MARZO 2018

IL CAFFÈ DIGITALE

THE INNOVATION GROUP NEWSLETTER

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

ROSY ALAIA
Head of Retail Product Management, ING Group

INVESTMENT MANAGEMENT E WEALTH MANAGEMENT

quali strategie per la finanza digitale?

CYBER RISK MANAGEMENT 2018 SURVEY

quale sarà in futuro il ruolo del Chief Information Security Officer?

Verrà un giorno in cui QUALCUNO CI PAGHERÀ *per i* NOSTRI DATI?

Sommario

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Rosy ALAIA

Head of Retail Product Management, ING Group

ING

Pag. 4

L'EDITORIALE

VERRÀ UN GIORNO IN CUI QUALCUNO CI PAGHERÀ PER I NOSTRI DATI?

Ezio Viola | Managing Director, The Innovation Group

> In sè, il brevetto del braccialetto elettronico di Amazon non basta a dimostrare che l'azienda in futuro applicherà quell'idea, anche se Amazon non è nuova all'abitudine di testare direttamente le tecnologie che punta a introdurre sul mercato

Il recente caso del braccialetto digitale progettato da Amazon da utilizzare per facilitare il lavoro nei magazzini per rintracciare la merce ci deve fare riflettere su diversi elementi. Il primo è come sia facile nel nostro Paese scatenare polemiche mediatiche con forti strumentalizzazioni da parte di una moltitudine di soggetti che molte volte non sanno di cosa parlano.

I fatti sono i seguenti: questo braccialetto è un brevetto depositato da Amazon la cui richiesta iniziale del 2016 è stata approvata solo recentemente.

Spesso questi brevetti vengono depositati da aziende come Amazon anche solo per segnalare, ed eventualmente rivendicare in futuro, una proprietà. Il brevetto in sè, insomma, non basta a dimostrare che l'azienda applicherà quell'idea, anche se Amazon non è nuova all'abitudine di testare direttamente le tecnologie che punta a introdurre sul mercato.

Il braccialetto può potenzialmente essere utilizzato anche per controllare i dipendenti. Se riflettiamo, strumenti simili già esistono per monitorare la corretta applicazione delle misure di salute e sicurezza sul lavoro, migliorare l'efficienza del processo produttivo e supportare i dipendenti nello svolgimento di specifiche attività lavorative.

Volendo con gli smartphone usati da ogni dipendente, l'azienda potrebbe identificare dove sono in ogni momento e il fatto che, sempre teoricamente, si possa fare lo stesso con i braccialetti elettronici non cambia la sostanza. In realtà non è la tecnologia che deve essere bloccata ma è il suo uso a dover essere controllato per garantire i diritti delle persone. Inoltre l'utilizzo è regolato da normative e leggi che disciplinano, tra l'altro, la protezione dei dati personali e le tutele dei lavoratori, assegnando un ruolo centrale alla negoziazione tra azienda e rappresentanza sindacale.

Se mai Amazon volesse introdurre il braccialetto nei suoi magazzini in Italia, dovrà rispettare le norme e convincere i sindacati dell'opportunità della cosa.

Questo può piacere o no, ma è un dato di fatto su cui si è completamente sorvolato in questi giorni.

Questa storia è la tipica "fake news" che purtroppo dimostra l'esistenza di un pregiudizio di fondo contro l'innovazione nel nostro Paese dove la prima reazione a qualsiasi cambiamento sta diventando un "no" preventivo e obbligatorio.

L'altro aspetto su cui nessuno si è soffermato però è che il "braccialetto intelligente" è solo l'ultimo esempio di un processo e trend già consolidati: attraverso le tecnologie e i device che utilizziamo per accedere a internet noi tutti siamo delle sorgenti e dei generatori di dati fin dalla mattina

> I dati devono essere trattati come "fattore lavoro" da remunerare e non come capitale e la loro proprietà rimane a coloro che generano queste informazioni a meno che decidano di fornirli in cambio di un pagamento

quando accendiamo il nostro smartphone. Questi dati sono la più importante risorsa per le aziende internet, in primis i giganti del web, che tutti conosciamo.

Questo ruolo che ognuno di noi ha come creatore di dati nell'economia è ciò di cui dovremmo incominciare a pensare più a fondo.

Uno studio recente elaborato da diversi economisti e tecnologici[1] propone una tesi molto controversa ma da porre sul tavolo: noi siamo quindi tutti dei "lavoratori digitali", e in prospettiva possiamo diventare parte di una nuova classe sociale, che sta rendendo possibile la fortuna di aziende come Google, Facebook, Amazon etc.

Per garantire il progresso economico ed evitare una crisi occupazionale legata al progresso tecnologico, come molti osservatori paventano con l'utilizzo delle nuove tecnologie cognitive e di AI, dobbiamo incominciare ad essere più consapevoli di questo fatto e pensare di cambiare la relazione tra le aziende internet e i loro utilizzatori.

Infatti l'AI sta progredendo e può trasformare molti settori: le tecnologie di machine learning usate per imparare a guidare un'automobile o riconoscere un viso, hanno bisogno di imparare utilizzando una grande quantità di dati e le aziende, li ottengono gratis tutte le volte che interagiamo con loro o con i device con cui accediamo ai loro servizi, siano essi smartphone, wearable, personal assistant etc...

E' anche vero che siamo abituati ad usare molti servizi gratis da queste aziende e ne siamo contenti e soddisfatti.

Il valore dei dati va ad accrescere sempre di più il loro capitale e la loro capacità di investimento in nuovi servizi entrando così in nuovi settori adiacenti.

Queste aziende sono delle vere e proprie piattaforme digitali globali che costruiscono ecosistemi di cui sono gli orchestratori dominanti.

Lo studio afferma anche che uno dei problemi, per cui il contributo dell'AI è ancora scarso alla crescita della produttività, è dovuto anche ai limiti della qualità dei dati raccolti.

Le aziende sono alla ricerca di modalità per "forzare" gli utenti a fornire dati migliori a nessun costo aggiuntivo.

L'utilizzo della AI impatterà su molti lavori e ancor di più il valore economico generato dai dati andrà sempre di più alle aziende e poco ai lavoratori in forma di salari e stipendi.

