La tutela del capitale intellettuale

di Giancarlo Butti

Abstract

La tutela del capitale intellettuale di un'organizzazione è un processo continuo basato sull'uso di una serie di misure di sicurezza fisica, logica, organizzativa, legali, contrattuali e su una consapevolezza diffusa di quali siano gli asset da proteggere e dei rischi che incombono sugli stessi. Una priorità per chiunque oggi si trovi a operare all'interno di un sistema sempre più complesso. Nell'articolo l'autore delinea la fase iniziale del ciclo di protezione delle informazioni: la loro identificazione.

Profilo dell'autore

Giancarlo Butti è security manager, project manager ed auditor presso gruppi bancari e consulente in ambito sicurezza e privacy presso diverse aziende. È inoltre membro della faculty di ABI Formazione e docente presso diversi istituti. È socio e proboviro di ISACA/AIEA e socio CLUSIT. Partecipa ai gruppi di ricerca di ABI LAB, Oracle Community for Security, ISACA/AIEA.

Keyword

sicurezza economica, capitale intellettuale, analisi del rischio, misure di sicurezza

Introduzione

Nell'articolo 'Il patrimonio delle competenze e il capitale intellettuale: una questione di sicurezza nazionale', Giuseppe Principato giunge sostiene: «da questa analisi emerge abbastanza chiaramente l'importanza del capitale intellettuale nella società contemporanea. Esso è fondamentale non solo per garantire uno sviluppo economico che assicuri migliori condizioni di vita alle persone, ma anche ai fini della sicurezza nazionale di ciascun paese. Le strategie competitive dei singoli Stati dovranno quindi essere orientate sempre di più verso lo sviluppo del capitale intellettuale in modo da assicurarsi il maggior numero di opportunità sul mercato globale»[1]. Prendendo spunto si vuole illustrare quali siano i passi che un'organizzazione deve compiere per tutelare una delle principali componenti del proprio capitale intellettuale, quella costituta dal relativo patrimonio informativo.

Ma cosa si intende per capitale intellettuale? Principato nel suo articolo riporta la definizione che ne fa Stewart[2] secondo la quale il capitale intellettuale è costituito dalla somma di tre elementi principali:

- il capitale umano, quale insieme delle competenze, abilità, capacità e conoscenze (sia implicite, sia esplicite[3]) possedute dai membri di un'organizzazione che permettono di svolgere in maniera efficace ed efficiente le attività istituzionali.
- il capitale organizzativo, costituito da tutte quelle strutture, quei meccanismi, quelle procedure, quei processi formalizzati ma anche non codificati che creano valore per l'organizzazione (fra i componenti del capitale organizzativo si trovano ad esempio brevetti e marchi, elementi della così detta proprietà intellettuale alla quale il diritto internazionale riserva, anche se non in forma omogena, una specifica tutela)
- il capitale relazionale, comprende tutte le relazioni che un'organizzazione instaura con i suoi stakeholder (clienti/utenti, fornitori, finanziatori, comunità locale ecc.)

Altre definizioni sono disponibili in letteratura e Fragouli Evaggelia ne riporta alcune nel suo articolo *Intellectual Capital & Organizational Advantage: an economic approach to its valuation and measurement*[4].

Per semplificare la trattazione, nel testo si parlerà genericamente di informazioni; tale concetto va inteso in senso trasversale alle tre sfaccettature classiche del capitale intellettuale, come sopra classificate, e vuole riferirsi sia ad un insieme di dati più o meno articolati e complessi, sia alle istruzioni relative all'utilizzo di tali dati.

In questo articolo non vengono prese ad in considerazione, ad esempio, quelle componenti del capitale umano che con estrema difficoltà possono essere formalizzate sotto forma di informazioni, ma che possono essere trasmesse con un affiancamento (come accade per molte attività manuali di alto artigianato che contraddistinguono la realtà italiana).

Considerando la valenza strategica che il capitale intellettuale riveste per una organizzazione, il problema della sua tutela non può essere affrontata adottando un semplice modello deterministico, quanto piuttosto tramite un approccio che si potrebbe definire euristico[5]. È infatti necessaria una costante attività di ricerca ed interpretazione che fornisca le conoscenze necessarie a definire esigenze e regole di protezione; tali conoscenze costituiscono anche la base per i successivi approfondimenti ed aggiornamenti che tengano conto della evoluzione e del ciclo di vita del 'capitale intellettuale'.

Il ciclo di protezione

Per tutelare il proprio patrimonio informativo le organizzazioni devono mettere in atto una serie di misure di sicurezza fisica, logica, organizzativa, legali e contrattuali nonché una intensa attività di formazione e sensibilizzazione a partire dai vertici aziendali.

Nel definire ed implementare tali misure, le organizzazioni devono prendere in considerazione sia la dinamicità del contesto interno ed esterno, sia l'evoluzione che le informazioni hanno durante il loro ciclo di vita. Questo si può ottenere idealmente mediante l'attuazione nel continuo di una serie di attività che partono con l'identificazione degli asset da proteggere (singolarmente o per classi omogenee) identificandone tipologia, collocazione e correlazioni.

In considerazione della natura intrinsecamente immateriale (intangibile) del bene da proteggere (le informazioni che sono parte del capitale intellettuale) prima di procedere nelle attività sopra indicate è opportuno effettuare una semplice considerazione: qualunque informazione richiede

obbligatoriamente, per la propria gestione e conservazione, un supporto fisico (quindi un asset tangibile). Si è abitualmente portati a considerare a questo riguardo che le informazioni siano conservate nel sistema informativo, nei relativi supporti di backup, su carta (un tempo nei microfilm e microfiche), su CD/DVD.

Troppo spesso ci si dimentica che le informazioni che costituiscono il proprio capitale intellettuale sono presenti in ambiti materiali molto più estesi, quali ad esempio prototipi, impianti, composti chimici o che siano, il patrimonio intellettuale specifico dei collaboratori[6] (quest'ultimo definito a volte capitale umano). La tutela di asset intangibili, quali sono le informazioni, non può quindi prescindere dalla protezione degli asset tangibili che li contengono. È quindi fondamentale non solo identificare quali siano gli asset informativi da proteggere, ma anche quali siano i relativi supporti fisici che li racchiudono.

