inizio è stato un importante investimento; le ricadute in termini di costo per la sua sicurezza forse inizialmente non sono state valutate appieno.

II) D. (dr.M.Recchia): Vi sono dati informazione dalla relazione CIPA sui dettagli e sulla qualità delle informazioni sulla Sicurezza inviate dalle Banche alla clientela, come per esempio comunicare al cliente : "attenzione tu sei in pericolo?"

R.: Nel questionario vi sono solo domande/risposte generiche; ABI LAB ha, tuttavia, sia stampato un volantino, sia fornito sul portale un corso interattivo per istruire la clientela sulla propria Sicurezza; anche la pubblicazione del 2005 di CIPA/CNIPA/ABI LAB ha dato alcuni suggerimenti per sottrarsi al furto d'identità (rischi e comportamenti).

III) D. (ing.F.Gargano): Da un dato fornito da analisti di mercato, il trend sulla crescita della spesa per la Sicurezza (in generale nei settori industria, banche, ecc.) è un valore a 2 cifre rispetto alla spesa complessiva ICT e quindi si discosta dal valore fornito da CIPA (circa 3% in media), ed ancora: le Banche Europee cosa stanno facendo?

R.: Per la valutazione della spesa per la Sicurezza occorre verificare diversi aspetti:

- 1) l'omogeneità del campione; in questo caso trattandosi di una indagine allargata, è abbastanza difficile che le industrie spendano più delle banche per la sicurezza;
- 2) la fonte delle informazioni; nel caso delle banche quasi sempre le informazioni vengono dalla funzione di controllo gestionale;
- 3) la metodologia utilizzata per definire le voci di spesa attribuibili alla "sicurezza"; per esempio, il D.R. non può considerarsi una spesa per la Sicurezza.

La differenza rilevata dall'interlocutore può essere, quindi, dovuta soprattutto alla metodologia di rilevazione.

In ogni caso il questionario e le istruzioni per la compilazione sono pubblicati sul sito della CIPA e quindi possono essere confrontate.

A livello europeo, come già detto non esiste un organismo analogo. Tuttavia c'è molto interesse per ciò che succede al di là delle Alpi. Quest'anno, all'interno della "Rilevazione"; è stato messo a punto un

approfondimento tematico sulla internazionalizzazione dei grandi gruppi bancari; sono stati formulati quesiti sul modello organizzativo e sulla governance dell' ICT, sul numeri degli addetti ICT, sulla disposizioni geografiche delle software factory e sulla spesa ICT.

Analoghi quesiti sono stati formulati da ABI Lab ad alcuni grandi gruppi bancari europei.

Le risposte hanno fornito dati comparabili tra loro soltanto per alcuni aspetti. Il rapporto finale conterrà gli esiti dell'approfondimento.

IV) D. (Dott.P.Bucci): La spesa per la Sicurezza Informatica è comprensiva di voci tipo personale, consulenza, ecc.?

R.: Il questionario prevede voci di spesa per il personale, per la componente di consulenza, per outsourcing, per il software, per l'hardware, per la manutenzione; la quota parte di ciascuna voce utilizzata per la sicurezza concorre a formare la spesa "sicurezza". I dati delle Banche sono, prevalentemente, forniti dalla funzione di controllo di gestione, quindi attendibili.

V) D. (Sig. Vallesi): Le fusioni di Banche richiedono un lavoro sulla Sicurezza molto impegnativo, occorre uniformare i prodotti, i processi, le analisi sui backup, sensibilizzare il personale addetto alla Sicurezza, e quant'altro e, quindi, forse è prevedibile estrapolare un andamento in aumento dei costi per il 2008.

R.: L'accorpamento senz'altro, all'inizio, genera maggiori costi, che poi nel tempo si riducono. I principali gruppi bancari presi in esame per il 2006 sono stati 20; a seguito degli accorpamenti, nel 2007 saranno di meno e, presumibilmente, ancora meno nel 2008.

2.Relazione di Wright

Il moderatore del Seminario Ing. Wright prende, quindi, la parola per sottolineare gli aspetti, che considera da sempre molto importanti, legati ad un evento imprevisto e destabilizzante: la crisi (gestione, stress, panico).

La crisi è caratterizzata da una minaccia all'organizzazione, da un fattore sorpresa e dalla necessità di rapidità nella risposta.