Lo studio quindi ha una proposta radicale: i dati devono essere trattati come "fattore lavoro" da remunerare e non come capitale e la loro proprietà rimane a coloro che generano queste informazioni a meno che decidono di fornirli in cambio di un pagamento.

In tale modo i dati possono anche essere venduti a diverse aziende e non costituire più una barriera all'ingresso per le altre e il prezzo a cui sono venduti può essere anche finalizzato a migliorare la qualità dei dati raccolti. In questa prospettiva, generare i dati diventa anche una forma di occupazione in un mondo fortemente automatizzato.

Queste proposte sono si controverse e forse non realizzabili ma ci devono fare riflettere e dovrebbero stimolare una discussione sul ruolo dei dati e su cosa sia e potrebbe essere o diventare l'economia, oggi fortemente sbilanciata in termini di potere dovuto alla sua concentrazione in poche aziende.

Il potere contrattuale dei nuovi lavoratori di dati potrà esistere solo attraverso un'azione collettiva.

Questo ci mette di fronte alla natura condivisa del valore economico creato dai dati che dovrà essere distribuito anche in modo più equo, ma nessuno ne parla.

1. Should we Treat data ad Labor? Moving beyond "Free": Imanol Arrieta Ibarra, Leonard Goff, Diego Jimenez Hernandez, Jaron Lanier and Glen Weyl

QUESTO MESE ABBIAMO FATTO COLAZIONE CON

Prodotti e processi digitali in banca: il percorso di ING Group

Intervista di **Camilla Bellini** a

Rosy Alaia, Head of Retail Product Management, ING Group

Cosa significa trasformazione digitale in un'azienda già digital-oriented come ING?

Il tema degli investimenti in digitalizzazione di ING è sicuramente un aspetto molto significativo nella strategia complessiva della banca, elemento che esprime quanto oggi sia rilevante una strategia digitale per le imprese. Basti pensare che, nonostante il nostro approccio già fortemente digitale, continuiamo ad investire in digitale in modo molto significativo, a tutti i livelli.

Anche da un punto di vista organizzativo abbiamo, sia a livello di gruppo sia in Italia, un'unità dedicata alla digital transformation, che affianca la struttura organizzativa classica e supporta tutta l'azienda nello sviluppo di nuovi processi. D'altra parte, questa continua attenzione al tema "digitale" non riguarda solo la strategia e l'organizzazione dell'azienda, ma offre anche supporto operativo: pensate alla scelta di sviluppare e adottare la metodologia PACE, una metodologia innovativa che oggi consente di sviluppare alcune parti dei nostri prodotti e serviziin modalità agile.

A questo riguardo, occorre tenere presente che in Italia - a differenza di quanto già accade a livello di gruppo - l'organizzazione non è ancora strutturata internamente in modo agile, spesso soffrendo della contenuta diffusione di questo approccio tra i partner.

Questo comunque non ci impedisce già ad oggi di adottare l'approccio nello sviluppo di prodotti, come nel caso della recente soluzione di lending per le PMI.

Per quanto riguarda i prodotti ING, di cui la soluzione di lending appena citata è un esempio, che cosa state facendo in ambito trasformazione digitale?

L'anno scorso abbiamo lanciato un programma di revisione dei nostri prodotti nell'ambito prestiti, che tradizionalmente non erano prodotti di punta per ING, ma che oggi lo stanno diventando sempre più fronte degli attuali scenari di mercato e della necessità per le banche di diversificare la composizione del proprio conto economico.

Questo percorso di revisione - che noi chiamiamo Dream Process, in quanto finalizzato a sviluppare il migliore processo possibile sui prestiti personali - l'abbiamo iniziato proprio in modalità agile, che ci ha consentito di rilasciare sul mercato dei MVP (Minimum Viable Product) già a maggio dello scorso anno; nel giro di un anno completeremo la revisione di questo processo che sarà così fruibile in modalità "fully digital", dopo aver lanciato in questi mesi sul mercato rilasci successivi di pezzetti di processi per target di clientela, prima per i customer e poi per i prospect.

Tenete presente che con una modalità organizzativa waterfall questo sarebbe successo solo dopo un anno.

Questo lo avete fatto sulla parte prestiti personali. E per gli altri prodotti?

Quest'anno lavoreremo per la digitalizzazione di un altro prodotto molto importante, quello del mutuo.

Il mutuo per ING è un prodotto molto consolidato sul mercato italiano, anche online.

Anche da questo punto di vista la digitalizzazione del processo è ancora indietro rispetto ad altri prodotti come il conto corrente, prodotto su cui tutte le banche si sono già concentrate negli anni scorsi.

Ad esempio, Widiba è stata la prima a lanciare un prodotto di conto corrente con un processo interamente digitale.

Anche noi l'abbiamo lanciato l'anno scorso. In altre parole, abbiamo iniziato con i conti correnti, ci siamo spostati sui prestiti personali e ora stiamo lavorando sui mutui.Il mutuo è di per sé un prodotto tradizionale.

Sul mercato esistono già player che offrono processi parzialmente, magari ricorrendo alla firma digitale, ma alla fine c'è sempre molta carta coinvolta e l'ingaggio del cliente avviene sempre tramite call center o referente.

Attualmente ING sta quindi rivedendo l'intero processo in modo che sia fully digital, tranne ovviamente la fase dal notaio che per ora in Italia prevede ancora la presenza fisica delle parti coinvolte.

Pertanto, anche in questo ambito vediamo ampi spazi di miglioramento e in questo momento ci stiamo concentrando su questo.

Qual è il riscontro dei nuovi prodotti fully digital sul mercato italiano e in cosa vi differenziate rispetto agli altri player presenti?

Facendo riferimento in particolare all'offerta fully digital process nell'ambito prestiti personali - come già è avvenuto nell'ambito dei conti correnti digitali - i risultati sono stati più che tangibili.

Innanzitutto, da un punto di vista di soddisfazione del cliente nello sperimentare il prodotto: siamo partiti a fine maggio 2017 con un processo di 5 minuti per i clienti, che ora hanno la possibilità di richiedere un prestito, di avere l'autorizzazione contestualmente in pochi minuti e con la firma digitale il cliente di firmare attraverso un OTP addirittura fino a tre contratti, il contratto di firma digitale, il contratto di prestito e il contratto di assicurazione, nel caso decida di sottoscriverlo.