Identificazione degli asset

Si può proteggere solo ciò che si conosce

L' identificazione degli asset da proteggere non si riduce tuttavia ad una mera elencazione; se infatti, per quanto attiene i tradizionali supporti fisici, è relativamente semplice capire dove sono le informazioni che costituiscono il proprio capitale intellettuale, molto meno facile è individuare quelle aree nelle quali tali informazioni siano patrimonio informativo non condiviso di qualche collaboratore.

Giuseppe Principato, nel suo articolo precedentemente citato, evidenziava come le competenze di una persona siano un insieme di esperienze finalizzate, conoscenze e capacità. In questo articolo prendiamo in considerazione solo la componente informativa, formalizzabile e quindi passibile di essere messa facilmente a fattor comune di altri colleghi, diventando quindi a tutti gli effetti patrimonio informativo dell'organizzazione.

Nella mia lunga esperienza lavorativa, in aziende di settori e dimensioni molto diverse, ho sempre riscontrato la presenza di qualche figura chiave (l'unica in grado di risolvere particolari situazioni) che custodiva gelosamente le informazioni che la rendevano indispensabile. Individuare e formalizzare tale componente del patrimonio informativo non è facile. In molti casi la presenza non formalizzata di tale capitale non è nemmeno evidente; spesso si subiscono le conseguenze della perdita di specifiche competenze anche dopo anni dalla fuoriuscita dei collaboratori dell'azienda; è per tale motivo che i costi di tale perdita difficilmente possono essere rilevati e quantificati in via preventiva.

Vengono così a mancare importanti elementi per una corretta valutazione dei rischi e delle relative contromisure (che devono ovviamente essere economicamente proporzionate al valore del bene da proteggere). Per i motivi sopra elencati la cultura e le policy aziendali dovrebbero evitare situazioni che permettano ad un'organizzazione di dipendere da un solo collaboratore per lo svolgimento di qualche attività e non dovrebbe essere tollerata la mancata condivisione di informazioni da parte di tale soggetto.

Nella realtà la maggior parte delle organizzazioni si comportano in modo miope, premiando le proprie figure chiave in funzione dei risultati raggiunti e non anche in funzione della loro capacità

di condivisione e formalizzazione delle conoscenze acquisite, incentivando in questo modo l'accentramento della conoscenza presso pochi soggetti e perdendo di conseguenza il controllo su parti significative del proprio patrimonio informativo.

Informazioni implicite ed esplicite

Le informazioni che non sono in qualche modo formalizzate, ma che costituiscono, ad esempio, il patrimonio personale esclusivo di un collaboratore, sono definite implicite. Viceversa le informazioni che in forma sia strutturata (un database) sia non strutturate (documenti), sono formalizzate, sono definite esplicite.

A queste due definizioni aggiungo personalmente quella di informazioni parzialmente esplicite. Nella pratica si tratta delle informazioni che pur essendo formalizzate non sono direttamente fruibili, ma richiedono per la loro fruizione un importante lavoro di decodifica o di misura.

Un tipico esempio di ciò che considero appartenente a questa categoria è costituito dalle applicazioni software. Senza opportuna documentazione di supporto un'applicazione software di media complessità è difficilmente gestibile e manutenibile se non da chi l'ha realizzata. È tuttavia innegabile che il codice di un'applicazione software è quanto di più formalizzato (e quindi teoricamente esplicito) possa esistere, in quanto traduce in un codice una serie di algoritmi definiti in fase di analisi.

Un altro esempio è costituito dalla taratura degli strumenti o dalla messa a punto di un congegno meccanico. L'insieme delle informazioni che ne permettono un perfetto funzionamento diventano embedded nel congegno stesso e la loro esplicitazione richiede una misurazione dei parametri impostati. Questa differenziazione non è solo accademica: in relazione al fatto che le informazioni siano implicite, esplicite o parzialmente esplicite variano le tecniche di protezione.

Mentre per le informazioni esplicite valgono i normali criteri di protezione basati sull'insieme di misure precedentemente citate, le informazioni implicite difficilmente possono essere protette se non vengono in qualche modo formalizzate. Solo in casi eccezionali, mantenere implicita una informazione (e quindi di fatto segreta) costituisce di per sé stessa una misura di tutela. Questo accade ad esempio in un'azienda allorquando è lo stesso imprenditore che detiene l'informazione.

Un mio conoscente aveva sviluppato diversi brevetti nell'ambito di prodotti realizzati con fibre di vetro. Per evitare che le maestranze fossero in grado di vendere alla concorrenza segreti relativi al processo di lavorazione aveva appositamente tarato in modo anomalo gli strumenti di misura di temperatura e pressione. In questo modo i suoi collaboratori non potevano conoscere parametri fondamentali per la corretta riuscita del trattamento del materiale. La mancata formalizzazione di questi valori, che erano noti solo all'imprenditore, costituiva un ottimo sistema di difesa del processo produttivo.

L'esempio qui riportato anticipa un concetto che verrà ripreso più avanti nell'ambito delle tutele legali. Il deposito di un brevetto rende di fatto pubbliche le informazioni relative all'oggetto del brevetto (che quindi sono tutelate solo dal punto di vista legale), mentre possono restare **segrete**, e quindi diversamente tutelate (anche dal punto di vista legale), le informazioni che riguardano ad esempio il processo produttivo.

Va da sé che le informazioni segrete non lo sono in senso assoluto, ma si intendono tali al di fuori dell'organizzazione (è evidente che i collaboratori dell'organizzazione solitamente possono aver accesso per lo svolgimento delle proprie attività ad informazioni che la stessa considera segrete).

Il primo passo per rendere proteggibili un'informazioni implicita è quello di esplicitarla, formalizzandola. Da diversi anni sono anche disponibili strumenti che consentono di pubblicare e condividere le informazioni. Si va dai semplici portali aziendali a vere e proprie applicazioni di knowledge management che consentono di mappare e sviluppare la conoscenza dell'organizzazione. L'ostacolo maggiore in tale attività non è però costituito dagli strumenti, quanto dalla resistenza posta da chi considera il proprio patrimonio informativo come una forma potere a cui non vuole rinunciare. Solo adeguate politiche di gestione delle risorse umane possono in questo caso premiare la condivisione.

