BASEL COMMITTEE ON BANKING SUPERVISION

BANK FOR INTERNATIONAL SETTLEMENTS

Rischi nei sistemi informatici e di telecomunicazione

(Luglio 1989)

La rapidità dell'innovazione tecnologica nei sistemi informatici e di telecomunicazione nel corso degli ultimi anni e l'integrazione delle operazioni automatizzate hanno reso le banche sempre più dipendenti dall'affidabilità e dalla costante disponibilità dei loro sistemi EAD.

Le banche sono sempre state esposte a rischi, quali l'errore o la frode, ma le dimensioni assunte da tali rischi e la velocità con cui possono insorgere sono cambiate in maniera sensazionale. Inoltre, con i sistemi di regolamento elettronico le relazioni creditizie interbancarie coprono ormai l'intero globo attraverso le reti interconnesse. Quando una banca non è più in grado di onorare le proprie obbligazioni di pagamento a causa di problemi nel sistema, di insolvenza o di altri fattori, anche le istituzioni esposte nei confronti della banca in questione presentano crediti in sofferenza, e l'inadempienza si propaga attraverso una reazione a catena che minaccia di investire e paralizzare l'intero sistema di regolamento.

I tipi di rischi che caratterizzano un ambiente informatico e le procedure di sicurezza e di controllo necessarie richiedono tutta l'attenzione delle autorità di vigilanza. In questo documento vengono esaminati i seguenti tipi di rischio: diffusione impropria di informazioni, errori, frode, interruzione dell'attività dovuta a disfunzione nei sistemi e nei programmi informatici, pianificazione inadeguata e rischi connessi con le operazioni elettroniche di utenti finali.

Il rapporto è stato predisposto come base di riferimento per le autorità di vigilanza che operano in una vasta gamma di giurisdizioni. Esso non è concepito come strumento tecnico a uso di esperti della materia, ma cerca piuttosto di porre in evidenza le principali aree problematiche, di cui devono essere a conoscenza gli organi di controllo.

Diffusione impropria di informazioni

La maggior parte delle informazioni bancarie viene creata con un procedimento informatico o è direttamente collegata ad esso. Dati e documenti vengono normalmente trasmessi all'interno di una banca o tra questa e i suoi corrispondenti e clienti attraverso le reti pubbliche di telecomunicazione, come le linee telefoniche e i satelliti. Molti utenti, tra cui gli impiegati e i clienti della banca, possono accedere direttamente a questi dati attraverso terminali o telefoni. Tutto ciò, pur migliorando i servizi per la clientela e le operazioni interne, accresce il rischio di errore o abuso delle informazioni della banca.

Molte di queste informazioni sono confidenziali e potrebbero danneggiare i rapporti con i clienti e la reputazione della banca, dando origine a richieste di risarcimento per danni qualora venissero manomesse. I saldi dei conti privati, i limiti di scoperto e gli estremi delle transazioni sono alcuni esempi di queste informazioni. Anche la corrispondenza e le strategie della banca sono create e memorizzate attraverso il trattamento testi. Il rischio particolare che comporta la diffusione non autorizzata di informazioni confidenziali nei sistemi EAD, rispetto ai sistemi manuali, deriva dal fatto che una quantità molto maggiore di informazioni può essere ottenuta in una forma più agevole e trattabile con elaboratore (ad esempio, copie su nastri o dischetti) senza che resti traccia dell'accesso non autorizzato.

Per proteggere la banca sono pertanto necessarie adeguate procedure di sicurezza e controllo. Il livello dei controlli necessari deve essere valutato in rapporto al grado di rischio e all'incidenza delle perdite (o della diffusione non autorizzata di informazioni) per la banca.

I controlli tecnici per la sicurezza dell'informazione possono comprendere: la cifratura, procedimento attraverso il quale un testo in chiaro è convertito in una serie di simboli privi di significato; l'utilizzo di codici di autenticazione dei messaggi che proteggono le transazioni elettroniche di dati contro

alterazioni non autorizzate nel corso della trasmissione o della memorizzazione; l'uso di applicazioni di sicurezza destinate a limitare l'accesso a dati, archivi, programmi, funzioni ausiliarie e comandi di sistema elettronici. Tali sistemi permettono di controllare l'accesso per utente, transazione e terminale e di segnalare la violazione o il tentativo di violazione della sicurezza.