Noi riteniamo che la tecnologia fine a sé stessa non porti necessariamente valore aggiunto e quello che noi vogliamo fare è portare la tecnologia al servizio del cliente in una maniera innovativa e digitale per soddisfare i loro bisogni.

Faccio un esempio: noi siamo partiti nel 2016 con una survey sulla nostra customer base per capire perché i nostri clienti facessero poche richieste di prestiti; e abbiamo ottenuto insight molto interessanti, che facevano riferimento alla mancanza di semplicità e rapidità del servizio.

Da lì è nata l'idea di creare un processo interamente digitale per realizzare quelle che erano le richieste dei clienti.

Siamo quindi partiti da un processo che richiedeva giorni a uno che richiede minuti.

Questo ha ridotto drasticamente tutti i KPI e il customer effort del cliente: ad esempio, prima il cliente doveva inviare tutta una serie di documenti senza sapere se avrebbe ricevuto il prestito oppure no; ora abbiamo ribaltato completamente il processo, informando in primis il cliente se, se sulla base delle informazioni che ha fornito, potrà ricevere il prestito e solo successivamente gli chiediamo di inviare la documentazione in formato digitale.

> Noi riteniamo che la tecnologia fine a sé stessa non porti necessariamente valore aggiunto e quello che noi vogliamo fare è portare la tecnologia al servizio del cliente in una maniera innovativa e digitale per soddisfare i loro bisogni

Inoltre, anche i KPI operativi sono migliorati: noi avevamo dei tassi di rinuncia molto alti, che si sono ridotti dal 33% al 5%, proprio perché il cliente è molto più ingaggiato nel momento in cui gli forniamo una risposta.

La soddisfazione dei clienti rispetto a questo fully digital process emerge anche dai risultati relativi alla percentuale che utilizza questo processo: l'anno scorso era il 25% mentre quest'anno copre più del 50% della nostra produzione. E anche i risultati delle survey sono altissimi.

NUMERI
E MERCATI

Tra Hybrid Cloud, LinkedIn e piattaforme di Gaming, trimestre positivo per Microsoft: cosa ci aspetta nel 2018?

Camilla Bellini
Senior Analyst, The Innovation Group

A fine gennaio, Satya Nadella, CEO della Microsoft, affiancato dal team delle Investor Relation, ha presentato i risultati del secondo trimestre fiscale 2018: un trimestre certamente positivo, caratterizzato per lo più dal segno più e dalla conferma, se non dal superamento, delle attese. Cosa ha guidato questo trend?

In primis il cloud, ed in particolare Azure, con una crescita di ricavi pari al 98%; il vantaggio competitivo in termini di capacità di gestione di workflow sia tradizionali sia innovativi (ad esempio per l'IoT) ha permesso all'azienda di registrare una crescita nei ricavi per server product e servizi cloud del 18%. È quello che Nadella ha chiamato Intelligent Cloud, segmento che ammonta a 7,8 miliardi di dollari.

Cresce anche l'ambito del Gaming, con Microsoft che sembra sempre più voler creare un vero e proprio ecosistema multi-device fondato sulla propria tecnologia.

Nello specifico, nel trimestre in questione Microsoft ha assistito ad una forte performance nelle vendite delle console Xbox One X e Xbox One S; ha inoltre portato avanti una strategia di aumento del valore degli abbonamenti Xbox (Xbox Game Pass), rilasciando contenuti di gioco esclusivi contemporaneamente alla versione globale; così come l'acquisizione di PlayFab, azienda che fornisce tool cloud- based per i game developer e che consente lo sviluppo multipiattaforma, che permette all'azienda di estendere l'investimento in Azure fornendo una piattaforma cloud per l'industria del gaming. Nel complesso i ricavi di questo settore sono cresciuti nel trimestre del 8%, guidati principalmente dalla crescita dell'hardware del 14%, grazie al lancio della nuova console nel corso del trimestre.

Altra area di crescita da citare è quella legata a LinkedIn, che a livello di azienda contribuisce a circa 4 punti nella crescita dei ricavi, con una crescita anno dopo anno dei livelli di engagement della piattaforma: crescono infatti le conversazioni attraverso la piattaforma, oltre il 60% anno su anno.

In particolare, questa crescita della community su Linkedin guida una significativa crescita nella domanda di contenuti sponsorizzati nell'ambito Marketing e HR. A fronte di questa crescita nella domanda, l'azienda sta aumentando il portfolio dei servizi offerti, ad esempio nell'ambito del Career Advice.

Se queste sono alcune delle aree di crescita di Microsoft, cosa ci attende nel prossimo trimestre?

A fronte di un mercato IT complessivamente in crescita e la crescita della domanda per servizi di hybrid cloud, l'azienda si attende un rafforzamento del business commerciale, della base installata e della base in scadenza.

Continua parallelamente il focus sull'AI, su Cortana e sulla Mixed Reality, elementi che sempre più andranno ad arricchire l'offerta Microsoft nei prossimi trimestri.

LA TRASFORMAZIONE DIGITALE

Sistemi Transazionali e Blockchain: riflessioni

Vincenzo D'Appollonio
Partner, The Innovation Group

Oggi parlare di Blockchain e Bitcoin è di estrema attualità, in diverse prospettive: informatiche, economiche, finanziarie, sociali.

Per molti la Blockchain rappresenta una sorta di Internet delle Transazioni, per altri la transazione Bitcoin/Blockchain può rappresentare la Internet del Valore.

Alcune 'keyword' informatiche usate nelle diverse trattazioni mi hanno stimolato riflessioni sulle origini di questi concetti, sulla base di esperienze del mio passato.

Agli inizi degli anni ottanta in Olivetti partì un progetto di sviluppo 'interno' di un Sistema Transazionale basato su un modello 'Client-Server', integrato con un Data Base basato su un innovativo 'Information Model reticolare-concatenato': mi assegnarono la responsabilità del Progetto, che venne poi realizzato dal mio Gruppo, distribuito tra i Laboratori dell'Olivetti Advanced Technology Center di Cupertino in Silicon Valley, e dell'Olivetti R&D di Trezzano S/N; nel 1985 rilasciammo il prodotto 'MTX - Multisite Transactional System on Unix', integrato con il prodotto 'C-DB Chained Data Base'.