Tabella 1 – Classificazione delle informazioni costituenti il capitale intellettuale

INFORMAZIONI	
Esplicite	Documenti, sistema informativo…
Implicite	Processi reali, prassi aziendali, conoscenze personali di collaboratori
Parzialmente esplicite	Software, taratura strumenti, prototipi, composti

Tabella 2 – Esempi di informazioni

INFORMAZIONI ESPLICITE	
DOCUMENTAZIONE	• manuali di prodotto, di processo, di istruzione • corsi • brevetti • documentazione tecnica • documentazione commerciale • documentazione legale • documentazione fiscale • …
SISTEMA INFORMATIVO	• database • datawarehouse • archivi documentali • archivi di posta elettronica • archivi fax • archivi multimediali (sia digitali che analogici) • Internet • Intranet • …

INFORMAZIONI IMPLICITE
• soluzioni vincenti e non vincenti • esperienze positive e negative • conoscenze personali • lezioni apprese • interpretazioni • riflessioni • scenari • idee • processi non documentati • prassi • …

Collocazione degli asset

Un altro aspetto che va considerato nel censimento degli asset da proteggere riguarda la loro collocazione fisica e concettuale. Anche in questo caso è necessario considerare che le informazioni costituenti il proprio patrimonio informativo possono essere presenti sia in asset fisici propriamente detti, sia essere patrimonio dei collaboratori di clienti e fornitori (si considerino ad esempio le informazioni sul processo di lavorazione con cui viene realizzato da un fornitore un componente importante di un prodotto brevettato dall'organizzazione).

Tabella 4 – Collocazione degli asset da proteggere

COLLOCAZIONE DEGLI ASSET INFORMATIVI	
ASSET FISICI	**CAPITALE UMANO**
Presso l'organizzazione	Dipendenti, collaboratori e consulenti
Presso i fornitori/subfornitori	Dipendenti, collaboratori e consulenti del fornitore
Presso i clienti	Dipendenti, collaboratori e consulenti dei clienti
Presso le istituzioni	Dipendenti, collaboratori e consulenti delle istituzioni

Il perimetro degli asset da proteggere si estende così oltre i confini dell'organizzazione, dove la tutela può basarsi unicamente su clausole contrattuali ed attività di audit.

Correlazione fra asset

Dopo aver individuato gli asset da proteggere è opportuno, anche se molto oneroso, individuare le relazioni esistenti fra gli stessi, al fine di ottimizzare sia l'analisi dei rischi, sia le opportune contromisure. Solo in questo modo sarà possibile effettuare una corretta valutazione dei costi/benefici di una misura di sicurezza. Come già sopra ricordato le informazioni da tutelare sono presenti in asset fisici, siano questi apparecchiature, documenti… o sono patrimonio degli individui.

Misure poste a tutela dei collaboratori o degli asset fisici aziendali tutelano di conseguenza anche il patrimonio informativo in essi contenuto.

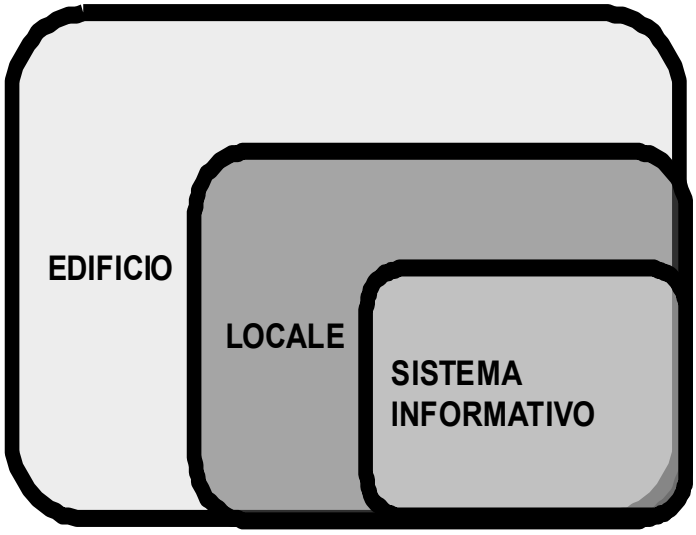

Figura 1 - Relazione fra asset

Proteggere ciò che serve

Le informazioni che sono state individuate sono veramente meritevoli di protezione?

L'attività di censimento degli asset non deve limitarsi ad individuare le informazioni ed i relativi 'contenitori, ma deve anche valutarne la qualità in termini di esigenza di protezione. È quindi fondamentale concentrare le proprie risorse per proteggere adeguatamente gli asset effettivamente importanti per l'azienda, classificando le informazioni in funzione sia del loro livello di importanza, sia dal punto di vista della loro riservatezza. Se le informazioni censite sono di dominio pubblico o se riguardano prodotti già esistenti sul mercato non è necessario mettere in atto un alto livello di protezione[7].

La valutazione dei rischi

L'attività di analisi del rischio può essere svolta utilizzando numerose metodologie di tipo quantitativo, qualitativo o semiquantitativo.

Al riguardo esistono diversi repertori quali ad esempio l'Inventory of Risk Management / Risk Assessment Methods and Tools di Enisa[8] o il documento Risk Analysis Approfondimenti dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione[9].

Sono inoltre stati prodotti numerosi frame work per guidare ad una più completa ed esaustiva gestione del rischio fra i quali il Cyber Security Framework del NIST[10] o il Framework Nazionale per la Cyber Security[11].

Alcuni di questi, come il già citato Framework Nazionale per la Cyber Security o il Pacchetto informativo per le PMI[12] sono pensati in funzione della specifica realtà italiana, che è costituita principalmente da realtà medio piccole.

Metodologie più articolate che prendono in considerazione l'insieme dei processi aziendali sono descritte ad esempio nell'articolo Un modello di valutazione dei rischi relativamente al trattamento dei dati personali nelle comunicazioni elettroniche[13] che anticipa le richieste del GDPR (General Data Protection Regulation).