Errori

Gli errori avvengono di norma e con frequenza durante l'immissione dei dati oppure in connessione con l'elaborazione e la modifica di programmi. Errori significativi possono anche prodursi nel corso della progettazione di un sistema, durante le procedure di ordinaria manutenzione interna dei sistemi o nell'impiego di programmi speciali per correggere altri errori. La causa è in genere dovuta all'errore umano e relativamente di rado al malfunzionamento di componenti elettroniche o meccaniche interne. È possibile introdurre errori anche nei programmi di software personalizzati e adattati alle esigenze di un particolare utente. Nell'acquistare programmi informatici standardizzati si dovrebbe cercare di ridurre al minimo le modifiche.

Frode

I flussi di dati bancari rappresentano attività o istruzioni che comportano in definitiva un movimento di attività. La rapidità con cui avviene il trasferimento di attività per mezzo di sistemi elettronici di pagamento e di commutazione dei messaggi rende più difficile il controllo interno. Le frodi non si traducono soltanto in una perdita finanziaria diretta per l'istituzione, ma possono anche comportare, se portate a conoscenza dell'opinione pubblica, una perdita di fiducia nell'istituzione e nel sistema bancario in generale. La vasta gamma di modalità di accesso ai documenti informatici crea molte possibilità di frode, come ad esempio:

- l'immissione di transazioni non autorizzate nel sistema informatico;
- il cambiamento non autorizzato di programmi durante le operazioni ordinarie di sviluppo o di manutenzione, per cui il programma può generare automaticamente transazioni fraudolente, ignorare i test di controllo su taluni conti o eliminare la registrazione di determinate transazioni;
- l'utilizzo di programmi speciali per modificare senza autorizzazione documenti informatici in modo da eludere i controlli normali e le procedure di verifica integrate nei sistemi informatici;
- rimozione fisica dall'installazione informatica delle schede elettroniche, che vengono modificate altrove mediante l'immissione fraudolenta di transazioni o saldi e quindi reimmesse per il trattamento;
- introduzione o intercettazione e successiva modifica fraudolenta di transazioni durante la loro trasmissione attraverso la rete di telecomunicazione.

Attualmente sono in fase di sviluppo nuove forme di pagamento che consentono a terzi di iniziare la transazione mediante l'uso di attrezzature elettroniche. È pertanto destinata ad aumentare la probabilità che si verifichino frodi di questo tipo attraverso l'accesso non autorizzato alle reti di telecomunicazione.

La maggior parte dei sistemi bancari contiene dispositivi di controllo e produce informazioni miranti a facilitare la prevenzione o la rilevazione di frodi. Anche queste informazioni possono essere tuttavia soggette a manipolazione da parte di persone che hanno accesso ai terminali o agli archivi elettronici.

Nel progettare efficienti sistemi di controllo interno è essenziale individuare i punti vulnerabili di ciascun sistema. Le registrazioni e i programmi d'importanza nevralgica devono essere particolarmente protetti contro modifiche non autorizzate. Si dovrà inoltre aver cura che nelle aree critiche il personale riceva una formazione adeguata e che sia assicurata un'appropriata separazione delle funzioni.

Interruzione dell’attività dovuta a disfunzione nei sistemi o nei programmi informatici

I sistemi informatici consistono di numerose installazioni e componenti singole, e il mancato funzionamento di una sola di esse può provocare il blocco del sistema. Spesso queste componenti sono concentrate in poche localizzazioni, aumentandone la vulnerabilità.

Il rimedio classico in caso di disfunzione consisteva nel ripristinare il procedimento manuale che il sistema informatico ha sostituito. Nella maggior parte dei casi tale procedimento è ormai irrealistico, e ben poche banche potrebbero funzionare senza sistemi informatici. Il trattamento e la trasmissione di informazioni per mezzo di tecniche sempre più sofisticate hanno accresciuto la dipendenza del management delle banche dalla disponibilità di sistemi elettronici affidabili. La costante accessibilità a tali sistemi è una componente essenziale di un efficace processo decisionale.

Quando i sistemi informatici sono fuori uso, gli effetti pregiudizievoli sui servizi bancari in tempo reale forniti ai clienti sono immediati e aumentano rapidamente. Il ritardo nel trattamento delle istruzioni può accumularsi rapidamente e, dopo un blocco di diverse ore, il suo recupero può richiedere diversi giorni. Particolarmente devastanti sono gli effetti nel caso dei sistemi EFT e dei sistemi di pagamento, specie per quelli che garantiscono il regolamento con valuta stesso giorno, in cui i beneficiari dipendono dalla ricezione dei fondi per rispettare i loro impegni. I costi generati da una grave disfunzione dei sistemi possono superare di gran lunga i costi di sostituzione del materiale, dei dati o del software danneggiati.