La gestione della crisi richiede cioè capacità tecniche atte a valutare, capire e risolvere, mentre il processo decisionale per superarla si avvale dell'articolazione degli obiettivi, della generazione di ipotesi alternative, di analisi di fattibilità, della valutazione delle diverse alternative e delle scelte più aderenti agli obiettivi dell'Organizzazione, il tutto da completare nel più breve tempo possibile.

L'Ing. Wright ha sostenuto che occorre affrontare il problema non incorrendo in quelli che sono gli errori più comuni, come: stime errate, insufficienti alternative, ritardo nelle decisioni, errata messa in opera, esame incompleto dello scenario, ed altri ancora.

Inoltre le cause che generano questi errori possono essere attribuite ad un errato filtraggio delle informazioni, ad un eccesso di persone coinvolte, ad una scarsa capacità di adattamento, all'ansia che

assale od anche ad una eccessiva distanza da chi prende le decisioni (gap, non solo fisico ma anche intellettuale fra chi fa e chi decide).

La rigidità delle procedure standard, la sensazione di invulnerabilità, l'ottimismo, la tendenza di centralizzare o la paura di prendere le decisioni possono concorrere a non affrontare correttamente l'evento.

Per evitare di commettere tali errori vengono proposti una serie di suggerimenti:

- pianificare ed effettuare simulazioni e test,
- schedulare procedure flessibili per gli incidenti e diversificate per la crisi,
- disegnare scenari differenti,
- utilizzare tecniche di *problem solving*,
- creare una unità di crisi apposita.

Inoltre occorre puntare su persone con leadership e capacità di controllo sullo stress.

Un ultima osservazione proposta, consiste nel porre molta attenzione alle comunicazioni creando canali specifici per il contatto con i *media* (attenzione alle informazioni in ambito concorrenza molto aperta; possono essere sfruttate dai concorrenti).

Infine il relatore conclude affermando che il tutto va accompagnato da un continuo aggiornamento e miglioramento.

3.Relazione Escape

Si passa, quindi, su invito del moderatore Ing.Wright, ad un'altra presentazione : Massimiliano Girolami di ESCAPE del gruppo BRAVE illustra la sua proposta di Governance dell'IT.

Escape nell'ambito del gruppo Brave raccoglie le competenze sulle problematiche relative alla Sicurezza a 360 gradi.

L'intervento si apre fornendo la definizione di Governance, ossia l'insieme di regole, relazioni, processi, strutture organizzative e sistemi aziendali che presiedono ad un corretto ed efficiente governo dell'impresa.

L'IT Governance è un sistema iterativo, un percorso, non una meta. Le tecniche di misurazione delle performance quantitative e/o qualitative sono comprese nell'architettura per fornire monitoraggio e gestione della qualità e possibilità di continuo miglioramento.

Il primo, fondamentale principio è che la Direzione ed il Management sviluppino un modello di Governance che omogenei e condivide obiettivi e metodiche operative e controlli periodicamente l'efficienza del modello.

Può essere descritta come un insieme di arte e scienza del comportamento.

Il relatore ha quindi enunciato quelli che vengono definiti problemi sistemici, tipo :

- la fornitura di informazioni contabili,
- la richiesta di informazioni,
- i costi di monitoraggio(audit),
- l'IT Governance.

Gli obiettivi principali dell'IT Governance sono assicurare che gli investimenti per l'IT generino valore per l'azienda e che i rischi associati con l'IT vengano gestiti e mitigati.

Ciò si realizza creando strutture organizzative adeguate con ruoli e responsabilità ben definite (sicurezza, applicazioni, processi aziendali, infrastruttura, analisi dei rischi).

In ogni caso l'implementazione dell'IT Governance necessita di un approccio strutturato (plan/do/check/act); il cui primo imperativo è il business e successivamente viene presa in considerazione la parte relativa alla comprensione dell'evento e alla situazione che causa la necessità dell'investimento nel campo dell'IT (operational excellence, risk management, regulatory compliance).

Sono state, quindi, approfondite, dal relatore, le varie componenti sulla comprensione dell'evento e sulla causa della necessità dell'investimento. Deve essere inserita in azienda una *road map* sulle modalità di implementazione dell'IT Governance e ci dobbiamo domandare se l'azienda opera in direzione innovativa o no, se l'IT è percepito come un creatore di valore business o solo fornitore di servizi. La Soc. Brave, specializzata in consulenza organizzativa, con una soluzione integrata si propone di collaborare alle risposte ai vari quesiti.