Una grande opportunità per le organizzazione per proteggere il proprio patrimonio informativo deriverà infatti dagli adeguamenti richiesti al GDPR europeo, che costringerà tutti coloro che trattano dati personali a rivedere le proprie strategie di sicurezza. Anche se le informazioni trattate in questo articolo sono in genere qualcosa di diverso dai dati personali (salvo ad esempio l'elenco dei clienti), nondimeno utilizzano in genere gli stessi strumenti ed infrastrutture e sono soggetti agli stessi rischi.

Non è scopo di questo articolo illustrare metodologie di analisi dei rischi, rinviando ai documenti sopra citati. Ci si limiterà pertanto ad illustrare alcuni esempi degli elementi che sono coinvolti in tale analisi.

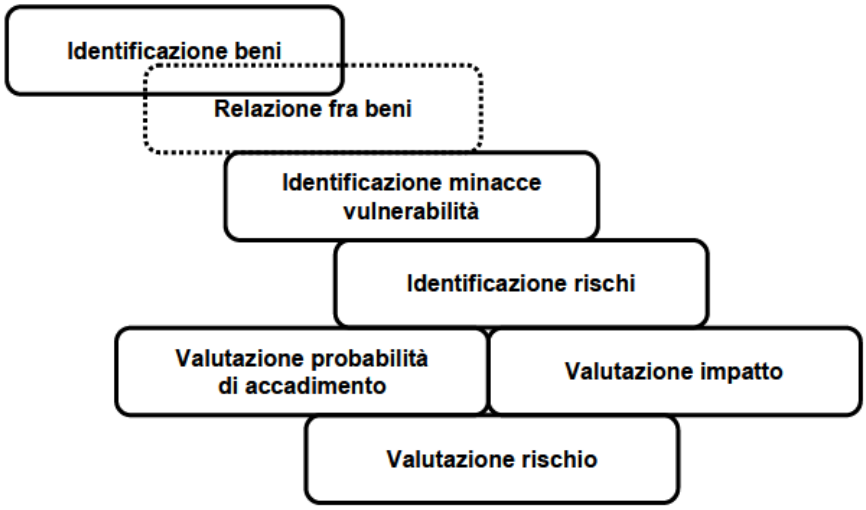

Figura 2 - Generico modello di analisi dei rischi

Una generica attività di analisi dei rischi prevede, dopo aver identificato gli asset da proteggere, a:

- identificare minacce e vulnerabilità
- valutare le probabilità di accadimento
- valutare i possibili impatti
- identificare e quantificare i rischi diretti, indiretti, consequenziali e la loro valorizzazione
- identificare le opportune misure di sicurezza in rapporto ai costi/beneficii
- gestire il rischio residuo
- valutare l' efficacia/efficienza delle misure predisposte.

il tutto secondo un ciclo ben noto e consolidato nella letteratura e negli standard ISO quali la 27001.

Nel seguito sono rappresentati esempi di minacce e vulnerabilità relative ad asset materiali ed immateriali.

Tabella 5 – Minacce relative ad asset materiali ed immateriali

MINACCE
Ambientali (Meteorologiche, Sismiche/Vulcaniche/Zunami), Macchie solari, Biologiche (Malattie/Epidemie),…
Accidentali (Esplosioni, Incendi, Cedimenti strutturali, Guasti agli impianti/sistemi informativi, Interruzione utilities ….)
Azioni volontarie da parte di personale interno/esterno (Furto, Danneggiamento, Accesso illecito, Alterazione dati…)
Azioni involontarie da parte di personale interno/esterno (Danneggiamento, Alterazione dati…)

Tabella 6 – Alcune minacce relative agli asset materiali ed immateriali

MINACCE AGLI ASSET MATERIALI	
Furto/Sottrazione/Perdita Guasto Danneggiamento/Distruzione/Alterazione Inaccessibilità (di breve/lungo periodo) Accesso/uso illegittimo/improprio (ad edifici, sistemi, attrezzature…) Invecchiamento (reale, tecnologico…) Assenza	
MINACCE AGLI ASSET IMMATERIALI	
Dirette	Copia illecita (la sottrazione dell'asset può anche non essere evidente, in quanto la copia dell'informazione ha lo stesso valore dell'originale, che quindi non scompare) Intercettazione/Consultazione Inaccessibilità Alterazione dell'informazione (modifica, correzione, cancellazione, inserimento di informazioni errate…) Comunicazione/diffusione illecita Perdita di qualità (degrado, invecchiamento…) Assenza o mancata esplicitazione Perdita
'Derivate'	Tutte quelle legate al 'contenitore' dell'informazione Tutte quelle legate al 'soggetto' che detiene l'informazione

Tabella 7 – Esempi di vulnerabilità relative ad asset materiali ed immateriali

VULNERABILITÀ	
Carenze Organizzative	Mancata regolamentazione a vari livelli Mancata definizione dei ruoli Mancanza di procedure, policy… Mancata identificazione del valore delle risorse Mancata identificazione dei rischi Mancata identificazione ed implementazione di adeguate contromisure Mancata definizione dei controlli e del processo di gestione degli stessi Mancata definizione della responsabilità dei controlli
Carenze nelle Risorse umane	Mancanza di una procedura di selezione e valutazione del personale Mancata gestione delle risorse umane e delle loro aspettative Mancato monitoraggio e valutazione dei livelli gerarchici Mancato monitoraggio del clima aziendale Mancanza di formazione Mancanza di norme di comportamento Insufficiente numero di addetti
Errori involontari nell'ambito dei sistemi informativi	Errori nella progettazione, installazione, implementazione, configurazione, gestione di hardware, software di base, software applicativo, software specialistico ed appliance, apparecchiature, sistemi di sicurezza Errori nella documentazione Errori nell'uso delle applicazioni Errori nel caricamento dati Errori nelle elaborazioni Errori dei sistemi Errori nel trasferimento dati Errori nelle comunicazioni Complessità dei sistemi

Per poter individuare le opportune contromisure è necessario declinare nella realtà dell'organizzazione come una minaccia possa manifestarsi.

Nella Tabella 9 sono elencate alcune possibile modalità con cui può essere sottratta una informazione che l'organizzazione considera segreta, mentre nella Tabella 10 sono elencate possibili modalità con cui involontariamente un collaboratore può diffondere informazioni sull'organizzazione.

Dovrebbero essere valutati inoltre anche altri aspetti; nella tabella che segue sono elencate le possibili conseguenze sul patrimonio informativo di un'organizzazione derivanti da una perdita parziale o totale di un collaboratore.