Un’efficace pianificazione di emergenza costituisce uno dei modi in cui la direzione della banca può ridurre le conseguenze di simili problemi operativi. I piani di emergenza dovrebbero rappresentare un’estensione del sistema di controlli interni e di sicurezza fisica di una banca. Essi dovrebbero contemplare dispositivi per il proseguimento dell’attività e procedure di recupero in caso di disfunzione dei sistemi della banca, ossia una duplicazione di schede, software e hardware, nonché procedure alternative per il trattamento delle informazioni in un luogo diverso da quello di installazione. I piani di emergenza di una banca dovrebbero essere controllati periodicamente per verificarne l’efficienza. Una banca che ricorra a servizi EAD esterni per il trattamento di dati dovrebbe accertarsi che i piani di emergenza del fornitore di servizi integrino i propri.

Pianificazione inadeguata

Una corretta pianificazione è d’importanza fondamentale. L’efficienza di una banca e la qualità dei suoi servizi dipendono ormai a tal punto dai sistemi informatici che qualsiasi deficienza nella pianificazione o nello sviluppo di nuovi sistemi può avere conseguenze commerciali rilevanti. Se una banca non riesce a introdurre con sufficiente rapidità nuovi sistemi e nuovi servizi, essa può trovarsi in una posizione di grave svantaggio rispetto ai suoi concorrenti. D’altra parte, l’informatizzazione a tutti i costi, specie allorché i benefici sono marginali, si è dimostrata spesso un errore costoso.

Alcune istituzioni finanziarie hanno incontrato notevoli problemi nel cercare di introdurre sistemi finanziari altamente integrati. Un software integrato rappresenta una struttura in cui i programmi per le diverse applicazioni – crediti, depositi, operazioni al dettaglio e all’ingrosso – che di norma sono concepiti e gestiti come programmi autonomi, vengono predisposti fin dall’inizio come parti di un unico insieme. Questo approccio mira ad aumentare la tempestività delle informazioni, a migliorare l’efficienza operativa e ad agevolare l’introduzione di nuovi prodotti. In alcuni casi i costi, i tempi e le risorse umane richiesti per assicurare l’installazione di sistemi integrati sono stati sottovalutati. Progetti elaborati nel corso di molti anni sono stati abbandonati con costi enormi.

La complessità dei sistemi EAD e la loro incidenza sull’intera organizzazione bancaria richiedono un impegno dell’alta direzione per assicurare il buon esito dei singoli progetti. Il management dovrebbe seguire attentamente la pianificazione (strategica) a lungo termine riguardante sistemi, attrezzature, applicazioni, studi di fattibilità, specifica dei sistemi, scelta dei fornitori e controllo del progetto.

Rischi connessi con le operazioni elettroniche di utenti finali

Fino a epoca recente, i personal computer (PC), i microelaboratori e le attrezzature informatiche messe a disposizione di utenti finali hanno svolto un ruolo relativamente modesto nel sistema di trattamento informatico dei dati. Attualmente i vantaggi tecnici, la rapidità e la convenienza economica dell'informatica d'utente hanno contribuito a incrementare notevolmente l'utilizzo di queste attrezzature, sottraendo parte del trattamento dati al controllo centralizzato. I rischi connessi con l'informatica d'utente investono ora nuovi settori bancari, e in molti casi non sono stati adottati meccanismi basilari di controllo e supervisione di tali attività. L'aspetto più preoccupante a riguardo dell'informatica d'utente è che lo sviluppo di queste nuove reti di trattamento e di distribuzione delle informazioni ha preceduto l'introduzione dei controlli.

Sebbene i rischi siano generalmente uguali a quelli connessi con gli elaboratori centrali, va prestata particolare attenzione alla possibilità di alterazione e perdita di dati o software che potrebbe impedire l'efficiente funzionamento dell'intera rete operativa dell'istituzione. I microelaboratori vengono ormai impiegati non solo per il trattamento di testi, ma anche come terminali di comunicazione con altri elaboratori e processori autonomi. Poiché questi sistemi tendono a essere fortemente personalizzati e indipendenti – spesso vi è un responsabile unico per lo sviluppo, la sperimentazione, l'introduzione e il funzionamento di una serie di programmi – aumenta la probabilità che vengano impiegati procedimenti e metodi di trattamento dati diversi e incompatibili rispetto agli standard adottati in altri comparti dell'istituzione.