Viene descritta la proposta BRAVE articolando lo scenario in varie componenti : la Governance cioè

- Organizzazione,
- Operatività,
- Valori,
- Metodi,
- Performance,
- Information Security,
- Business Continuity,
- IT Service Support,
- IT Service Delivery,
- IT Service Continuity,
- IT Security Management,
- ICT Infrastructure Management).

Il relatore passa, quindi, a definire il risk management, ossia conoscere a cosa andiamo incontro e costruire sistemi di valutazione senza escludere i rischi assunti, utilizzando adeguati indicatori di allarme.

Il relatore prosegue osservando che al rischio va associata l'opportunità di organizzare processi efficienti, trattenere le migliori risorse, guadagnare quote di mercato, conquistare la fiducia dei clienti, fare meglio dei concorrenti ed anche che una buona gestione del rischio debba essere costruita attorno a tre principi fondamentali : nessuna scusa, nessuna lamentela, nessuna copertura.

Si passa ad osservare come la strategia dell'IT deve essere orientata ad una coerente gestione dei costi, al supporto ai processi di gestione, alla standardizzazione dei processi, alle best practices, al cambiamento ed all'innovazione garantendo sempre flessibilità ed agilità alle modifiche.

Vengono elencati i servizi che compongono l'IT Service e precisamente : gestione del network, delle postazioni di lavoro, delle applicazioni e l'help desk che concorrono alla definizione delle attività di infrastructure change management, operation management, asset management, customer service, training, ecc.

Le osservazioni che il relatore propone indicano quali possono considerarsi scelte giuste e quali sono da evitare e cioè: si alla responsabilità dei risultati, si all'integrazione organizzativa, si a standard, si ad analisi dei costi, si a leadership, no a culture non convergenti, no a processi e decisioni lente. In questa analisi ricopre una notevole importanza l'aspetto decisionale da parte dei leader indirizzato soprattutto al bene dell'azienda.

Vengono anche trattati alcuni indicatori di performance(debbono essere interpretati come indicatori di business non tecnologici) e vengono utilizzati per documentare l'attività di analisi e valutazione di un sistema informativo ed evidenziare con l'attività di reporting gli aspetti relativi al contesto aziendale, alla strategia e al supporto IT, alla qualità del servizio e alla roadmap da percorrere.

Come conclusione Massimiliano Girolami afferma che l'IT Governance dovrebbe consentire di aumentare l'efficacia e l'efficienza dell'infrastrutture IT nel medio e lungo periodo, abbattere i costi dovuti ai disservizi ed allineare i sistemi IT alle finalità di business.

4.Relazione IBM

Il moderatore passa, quindi, la parola a Fausto Nigioni di IBM che interviene su un "Nuovo approccio alla Sicurezza Fisica".

La soluzione che IBM propone da 5/6 mesi sul mercato, nasce da circa da circa 4/5 anni di test e sperimentazioni in vari Paesi.

L'approccio proposto è : cosa proteggere in ambiente bancario e come trasformare la spesa di sicurezza da costo in vantaggio competitivo.

In Italia dal 1995 al 2004 vi sono state 275 fusioni/acquisizioni in ambito bancario, 170 in Germania, 95 in Spagna e 23 in Olanda.

Si è creata, quindi, la necessità di rivedere processi, procedere e creare nuove offerte per ridurre i costi.

Dal punto di vista della Sicurezza ci si domanda come deve evolvere l'Organizzazione, con quali processi, se esiste un modello, quali sono le minacce, come controllare le filiali, quali sono le tendenze tecnologiche.

La Sicurezza è sempre stata vista come un costo, mentre può in effetti contribuire al business dell'azienda, essere un vantaggio competitivo.

Non esiste una soluzione sicura al 100%, ma l'integrazione di soluzioni tecnologiche diverse per aumentare il livello di sicurezza.

Oggi le banche sono organizzate come una tipica compagnia multinazionale con differenti linee di business e offerte di prodotti e con, quindi, diversi tipi di minacce e rischi.

Vengono elencati dal relatore i vari tipi di rischi e minacce da combattere :

- attentato,
- furto,
- frode,
- danneggiamento,

contro dipendenti, clienti, beni, immagine o reputazione.

Le soluzioni per contrastare ciò debbono tener conto dei Trend Tecnologici (convergenza del protocollo di comunicazione, contenuti digitali, videoanalisi, biometria, RFID, integrazione sicurezza fisica e logica).