Tabella 8 – Conseguenze al patrimonio informativo derivante dalla perdita di un collaboratore

Perdita assoluta	Perdita di informazione che il collaboratore non aveva condiviso ed esplicitato e che quindi non sono state acquisite nel patrimonio informativo aziendale Danno derivante dal passaggio del collaboratore alla concorrenza alla quale potrà 'vendere' le proprie specifiche competenze e le informazioni relative all'azienda di provenienza
Perdita parziale	Perdita di competenza e conoscenza in seguito a variazione di ruolo in azienda Degrado delle prestazioni in seguito ad insoddisfazione o 'stress'

Tabella 9 – Sottrazione di informazioni

'SOTTRAZIONE' DI INFORMAZIONI	
Con furto del 'contenitore'	Furto di: • documenti • supporti magnetici/ottici • pc • prototipi…
Senza furto del contenitore	Consultazione, osservazione di: • documenti • dati sul sistema informativo • comportamenti • impianti… • Copia di: • documenti • supporti magnetici/ottici • Fotografie, riprese video, registrazioni audio…
Intercettazione	• di comunicazioni e trasmissioni (telefoniche, vocali, e-mail, transazioni su rete locale o geografica, radio...) • dei tasti premuti sulla tastiera • delle emissioni video…
Recupero	Rifiuti (documenti, supporti, oggetti…) Dischi di apparati dismessi o in riparazione
Ricostruzione	Abbinamento di informazioni da diverse fonti, anche pubbliche
Social engineering	• assunzione di personale proveniente da altra azienda • colloqui di lavoro con personale di altra azienda • due diligence non seguita da acquisizione dell'azienda • visita agli impianti da parte di falsi clienti • falsi profili social per la raccolta di informazioni • …

Tabella 10 – Diffusione involontaria di informazioni

'DIFFUSIONE' DI INFORMAZIONI
• Pubblicazione di informazioni sui progetti seguiti (a volta con indicazione del cliente) su social professionali come linkedin • Pubblicazione sui social e blog di commenti e risultati della propria attività • Parlare di lavoro in luoghi pubblici e mezzi pubblici • Rispondere a telefonate di lavoro in luoghi pubblici e mezzi pubblici • Rispondere a messaggi o lavorare con pc e tablet in luoghi pubblici o su mezzi pubblici che consentano a terzi di visualizzare lo schermo del proprio dispositivo • Pubblicare articoli, partecipare a convegni e seminari presentando i risultati della propria attività senza validazione dell'organizzazione • Usare in modo promiscuo (personale e lavorativo) propri dispositivi senza adeguata protezione • Lasciare documenti sulle scrivanie o nelle sale riunioni • Non distruggere i documenti • …

Le misure di sicurezza

Le misure di sicurezza sono quei presidi che consentono di ridurre la probabilità o l'impatto di un evento dannoso; possono essere raggruppate con diversi criteri.

Tabella 11 – Classificazione delle misure di sicurezza

CLASSIFICAZIONE DELLE MISURE DI SICUREZZA		
Per ambito	Organizzative Fisiche Logiche Legali	
Per momento	Preventive Successive	Se si utilizzano dischi in RAID o componenti ridondati in un server, si riduce preventivamente la possibilità di perdita di dati o di interruzione di un servizio in seguito alla rottura o guasto di un componente. La disponibilità di copie aggiornate di dati, di immagini dei dischi, di un contratto di assistenza con intervento immediato, riduce l'impatto derivante dalla perdita di dati o dal fermo di un servizio consentendo a posteriori di ripristinare dati e sistemi.
Per finalità	Riduzione delle probabilità di accadimento Limitazione dell'impatto	Se si utilizzano dischi in RAID si riducono le probabilità del blocco di un server. Se si dispone di copie aggiornate di dati, di immagini dei dischi, di un contratto di assistenza con intervento immediato si riduce l'impatto derivante da un malfunzionamento di un server.

Ciclo di vita delle misure di sicurezza

L'implementazione di una misura di sicurezza prevede una serie di attività e una revisione periodica della validità delle scelte effettuate.

Tabella 12 – Ciclo di vita delle misure di sicurezza

CICLO DI VITA DELLE MISURE DI SICUREZZA	
Fase preliminare	Identificazione Valutazione dei costi/benefici Valutazione in relazione alle altre misure in essere Progettazione Implementazione Gestione del rischio residuo Definizione di procedure di gestione e controllo Formazione
Processo di gestione	Controllo di attivazione delle misure di sicurezza Controllo di efficacia delle misure di sicurezza Procedura di intervento in caso di allarme
Revisione periodica	Controllo periodico della adeguatezza delle misure di sicurezza in atto

Consideriamo ad esempio il caso di una comune misura di sicurezza quale un antifurto; la decisione della sua implementazione deriva da un'analisi dei rischi (non necessariamente formalizzata) che ha evidenziato come sia opportuno attivare questa misura di sicurezza a tutela di uno o più asset aziendali.

La scelta del tipo di soluzione può essere vincolata da aspetti tecnici (posizionamento, interazione con altre misure di sicurezza già in essere…), economici (favorevole rapporto costi/benefici), normativi; è inoltre opportuno valutare eventuali controindicazioni.

Per l'adeguata gestione delle misure di sicurezza devono essere definite una serie di regole, in quanto le misure tecniche devono essere SEMPRE accompagnate da procedure di gestione nei vari momenti del loro ciclo di vita:

- l'attivazione dell'antifurto può essere automatica, basata ad esempio su una programmazione oraria, oppure manuale; in questo caso va definito chi deve inserire l'antifurto (ad esempio l'ultimo ad uscire dall'ufficio)
- è necessario verificare con dei controlli a campione che effettivamente tale policy aziendale sia nota, che l'antifurto venga effettivamente inserito, che effettivamente l'antifurto funzioni
- deve essere definito quale comportamento adottare in caso di allarme, chi deve essere avvisato, come intervenire.

Tali regole si sommano a quelle di carattere più generale che rappresentano le misure di sicurezza organizzativa.