Responsabilità degli organi direttivi

Spetta alla direzione della banca il compito di assicurare che le operazioni siano adeguatamente protette contro i rischi menzionati in precedenza. La prima azione che gli organi direttivi devono compiere è la fissazione di adeguate *misure preventive* destinate a rendere minima la probabilità che tali rischi si concretizzino. Esempi di misure preventive sono l'accurata progettazione e localizzazione dei centri informatici, i controlli sull'immissione di dati, i dispositivi di sicurezza per prevenire l'accesso non autorizzato alle installazioni di PC e l'uso di una parola chiave per limitare l'accesso a programmi e dati.

Poiché un'azione preventiva non può mai essere totalmente efficace, la direzione dovrebbe elaborare anche un sistema adeguato di *misure correttive*. Queste devono servire a individuare e contenere gli effetti prodotti da eventi che sfuggono al controllo preventivo e minacciano l'operatività della banca. Tali misure dovrebbero comprendere la duplicazione della capacità delle reti di telecomunicazione e di PC per fronteggiare il rischio di arresto del sistema, nonché procedure di riscontro per individuare errori e piani di emergenza in caso di gravi sinistri. Una particolare misura di contenimento dei danni che dovrebbe far parte di un'accurata politica di EAD consiste in un'assicurazione contro le perdite imputabili a frode da parte di dipendenti, a costi di sostituzione dei dati e a distruzione di software o installazioni.

Audit interno

Spetta inoltre agli amministratori e alla direzione il compito di verificare, sorvegliare e sperimentare i sistemi di controllo informatico per accertarne l'efficacia su base giornaliera e la costante congruità dal punto di vista operativo. Dovrebbe essere posto in atto un regolare programma di test indipendenti delle procedure di sicurezza e di controllo da parte di ispettori, revisori o consulenti. Questo programma dovrebbe essere in grado di individuare le lacune nel sistema di controllo prima che queste compromettano seriamente le operazioni bancarie. La frequenza e la portata dei test di revisione realizzati in ciascun'area dovrebbero riflettere il livello di rischio cui è esposta la banca qualora le procedure di sicurezza e di controllo in quell'area dovessero fallire.

Ruolo delle autorità di vigilanza

Dal punto di vista delle autorità di vigilanza vi è l'esigenza di valutare sia l'adeguatezza della politica seguita da un'istituzione in materia informatica, sia l'efficienza dei suoi sistemi elettronici di controllo e di auditing interni. Un modo in cui le autorità di vigilanza possono assolvere il loro compito è quello di valutare la situazione per mezzo di *questionari* o rapporti, ma più spesso questa funzione è di competenza di revisori o ispettori esterni. Un semplice questionario o rapporto permette generalmente di fornire un'indicazione preliminare alle autorità di vigilanza, ma non dovrebbe essere considerato come un'alternativa a una dettagliata analisi da parte di specialisti della sicurezza o dell'audit informatici. Questa materia è tecnicamente complessa, e in ciascuna banca i diversi tipi di sistemi e di impianti presentano differenze considerevoli in termini di vulnerabilità e di tecniche di controllo.

In un campo così specialistico sarebbe particolarmente utile che le autorità di vigilanza si avvalessero della competenza di *revisori esterni*. Esse dovrebbero essere incentivate a dedicare risorse sufficienti a questo aspetto delle loro funzioni.

Sarebbe raccomandabile richiedere alle banche di richiamare l'attenzione dei revisori esterni su tale area, specificando nel mandato di audit che il revisore esterno valuti periodicamente la solidità delle procedure EAD vitali per l'operatività e l'efficacia dei controlli informatici interni. Il revisore esterno dovrebbe essere anche tenuto a menzionare nel suo rapporto annuale alla direzione eventuali carenze e imperfezioni rilevate nel corso dell'esame effettuato in questo specifico settore.

Nei casi in cui le autorità di vigilanza svolgono le loro funzioni prevalentemente attraverso *ispezioni in loco*, le normali procedure seguite dagli ispettori comprendono colloqui, esami documentali e controlli a campione. Nondimeno, la limitatezza e la scarsa qualificazione delle risorse, oltre ai vincoli di bilancio e di altra natura, rendono difficile agli ispettori il compito di tenere il passo con gli sviluppi nei nuovi sistemi informatici. Indubbiamente è ormai indispensabile che il corpo ispettivo comprenda esperti di EAD la cui formazione corrisponda al grado di sofisticatezza dei sistemi informatici impiegati dalle banche ispezionate.

Sia gli ispettori che i revisori utilizzano di norma, per il loro lavoro nel campo dell'EAD, uno schema oppure un manuale di riferimento, predisposti dalle autorità di vigilanza con l'assistenza di istituzioni specializzate e rivelatisi estremamente utili nell'esercizio dell'attività di vigilanza.