MTX era un Sistema Transazionale dedicato all'attività di elaborazione dei dati di tipo gestionale, caratterizzato quindi da più utenti Client che accedono concorrentemente a dati condivisi mediante procedure predefinite, le cosiddette Transazioni, cioè una sequenza raggruppata (...Blocco...) di operazioni elementari (...Transaction Unit...) che, se eseguita in modo corretto, produceva una variazione nella base di dati C-DB.

MTX garantiva che, preso un qualsiasi elemento (TU) di tale raggruppamento, la sua esecuzione dovesse avvenire solamente al momento in cui vi fosse la possibilità di poter portare a termine l'esecuzione di ogni altro elemento dell'insieme Transazione (...validazione...); banalmente il meccanismo doveva essere tale da far sembrare, all'esterno della Transazione, che tali operazioni elementari (TU) fossero svolte in contemporanea (azione di Commit). In caso di successo, il risultato delle operazioni doveva essere permanente o persistente, mentre in caso di insuccesso si doveva tornare allo stato precedente all'inizio della Transazione (caratteristica di Revocabilità, con procedure di rollback/undo applicate al... Registro/LOG delleTransazioni...associate ad una ...Marca Temporale...).

MTX garantiva dunque alle Transazioni che operavano su C-DB le cosiddette proprietà ACID, acronimo di Atomicity (tutte o nessuna delle operazioni che vengono raggruppate in una transazione devono andare a buon fine); Consistency (il completamento della transazione deve lasciare il sistema in uno stato coerente); Isolation (ogni transazione non deve avere nessun effetto sulle altre); Durability (il risultato di una transazione deve essere persistente come l'entità nella quale la transazione ha avuto un Commit). La reale innovazione di MTX consisteva nella

gestione delle Transazioni 'ACID' in ambiente Distribuito-Multisito Client/Server (...Nodi...), in un momento in cui i Sistemi Transazionali di riferimento (CICS, IMS/DB-DC) erano tutti realizzati sul modello 'main-frame'.

Nel 2009 un anonimo inventore, noto con lo pseudonimo di Satoshi Nakamoto, pubblica la sua idea di criptovaluta Bitcoin basata su un modello di Sistema Transazionale ACID per operare in Internet, che dà il nome a una nuova piattaforma tecnologica: la Blockchain, grande database distribuito per la gestione di transazioni crittografate su una rete decentralizzata di tipo peer-to-peer, grazie a un processo che unisce sistemi distribuiti, crittografia avanzata e teoria dei giochi (puzzle crittografici).

Pensando alle componenti basilari della Blockchain, ho ritrovato, in una sorta di 'deja-vu',molti concetti sviluppati in MTX, quali Nodo (i partecipanti alla Blockchain costituiti fisicamente dai Server di ciascun partecipante); Transazione (costituita dai dati che rappresentano i valori oggetto di "scambio" e che necessitano di essere validate); Blocco (rappresentato dal raggruppamento di un insieme di transazioni/TU che sono unite per essere verificate, approvate e poi archiviate dai Nodi); Processo di Validazione/gestione del Consenso in Rete, Registro/Ledger delle Transazioni distribuito (i Distributed Ledger vengono aggiornati solo dopo aver ottenuto il Consenso, ogni nodo viene aggiornato con l'ultima versione di ogni singola operazione di ciascun partecipante, ogni operazione rimane poi in modo indelebile e immutabile su ogni singolo Nodo), Marche Temporali/Time stamp; Miner (i veri Client della Blockchain per "l'estrazione dei Bitcoin").

Riflessione finale di un 'ex' informatico: nihil sub sole novi... Purtroppo il mio MTX non generava Bitcoin...

NEL 2009 UN ANONIMO INVENTORE PUBBLICA LA SUA IDEA DI CRIPTOVALUTA BITCOIN

LA TRASFORMAZIONE DIGITALE

IT e digitale nelle aziende italiane: dove sta l'innovazione?

Camilla Bellini
Senior Analyst, The Innovation Group

Recentemente abbiamo concluso l'analisi dei risultati di una survey che conduciamo ogni anno sui trend di adozione delle tecnolgoie IT e digitali nelle aziende italiane: per sapere cosa sta accadendo nei dipartimenti IT, abbiamo intervistato 113 aziende. Ecco cosa ci hanno raccontato.

Oggi è indubbio che esiste un gap tra la "propaganda" marketing dei tech vendor e i toni trionfalistici/ catastrofici dei mass media sul ruolo e la diffusione del digitale, anche in Italia. Sembra tutto digitale, città connesse che si muovono con noi, filiere intelligenti in grado di ottimizzare la produzione, macchinari intelligenti che invadono fabbriche e software che trasformano uffici.

Forse però la realtà è leggermente diversa, o meglio, più complessa. La tecnologia infatti, e con lei i processi di trasformazione digitale, non può essere ready-made, non si può acquistare a catalogo confidando che questo basti.

Il digitale è un percorso, spesso lungo e faticoso, che si compone di diversi elementi, tecnici, organizzativi e manageriali, e che indubbiamente non può limitarsi all'adozione della tecnologia.

Il digitale è un percorso, spesso lungo e faticoso, che si compone di diversi elementi, tecnici, organizzativi e manageriali, e che non può limitarsi all'adozione della tecnologia.

Ed è proprio questo che emerge dall'analisi: nel complesso, quello descritto è uno stato dell'IT in Italia tendenzialmente tradizionale, in cui certo a volte si intravedono degli slanci verso nuove tecnologie e nuovi modelli, ma per lo più ci si confronta con le necessità del quotidiano, di mantenimento e miglioramento dell'esistente, senza che si verifichino vere e proprie discontinuità rispetto a quello che è tradizionalmente il ruolo dell'IT in azienda.