Parte delle attività manuali descritte nell'esempio potrebbe essere eliminata, riducendo il rischio di errore e la necessità di controlli, se:

- l'antifurto entra in funzione ad una certa ora e solo in caso di variazione di orario è necessario attivarlo manualmente

– il sistema è dotato di strumenti diagnostici che segnalano malfunzionamenti, eventualmente con chiamata automatica al servizio di manutenzione.

A seguire alcuni esempi di misure di sicurezza di varia natura.

Tabella 13 – Esempio di misure di sicurezza

PROTEZIONE DA TENTATIVI DI ACCESSO NON AUTORIZZATI	
Aspetti tecnici	Protezione perimetrale Pareti di adeguata robustezza Recinzioni Cancello esterno Porte blindate Serrature di sicurezza Finestre con grate Vetri antisfondamento Videosorveglianza Monitoraggio movimentazione interna asset (RFID)
Aspetti organizzativi e gestionali	Verifica periodica dell'integrità delle barriere fisiche Procedura di gestione dei supporti delle registrazioni video Procedura di gestione dell'accesso alle registrazioni video Procedura di allerta Non pubblicizzare (ad esempio sulle planimetrie esposte per i piani di fuga) le zone con elementi critici per l'azienda

Tabella 14 – Esempio di misure di sicurezza

BACKUP E RIPRISTINO	
Misure tecniche ed organizzative per la gestione delle copie di dati e software, per la loro conservazione e per la verifica della effettiva capacità di ripristino	
Aspetti tecnici	Copia periodica (software, dati, configurazioni, log…)
Aspetti organizzativi e gestionali	Identificazione delle risorse che richiedono copia Definizione delle modalità di copia Definizione della frequenza di copia Documentazione delle configurazioni Uso di supporti alternati Custodia dei supporti in luogo controllato durante la permanenza Custodia delle copie in luogo sicuro, diverso da quello principale Custodia durante tutto il tragitto di trasferimento fra il luogo di generazione delle copie ed il luogo di conservazione Verifica periodica delle copie Verifica periodica della capacità di ripristino dei sistemi Rigenerazione periodica delle risorse di dati archiviati Rigenerazione periodica di dati criptati Sostituzione periodica dei supporti

Tabella 15 – Esempio di misure di sicurezza: policy aziendale sulle comunicazioni

Cosa fare	Cosa non fare
Telefono	
• Fornire solo le informazioni per le quali si è stati esplicitamente autorizzati • Segnalare al proprio responsabile richieste inusuali di informazioni • Nel caso di comunicazioni in viva voce informare l'interlocutore dell'attivazione di tale modalità e della presenza di eventuali altri ascoltatori; verificare in questo caso la presenza di terzi non autorizzati	• Fornire informazioni sulle misure di sicurezza in atto • Fornire informazioni sull'organizzazione aziendale • Fornire le proprie credenziali di autenticazione • Fornire informazioni relative agli interessati a terzi non autorizzati
Segreterie telefoniche	
	• Lasciare informazioni riservate sulle segreterie telefoniche
Cellulari	
• Utilizzare password di accesso per la protezione della rubrica e dei dati • Bloccare il cellulare in caso di perdita o furto	• Effettuare registrazioni audio, video o fotografiche mediante cellulari, palmari o altri dispositivi se non preventivamente autorizzati
Fax in uscita (effettuabile solo da personale preventivamente autorizzato)	
• Controllare il numero di telefono chiamato • Aggiungere avvertenza sulla riservatezza sui documenti inoltrati • Verificare il corretto inoltro • Cancellare la memoria	• Dimenticare i documenti inoltrati e relativa ricevuta • EFFETTUARE INOLTRI AUTOMATIZZATI SENZA CONSENSO DEGLI INTERESSATI
Fax/posta in entrata	
• Controllare il destinatario (azienda) prima di accedere ai documenti • Controllare il destinatario (interno) prima di accedere ai documenti • Cancellare la memoria	• Accedere a documenti che non ci sono indirizzati
Posta convenzionale in uscita (effettuabile solo da personale preventivamente autorizzato)	
• Controllare che il destinatario sia corretto • Utilizzare una modalità di trasmissione congruente alla tipologia di dato (esempio: assicurata per dati sensibili)	

<table>
<tr><td colspan="2">Posta elettronica (*)
La posta elettronica non fornisce garanzia di consegna al destinarlo e non da alcuna garanzia di riservatezza del messaggio. L'uso dell'e-mail e la sua valenza ai fini contrattuali con le controparti deve essere regolamentata.
(*) Ipotesi di regole da coordinare con il Provvedimento del Garante: Lavoro: le linee guida del Garante per posta elettronica e internet - Gazzetta Ufficiale n. 58 del 10 marzo 2007</td></tr>
<tr><td>• L'uso dell'e-mail è limitato ai soggetti autorizzati
• La posta elettronica è utilizzabile solo per fini aziendali
• Nel caso di inoltro a più destinatari utilizzare come indirizzo di destinazione quello dell'azienda e mettere in CCN i singoli destinatari, per evitare che un destinatario possa conoscere l'indirizzo degli altri
• Utilizzare il disclaimer riportato
• L'invio di comunicazioni ufficiali o contenenti impegni contrattuali e precontrattuali deve essere autorizzata dal Titolare</td><td>• Utilizzare l'indirizzo aziendale a fini personali
• INOLTRARE IN AUTOMATICO E-MAIL SENZA CONSENSO DELL'INTERESSATO
• Aprire e-mail e file provenienti da mittenti sconosciuti
• Utilizzare l'e-mail per l'inoltro o ricezione di dati sensibili, giudiziari o riservati
• Inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica</td></tr>
<tr><td colspan="2">Posta elettronica certificata (effettuabile solo da personale preventivamente autorizzato)
La PEC ha lo stesso valore della raccomandata r.r. fra due caselle di PEC; il suo utilizzo deve sottostare alle medesime regole aziendali che riguardano l'utilizzo della posta tradizionale.</td></tr>
<tr><td>• L'uso della PEC è limitato ai soggetti autorizzati
• Verificare periodicamente la casella di PEC</td><td></td></tr>
<tr><td colspan="2">Conversazioni</td></tr>
<tr><td></td><td>• Parlare con terzi o in luoghi pubblici o aperti al pubblico di fatti relativi all'attività aziendale
• Parlare anche con colleghi o in luoghi aziendali condivisi di informazioni alle quali tali colleghi non sono autorizzati ad accedere</td></tr>
<tr><td colspan="2">Visitatori</td></tr>
<tr><td>• Verificare l'identità
• Invitare i visitatori a sostare nelle aree di attesa
• Accompagnare i visitatori presso l'area di destinazione</td><td>• Lasciare documenti visibili
• Consentire l'accesso alle aree riservate
• Consentire l'accesso a dati o documenti
• Lasciare da solo un visitatore in un locale dove sono presenti documenti</td></tr>
<tr><td colspan="2">Sale riunioni</td></tr>
<tr><td></td><td>• Lasciare materiale nelle sale riunioni</td></tr>
<tr><td colspan="2">Convegni – Pubblicazioni – Social network</td></tr>
<tr><td></td><td>• Dare informazioni sull'azienda e sulle attività dell'azienda senza la preventiva autorizzazione del Titolare</td></tr>
</table>