Fausto Nigioni introduce, quindi, la soluzione di sicurezza fisica integrata (IBM Information Security Framework) in cui vengono affrontate congiuntamente sia la tematica della Sicurezza ICT sia quella relativa alla protezione delle infrastrutture critiche con soluzioni di videosorveglianza digitale avanzata, controllo degli accessi, multimedia communications, anti-intrusione, anti-incendio, ecc.

Attualmente le soluzioni sul mercato sono sostanzialmente allarmi realtime con rilevazioni di movimento, di direzione del moto, di oggetti abbandonati o rimossi, offuscamento o spostamento di telecamera, rilevazione di targa che possono definirsi di tipo classico.

Le peculiarità della soluzione IBM consentono anche :

- la rilevazione automatica dei volti,
- gli allarmi di tipo statistico,
- la ricerca di eventi su base temporale con interfaccia web per durata, tipo, dimensione, colore, posizionamento,
- le statistiche degli eventi,
- la rilevazione di comportamenti anomali,
- la correlazione di eventi provenienti da sensori differenti,
- l'integrazione con infrastrutture già esistenti,

il tutto viene registrato su di un DataBase in vari formati.

Esempio si può agganciare la video sorveglianza per il controllo degli accessi (mettere in sicurezza il sito) e per il monitoraggio del controllo delle code.

Vengono proposte alcune domande :

I) D. : Nella soluzione IBM come viene affrontata la problematica relativa alla visualizzazione dei dati, dati senz'altro da definire sensibili?

R. : Ciò è regolamentato consentendo agli operatori di fare query, estrarre informazioni, come per esempio traiettorie di transito dei clienti, ecc., secondo profili definiti : operatore, autorità giudiziaria, utente, ecc. Viene anche regolamentato con quali criteri mantenere questi dati nel database e viene definito chi ha e chi non ha accesso a tali informazioni.

II) D. : Nella realtà lavorativa italiana esistono problemi sindacali sull'utilizzo di video riprese che coinvolgono i lavoratori; come vengono affrontati dalla soluzione.

R. : Il problema attualmente è in analisi con le autorità coinvolte : si sta contattando il Garante della Privacy per regolarizzare la questione, individuare le linee guida e condividere gli aspetti sindacali; inoltre la soluzione italiana è stata implementata per poter schermare il volto delle persone.

L'ing. Nigioni torna, quindi, alla presentazione descrivendo alcuni esempi sull'utilizzo dei dati registrati: indagare sulle frodi in ambiente ATM utilizzando la video-sorveglianza sul terminale associata a sensori ed allarmi, verificare l'efficacia dei dispositivi interattivi, tracciare il percorso dei clienti in filiali/agenzie bancarie per valutare l'efficacia di aree di interesse (pubblicità) in tali ambienti, piuttosto che i picchi di accesso (code) per innalzare la qualità del servizio.

La gestione degli allarmi utilizza un interfaccia classica web rappresentando la distribuzione degli allarmi, con la possibilità di effettuare query sulle immagini per tipo di oggetto, colore, permanenza, dimensione, durata nel tempo, ecc.

In una Organizzazione complessa la soluzione di Sicurezza si deve appoggiare ad una Control Room in cui viene centralizzata la gestione degli allarmi e degli eventi ed in cui agli operatori è demandato secondo priorità la reazione a tali eventi.

Infine il relatore conclude descrivendo come l'IBM si appoggi a partner di hardware (telecamere, controllo accessi) per proporre soluzioni integrate, mettendo a frutto tutta l'esperienza dei propri laboratori (centro di Watson) o laboratori e centri di ricerca sia a livello nazionale che internazionale, per capitalizzare al massimo le attività svolte di progettazione, implementazione, centralizzazione, integrazione, analisi compartimentali, correlazione, ottimizzazione, supporto e manutenzione rivolta ai clienti.

Il Presidente, ringrazia il relatore IBM ed aggiunge, a favore della soluzione proposta da IBM, dei commenti derivanti dalla sua precedente esperienza di responsabile dell'ICT auditing in BNL e, in particolare, a quando progettò e realizzò dei sistemi di monitoraggio per la prevenzione di rischi da "insiders".

5.Conclusione

L'ing.Wright ringrazia i partecipanti al Seminario e ricorda che il giorno 20 si terrà un'analogia edizione a Milano, ove però si aggiungerà una interessante relazione di Cap Gemini sulla Gestione della Crisi in caso di mancanza di liquidità.