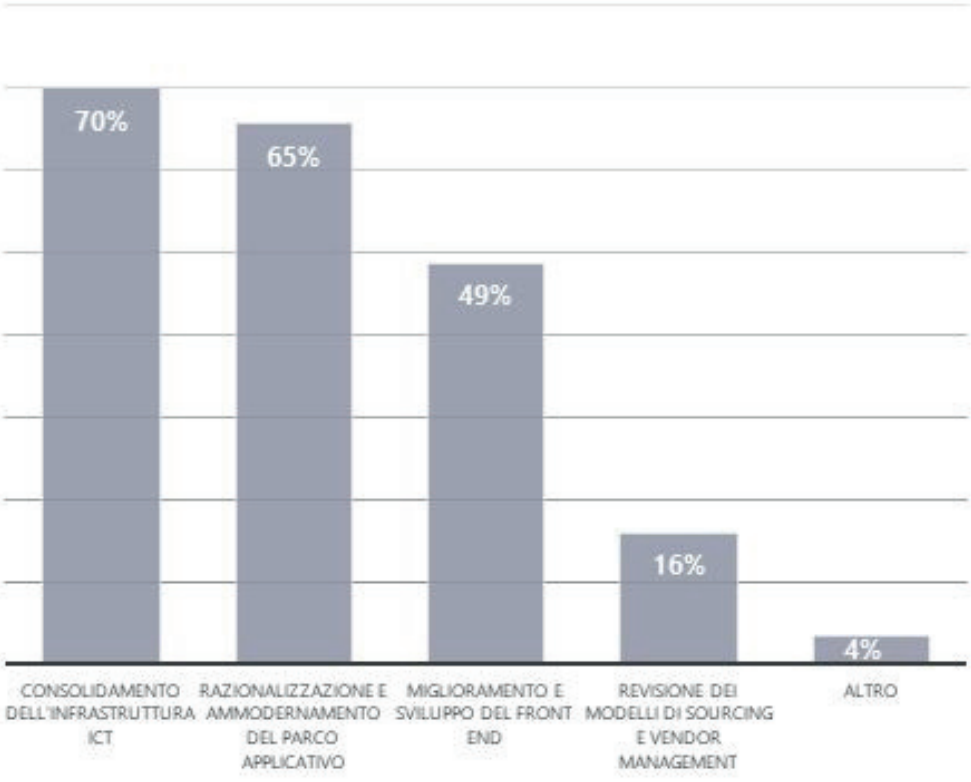
Basti pensare alle iniziative che oggi la maggior parte delle aziende stanno sviluppando, orientate soprattutto al consolidamento dell'infrastruttura ICT (il 70% dei rispondenti) e alla razionalizzazione e ammodernamento del parco applicativo (65%). Si investe anche, ma l'attenzione è rivolta soprattutto agli applicativi (nuovi o in sostituzione) nell'ambito CRM e ERP. Ancora una volta, non si tratta di salti quantici verso le tecnologie del futuro, ma un percorso a piccoli passi che punta a innovare e rinnovare la tecnologia in azienda.

D'altra parte, l'IT continua ad avere un ruolo orientato allo sviluppo di nuove funzionalità e all'aggiornamento di sistemi e applicazioni, accentrando ancora la maggioranza della spesa ICT dell'azienda: il 64% delle aziende dichiara infatti che meno del 10% della spesa IT è effettuata senza il coinvolgimento della funzione, una percentuale relativamente contenuta, che segnala una ancora contenuta diffusione del fenomeno della Shadow IT nella maggior parte delle aziende intervistate.

Interessanti anche i risultati relativi alla diffusione del cloud computing, dal momento che dalla rilevazione emerge come le aziende mediamente impieghino un quarto della spesa complessiva per hardware, software e middleware in risorse cloud, mentre gli applicativi SaaS più diffusi sembrano essere le soluzioni in ambito collaboration e produttività.

Un piccolo focus poi sull'attività di gestione e analisi dati in azienda, tema oggi particolarmente interessante anche a fronte della diffusione delle cosiddette data-driven enterprise: dall'analisi emerge come quest'attività spesso abbian ancora un taglio tradizionale, orientata soprattutto all'analisi interna dei "core data" (soprattutto in ambito finanziario e commerciale), con strumenti quali i fogli elettronici e BI.

Quali sono le principali iniziative che la funzione IT della sua azienda sta sviluppando?



BANCHE E FINTECH

Investment Management e Wealth Management: quali strategie per la finanza digitale?

Ezio Viola
Managing Director, The Innovation Group

Lo scorso 22 febbraio, presso il Fintech District di Milano, abbiamo organizzato una tavola rotonda sul tema della trasformazione digitale nell'ambito dell'Investment & Wealth Management, ambito che spesso viene marginalizzato nel più ampio dibattito sul digitale nel retail banking. Grazie alla collaborazione con Excellence Consulting nel corso dell'incontro abbiamo raccontato alle aziende e ai consulenti finanziari presenti qual è il potenziale della tecnologia nella gestione dei patrimoni e quali sono le sfide specifiche che i diversi player devono affrontare in un nuovo contesto più digital-oriented.

Di seguito, riportiamo alcune dei trend emersi nel corso della discussione.

Come si caratterizza oggi il mercato del risparmio gestito in Italia?

In primo luogo, è indubbio che il 2018 sarà un anno di rinnovamento per il sistema finanziario – globale e italiano – sia per la concretizzazione dei macro-trend che caratterizzano il settore sia per l'affermarsi di nuove normative (MFID2, PSD2, GDPR e IDD): nello specifico del settore dell'asset and wealth management, le evoluzioni in questi ambiti porteranno indubbiamente allo sviluppo di nuovi prodotti e servizi e, conseguentemente, dei modelli di business e dello scenario competitivo nel panorama del risparmio gestito.

Negli ultimi 26 anni il mercato ha registrato un trend di crescita del risparmio gestito, con un'allocazione delle dei risparmi famigliari del 35%, valore allineato a quello degli altri paesi nostri peer. D'altra parte, resta ancora una quota rilevante di asset sotto forma di liquidità.

Il mercato ha assistito negli ultimi anni ad un'apertura a diverse tipologie di player, come ad esempi i family office, i consulenti indipendenti e i robo-advisor, che oggi si affiancano alle banche commerciali, alle banche private e alle reti di consulenti. In particolare, le reti di consulenti nel mercato stanno crescendo a discapito delle banche tradizionali: si sta assistendo ad una crescita del ruolo delle reti, con un aumento della similitudine con il mercato americano, dove tra il 40-50% del mercato è coperto dalle reti di consulenze.