Coerenza nelle contromisure

Un altro aspetto importante nella scelta e gestione delle misure di sicurezza è che queste siano fra loro coerenti: il livello di protezione di un asset è condizionato dalla misura di sicurezza più debole o dall'assenza di una particolare misura di sicurezza.

Ad esempio se un'informazione è presente nel sistema informativo aziendale, è possibile mettere in atto misure di protezione logiche, organizzative e fisiche, che consentano solo a ruoli ben definiti di accedervi.

Organizzazioni di una certa dimensione sono dotate in genere di sistemi centrali di elaborazione dati che offrono un'elevata protezione a livello logico; tuttavia sono diverse le situazioni in cui tale livello di sicurezza può diminuire drasticamente: ad esempio quando un file viene trasferito dal sistema centrale su un pc per effettuare elaborazioni con prodotti di operatività individuale.

Questo caso, frequentissimo, riduce il livello di protezione alle misure di sicurezza presenti sul pc. Tali misure sono in genere facilmente superabili (ad esempio attivando il pc con un sistema operativo diverso lanciato da CD o altro supporto, è possibile accedere al contenuto del disco senza necessità di alcuna autenticazione).

Anche la sicurezza fisica del pc è in genere più limitata rispetto a quella riservata ai sistemi centrali.

Un ulteriore degrado nel livello di protezione dei dati si ha quando un file viene esportato su un supporto rimuovibile. In questo caso la protezione si limita alla sicurezza fisica del supporto, salvo il raro caso che l'utente che ha effettuato tale operazione non abbia avuto l'accortezza di criptare il file.

Analogamente, il livello di protezione quasi si annulla nel caso in cui il contenuto del file venga stampato; il documento così prodotto ha un livello di protezione pari unicamente a quello della sicurezza fisica dello stesso. La gestione dei documenti lascia molto spesso a desiderare anche nelle aziende più organizzate, in quanto sono spesso trascurati parti importanti del loro processo di gestione, quali ad esempio lo smaltimento.

È quindi necessario un approccio complessivo nell'individuare le misure di sicurezza da adottare in quanto anche le migliori soluzioni tecniche possono essere vanificate da errati comportamenti degli utenti, derivanti da scarsa sensibilità, da scarsa formazione, o molto spesso da assenza di regolamentazione.

È inoltre indispensabile un adeguato presidio che verifichi l'applicazione delle regole; in assenza di adeguati controlli, l'efficacia delle misure di sicurezza può ridursi sensibilmente o annullarsi del tutto.

Differenza nelle contromisure

Esistono diverse tipologie di misure di sicurezza; in particolare lo stesso risultato può essere ottenuto utilizzando misure tecniche o misure organizzative (regole da seguire). Mentre il vincolo tecnico (ad esempio la lunghezza di una password) non può essere violato dall'utente, la misura

organizzativa può essere facilmente disattesa. Cambiano quindi i tipi di controlli da eseguire, la loro frequenza, l'impegno richiesto per effettuarli. Nel caso della misura tecnica, sarà sufficiente verificare che la stessa sia stata correttamente implementata e che l'utente non abbia la possibilità di modificarla.

Nel caso della misura organizzativa, sarà necessario effettuare impegnativi controlli a campione per verificare il rispetto delle prescrizioni date.

La tutela legale

La tutela legale del capitale intellettuale copre diversi ambiti.

Non esiste alcuna normativa che obbliga una organizzazione a tutelare il proprio capitale intellettuale; esistono tuttavia numerose normative che, nate con la finalità di tutelare interessi di terzi (ad esempio i dati personali, la salute e la sicurezza dei lavoratori, la continuità del servizio per le pubbliche amministrazioni o per il sistema bancario…) obbligano le organizzazioni a dotarsi di strumenti e misure di sicurezza che indirettamente tutelano anche tale capitale.

Inoltre esistono una serie di misure che il legislatore (o meglio i legislatori a livello internazionale) hanno posto in essere per tutelare la così detta proprietà intellettuale (diritto d'autore, brevetti, marchi...[14]) in particolare allorquando le informazioni diventano di dominio pubblico.

È infatti proprio la caratteristica di pubblicità che fa perdere a tali informazioni la protezione intrinseca derivante dalle misure di sicurezza messe in atto dall'organizzazione.

Del resto quando un prodotto (tangibile come ad esempio un automobile o intangibile come un software) è sul mercato è possibile individuarne i componenti e ricostruirne il funzionamento con attività più o meno complesse di *reverse engineering*.

Al produttore non resta quindi che affidarsi alla tutela legale del prodotto finito ed a forme integrate di difesa per le componenti tangibili ed intangibili che possono restare segrete.

La normativa italiana prevede anche per queste informazioni una specifica tutela[15] che si affianca alle misure di sicurezza che necessariamente (lo prevede la stessa normativa) l'organizzazione deve mettere in atto.

Le informazioni segrete non sono strettamente quelle di natura tecnica, ma possono essere anche quelle di natura commerciale ed organizzativa; lo stesso elenco dei clienti, se contiene ulteriori informazioni significative per il business dell'organizzazione, può essere oggetto di tutela.

Relativamente alla capacità attuale di mantenere segrete le informazioni è comunque utile citare la seguente affermazione di Joel Brenner (consulente senior NSA): «Ci saranno pochi segreti, ormai, e le cose che saranno tenute segrete non resteranno segrete a lungo. L'obiettivo reale oggi, in tema di sicurezza, è ritardare l'emivita dei segreti. I segreti sono come gli isotopi.»

In alcuni casi un'informazione considerata segreta (ad esempio il risultato di una ricerca) potrebbe portare a risultati interessanti per l'organizzazione che la possiede, ma non immediatamente utilizzabili per i più diversi motivi (economici, strategici…).

L'organizzazione potrebbe allora decidere di non tutelarla legalmente, ma di riservarsi la possibilità di sfruttarla in futuro quando le condizioni si riveleranno favorevoli, impedendo che nel contempo terzi possano ottenere gli stessi risultati e decidano di tutelarli.

Questo si può ottenere rendendo pubblica l'informazione ad esempio tramite la pubblicazione di un articolo.

Di fatto con questo sistema si rende non più tutelabile legalmente l'informazione, che può essere liberamente utilizzata da chiunque.

La tutela contrattuale

Un'ulteriore forma di tutela legale è quella legata ai contratti che l'organizzazione può instaurare con le sue controparti.

Un'organizzazione che vuole tutelare nel tempo il proprio patrimonio informativo dovrebbe formalizzare accordi di riservatezza (anche successivi al rapporto contrattuale) e di non concorrenza con tutte le controparti che in qualche misura entrino in contatto con tali informazioni. Questi soggetti possono essere collaboratori a vario titolo, fornitori, ma anche clienti. Inoltre, tali accordi devono prevedere espressamente che la tutela contrattuale debba intendersi estesa a cascata sia ai collaboratori di clienti e fornitori, sia agli eventuali sub contraenti.

La tutela contrattuale non riguarda solo la protezione dell'informazione, ma permette anche lo sfruttamento economico della stessa, tramite i così detti contratti di trasferimento tecnologico. Questi possono comprendere ad esempio la cessione o la concessione in licenza d'uso ad esempio di brevetti o know how[16].

Conclusioni

Il primo passo per la tutela del capitale intellettuale di un'organizzazione è un'attenta e completa mappatura del proprio patrimonio informativo, la formalizzazione delle informazioni implicite e la definizione di un equilibrato insieme di misure di sicurezza che bilanci rischi e costi di protezione. Sono disponibili anche gratuitamente molti strumenti che possono aiutare le organizzazioni a svolgere al meglio tali attività e l'adeguamento alle richieste del nuovo GDPR potrà costituire un'importante occasione per salvaguardare non solo i dati personali, ma anche il proprio capitale intellettuale.[17]

Le tabelle e stralci del testo relativo alle misure di sicurezza sono ripresi dai libri dell'autore, Giancarlo Butti, *Sicurezza Totale* e *Dalla carta alle nuvole* editi dalla ITER (http://www.iter.it).

Note

(ultimo accesso ai link indicati: 20 giugno 2016)

[1] G. PRINCIPATO, *Il patrimonio delle competenze e il capitale intellettuale: una questione di sicurezza nazionale*, 17 luglio 2014, http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/il-patrimonio-delle-competenze-e-il-capitale-intellettuale.html.

[2] Th. A. STEWART, *Intellectual Capital: The New Wealth of Organizations*, New York 1997.

[3] Il concetto di conoscenza implicita (o tacita) è stato trattato da Ikujiro NONAKA e Hirotaka TAKEUCHI nella loro pubblicazione *The Knowledge-Creating Company* (1995), anticipati da Michael POLANYI nel testo *The Tacit Dimension* (1967)

[4] E. FRAGOULI, *Intellectual capital and organizational advantage: an economic approach to its valuation and measurement*. 2010. Paper presented at 9th Annual Meeting of the EEFS International Conference, Athens, Greece.

[5] *Non ti insegno le regole, ma ti insegno come scoprire le regole da applicare per ottenere l'obiettivo desiderato*.

Tale approccio viene ad esempio utilizzato nella esposizione di questo articolo.

[6] Con collaboratore di intende una persona fisica indipendentemente dal tipo di relazione contrattuale che la stessa mantiene con l'organizzazione

[7] La WIPO (World Intellectual Property Organization) fornisce indicazioni sulle ricerche che nel mondo vengono effettuate dalle aziende per lo sviluppo di prodotti già esistenti, http://www.wipo.int/.

[8] European Union Agency for Network and Information Security (ENISA), https://www.enisa.europa.eu/activities/risk-management.

[9] Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, *RISK ANALYSIS Approfondimenti*, Linee Guida Iscom, http://www.isticom.it/documenti/news/linee_guida_rischi_due.pdf.

[10] National Institute of Standards and Technology (NIST), http://www.nist.gov/cyberframework/.

[11] Framework Nazionale per la Cyber Security, http://www.cybersecurityframework.it/.

[12] ENISA, *Pacchetto informativo per le PMI*, 2007, https://www.enisa.europa.eu/publications/information-package-for-smes-1.

[13] «La Comunicazione – Note Recensioni & Notizie», Rivista dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, 2015, http://www.isticom.it/index.php/divulgazione/la-rivista/rivista-2015.

[14] Il Codice della proprietà industriale, a norma dell'articolo 15 della legge 12 dicembre 2002, n. 273 regola la tutela di Marchi, Indicazioni Geografiche, Disegni e Modelli, Invenzioni, Modelli di Utilità, Topografie dei prodotti a Semiconduttori, Informazioni Segrete, Nuove Varietà Vegetali

[15] Codice della proprietà industriale, a norma dell'articolo 15 della legge 12 dicembre 2002, n. 273, Sezione VII Informazioni segrete, Art. 98. Oggetto della tutela:
1. Costituiscono oggetto di tutela le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni:
a) siano segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore;
b) abbiano valore economico in quanto segrete;
c) siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete.

[16] La Camera di Commercio di Bologna rende disponibili sul proprio sito i seguenti contratti-tipo: cessione di brevetto, cessione di diritti di priorità su brevetto, licenza di brevetto, cessione di marchio, licenza di marchio, cessione di design, licenza di design, licenza di know how e accordo di segretezza, http://www.bo.camcom.gov.it/regolazione-del-mercato/contratti-tipo/.