Quali criticità e strategie per asset manager e banche?

Oggi sono quattro le principali criticità che gli asset manager devono affrontare: in primo luogo il tema della comprensione dei margini, che riducono la redditività del mercato; la conseguente concentrazione del mercato, dove solo i player in grado di scalare e fare leva sulle economie di scala restano sul mercato; il tema del digital divide, non solo per quanto riguarda i clienti ma anche all'interno stesso dei professionisti del settore; e infine il tema delle nuove competenze necessarie per far fronte alle nuove esigenze e ai trend evolutivi del mercato.

Per far fronte a queste criticità gli asset manager

possono avvalersi di diversi modelli strategici, distinti tra strategie di breve e di medio periodo, come ben ha raccontato durante l'incontro Maurizio Primanni, President & Founder di Excellence Consulting.

Quali azioni di breve e medio periodo per gli asset manager?

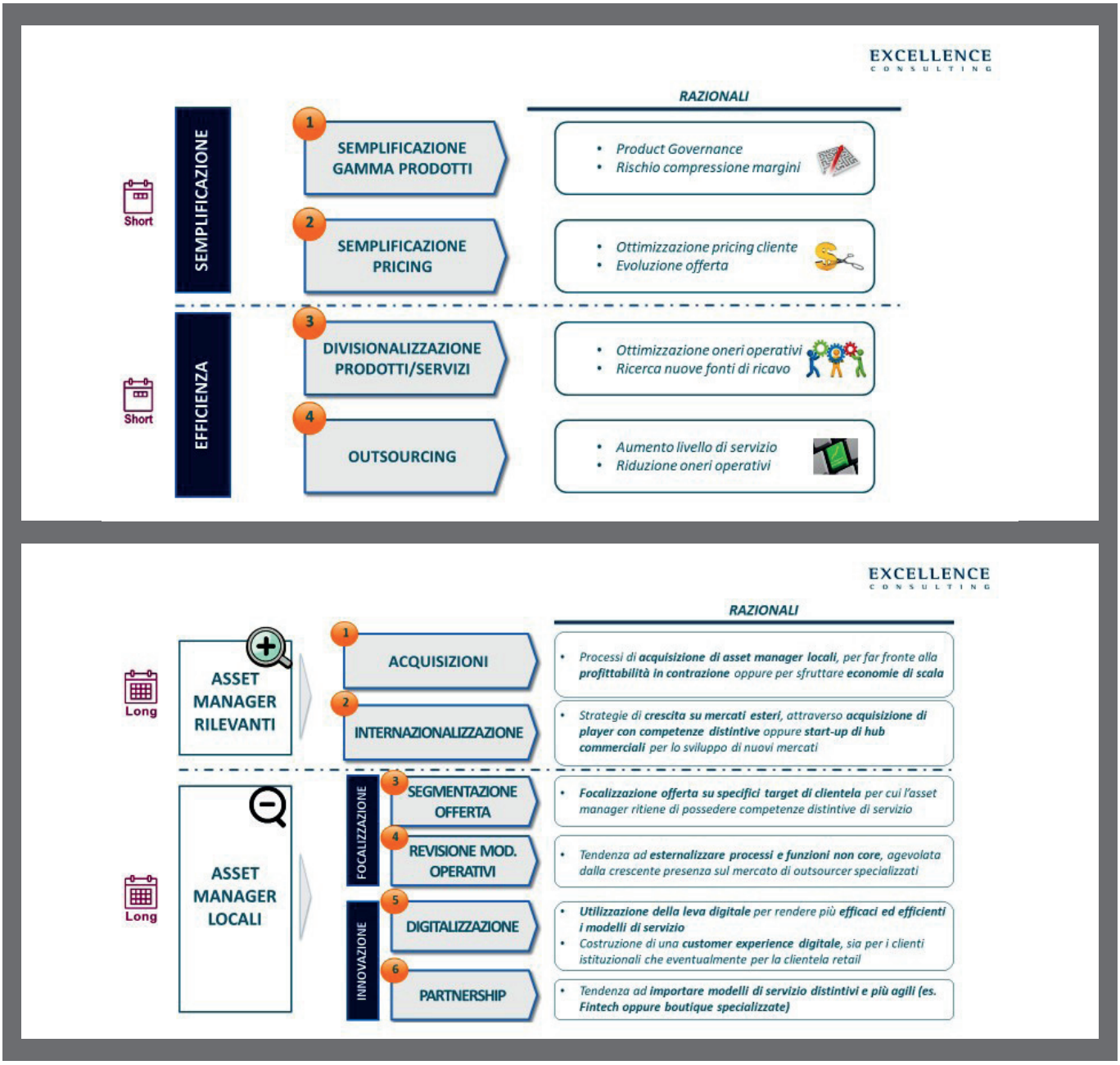
Nel breve periodo un asset manager può scegliere due strade: da un lato, la semplificazione dei cataloghi e delle logiche / strutture di pricing; dall'altro, l'aumento dell'efficienza tramite la divisionalizzazione dei prodotti / servizi o l'outsourcing.

Per quanto riguarda invece il medio - lungo periodo, le strategie si differenziano sulla base del livello di rilevanza degli asset manager: gli asset manager rilevanti possono infatti ricorrere a strategie di internazionalizzazione e acquisizione, mentre gli asset manager locali a strategie di focalizzazione o d'innovazione.

Per i player minori la focalizzazione può avvenire tramite una migliore segmentazione della clientela, grazie ad un'attività di marketing a monte; l'innovazione passa invece dalla trasformazione digitale, sia sotto forma di mobile e social marketing, sia di strategie di content management online, sia di creazione di community digitali che ad esempio fanno leva sull'affinity, fino addirittura alla creazione di piattaforme per fornire direttamente servizi ai propri clienti (robo-advisor).

Qualche esempio in Italia?

In Italia, ad esempio, Generali ha sviluppato un nuovo modello multi-boutique per rafforzare la propria presenza nel mercato: ha in altre parole adottato una strategia di medio - lungo periodo orientata alle acquisizioni; Intesa Sanpaolo, invece, parla di sviluppo di asset management attraverso l'internazionalizzazione, sia su mercati storici, sia su mercati potenziali: in questo caso la strategia adottata è quella dell'internazionalizzazione.



DIRITTO ICT
IN PILLOLE

Questo braccialetto non s'ha da fare!

Yuri Monti
Consultant, Colin & Partners

Tra rispetto della normativa in materia di protezione dei dati personali e tutela dei lavoratori, a tenere banco negli ultimi tempi è la spinosa questione circa il possibile utilizzo di un braccialetto elettronico (al momento solamente oggetto di brevetto) da parte degli operatori all'interno degli stabilimenti italiani di Amazon. In particolare, il device ideato dal colosso americano sarebbe volto a ottimizzare il lavoro dei dipendenti: esso infatti sarebbe una delle componenti di un sistema di trasponder, in grado di individuare la merce presente nei magazzini a fronte degli ordini, comunicati proprio al braccialetto. In altre parole, una ricerca pressoché automatizzata con conseguenti riduzioni di tempi nella gestione del prodotto; la tracciatura dei movimenti è parte integrante di tale meccanismo e, inevitabilmente, crea una situazione di potenziale controllo sulle attività dei lavoratori che indossano la strumentazione. Gli schieramenti si sono ben presto formati attorno alla prospettiva di utilizzo del braccialetto, con una pluralità di voci di dissenso proveniente dal versante politico, sindacale ed istituzionale.

In tal senso è intervenuto anche Antonello Soro, attuale presidente dell'Autorità garante della privacy, affermando la piena incompatibilità tra il ricorso al braccialetto e "l'ordinamento in materia di protezione dati, non solo in Italia ma anche in Europa". Meno "rigidi" nella condanna, invece, sembrano essere i direttori italiani del personale, che in larga maggioranza vedono nella famigerata

LO STRUMENTO DI AMAZON
È COMPATIBILE CON NOSTRO ORDINAMENTO?

strumentazione un'opportunità di incremento della produttività, laddove inquadrata in un corretto contesto normativo che eviti qualsiasi forma di abuso. Riconducendo il dibattito ad una valutazione di tipo strettamente giuridico, la questione di fondo rimane però una soltanto: può lo strumento dell'azienda di Jeff Bezos essere compatibile con le regole del nostro ordinamento?

La normativa direttamente chiamata in causa è ovviamente quella della L. 300/70, meglio nota come "Statuto dei Lavoratori".

L'art. 4 di tale Legge rappresenta il fondamentale punto di contatto tra salvaguardie giuslavoristi e protezione dei dati personali dei lavoratori, disciplinando proprio il ricorso a "impianti audiovisivi e altri strumenti" da cui possa derivare un controllo dei lavoratori nell'esecuzione della prestazione professionale. E proprio l'articolo 4 ha rappresentato uno dei campi di maggior intervento della riforma apportata dal c.d. "Jobs Act", che ne ha ridisegnato la struttura e modificato i tratti essenziali:

Nella precedente formulazione erano previsti:

- Un espresso e diretto divieto dell'uso di "impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori";
- Il permesso al ricorso di impianti ed apparecchiature da cui derivi un potenziale controllo dei lavoratori, purché accompagnato da specifico accordo sindacale o da espressa autorizzazione dell'Ispettorato del lavoro competente.

Nella nuova formulazione, viene ora previsto:

- Il solo permesso al ricorso di impianti ed apparecchiature da cui derivi un potenziale controllo dei lavoratori previo accordo sindacale o autorizzazione della Direzione territoriale del lavoro, con il venire del divieto generale;
- L'eventualità, al nuovo comma 2, di disapplicare tale regime condizionato a fronte del ricorso a "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze".

Quest'ultima previsione è sicuramente la più rilevante nell'ottica del braccialetto elettronico: prefigurando tale strumento come utile a rendere la prestazione lavorativa – così come suggerito dal tenore della documentazione brevettuale –, si sembra ricadere nell'ipotesi di esclusione prevista al già citato comma 2.

Definire a pieno la natura del dispositivo di casa Amazon non è dunque mero esercizio finalizzato ad una querelle dai contorni indubbiamente anche "politici", ma diventa elemento fondamentale per poter garantire l'applicabilità della normativa in materia e l'effettiva difesa dei diritti dei soggetti coinvolti.

L'art. 4 dello "Statuto dei Lavoratori" rappresenta il fondamentale punto di contatto tra salvaguardie giuslavoristi e protezione dei dati personali dei lavoratori, disciplinando proprio il ricorso a "impianti audiovisivi e altri strumenti" da cui possa derivare un controllo dei lavoratori nell'esecuzione della prestazione professionale

CYBERSEC
E DINTORNI

Quale sarà in futuro il ruolo del Chief Information Security Officer

Elena Vaciago
Associate Research Manager, The Innovation Group

Presentiamo di seguito un'anticipazione dei risultati della Cyber Risk Management 2018 survey, indagine svolta in Italia da The Innovation Group, tra dicembre 2017 e gennaio 2018, su un campione di 88 aziende medio grandi dei diversi settori.

Sono commentate in particolare le risposte ottenute sul tema delle problematiche oggi più sentite dai CISO/Security Manager italiani.

I risultati completi della Cyber Risk Management 2018 survey saranno oggetto di presentazione e discussione durante il Cybersecurity Summit 2018, organizzato da The Innovation Group il prossimo 21 marzo 2018 a Roma.

Oggi solo una minoranza di aziende italiane si è dotata di una figura con responsabilità specifica sugli aspetti di sicurezza ICT, di un Security manager o di un Chief Information Security Officer (CISO). In prospettiva però questo ruolo sarà sempre più diffuso, via via che il tema della protezione in chiave digitale sarà considerato strategico e fondamentale per la stessa sostenibilità del business.

Quale sarà in futuro il ruolo del Chief Information Security Officer?

Guardando alle best practices internazionali, si tratta di solito di un Executive di livello elevato, che riporta direttamente ai livelli apicali dell'organizzazione, guidando team cross funzionali e rispondendo su qual è, in ogni momento, l'esposizione dell'azienda ai rischi cyber. In molte grandi aziende, il CISO è oggi una figura che collabora strettamente con la corporate governance e che assicura una crescita costante del business garantendo che il rischio da lui presidiato sia gestito entro limiti di "risk appetite" accettabile.

In molte aziende in cui invece l'approccio ai temi della cybersecurity è rimasto di tipo tradizionale, il CISO deve farsi carico di promuovere una cultura più allineata alle nuove sfide e ai nuovi rischi; interagisce di frequente con il top management / il Board e siede al tavolo dove sono decisi i nuovi prodotti /servizi o la strategia dell'organizzazione.

È inoltre responsabile della gestione di un team di persone che operativamente garantiranno la disponibilità dei sistemi e l'integrità e la riservatezza delle informazioni.

Poiché disporre di uno staff di per la cybersecurity è sempre più complicato, vista la scarsa disponibilità di queste competenze sul mercato, il CISO dovrà farsi carico della crescita delle sue risorse, tramite programmi di training, volti anche ad aumentare contemporaneamente la retention dello staff.

Se questo è a grandi linee "quello che il CISO dovrebbe essere e fare", vediamo in base alle risposte ottenute dalla Cyber Risk Management 2018 survey qual è oggi la situazione con riferimento alle problematiche di un Security Manager/CISO italiano.

Consideriamo quindi le principali sfide e le problematiche più urgenti di un CISO/Security Manager partendo da un insieme di aziende che dimostra di essere già matura su questi temi, avendo già piani consolidati ed estesi per la cybersecurity.

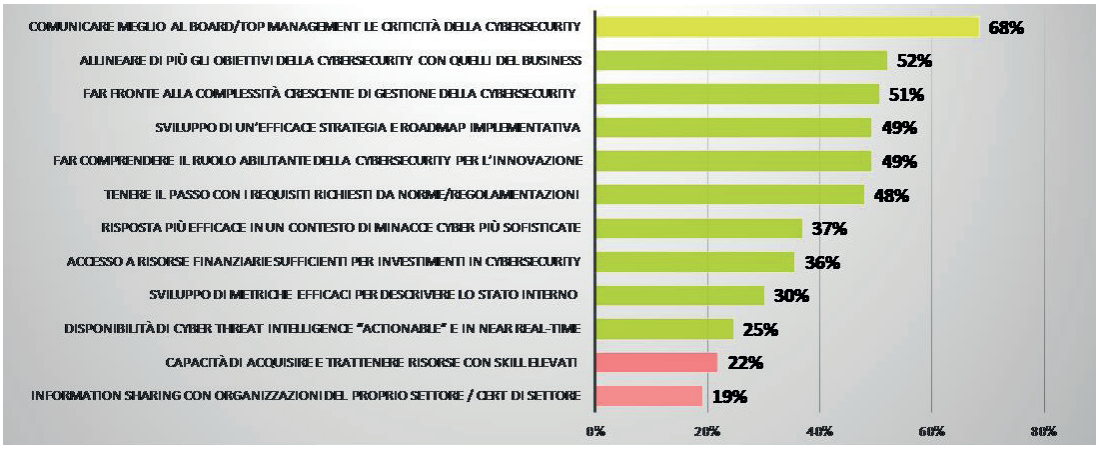
Come mostra la figura successiva, gli aspetti critici sono numerosi.

Analizzando le prime due risposte ("Comunicare meglio al Board" e "Allineare meglio cybersecurity al business") vediamo che le criticità maggiori risiedono non tanto nell'area della Security, quanto piuttosto nella sua relazione con il resto dell'organizzazione che le sta intorno.

sostanzialmente di impostare una corretta governance. Ulteriori considerazioni sulle problematiche incontrate oggi da un Security Manager, riprendendo i risultati della nostra survey, sono inoltre:

- Difficoltà nel far fronte alla continua crescita di processi e controlli, a una complessità crescente per la gestione della cybersecurity. Questo problema è molto sentito, si posiziona al terzo posto, con oltre la metà dei rispondenti (51% delle risposte), ed è evidente che non farà altro che peggiorare in futuro, via via che le aziende si esporranno in nuovi ambiti dell'innovazione digitale.

Quali sono oggi le principali sfide per il CISO



Il primo problema di un CISO (68% delle risposte) è quindi come rendere più partecipe, come ingaggiare meglio il top management/il Board dell'azienda comunicandogli nel modo più efficace possibile le criticità della cybersecurity che lui vede, ma che il resto dell'organizzazione non conosce o non capisce. Il secondo problema (indicato dal 52% dei rispondenti) è invece allineare meglio gli obiettivi della cybersecurity a quelli del business.

Molti responsabili della security oggi si pongono infatti il problema su quale sia il livello di sicurezza ideale per la propria realtà.

Se la sicurezza sarà eccessivamente pesante, comporterà inevitabilmente una serie di misure pesanti, per i dipendenti, per i clienti, misure che potrebbero peggiorare la user experience e condizionare la competitività dei prodotti o dei servizi dell'azienda. Proibire la navigazione o l'utilizzo di device mobile ai dipendenti non favorisce di certo la crescita e l'innovazione in azienda: se i sistemi sono bloccati, le informazioni critiche messe sotto custodia, se devo imporre procedure e training ogni qualvolta incremento le misure di sicurezza, è probabile che le ricadute in termini di produttività e agilità del business saranno pesanti. Come bilanciare quindi al meglio sicurezza e obiettivi del business?

In ogni realtà in cui ci si pone questo problema le soluzioni sono spesso diverse: si tratta

È un tema legato alla mancanza di competenze e risorse per la security, che può essere affrontato soltanto se si lavora in un'ottica di PROGRESSIVA AUTOMAZIONE di un numero sempre maggiore di task, in modo da lasciare il tempo allo staff di concentrarsi sulle attività più critiche o a maggiore valore aggiunto.

Ancora oggi moltissime attività IT (pensiamo al patching, all'e-commerce, alla gestione del cliente), sono svolte in modo manuale.

Oltre a comportare maggiori rischi di errore, le attività manuali sono un collo di bottiglia: ad esempio, quando viene completato un vulnerability scan, passa moltissimo tempo prima che tutti i problemi trovati ricevano il rispettivo fix – un tempo che gli attaccanti conoscono bene, perché sfruttano queste "finestre temporali" per completare con successo le proprie azioni.

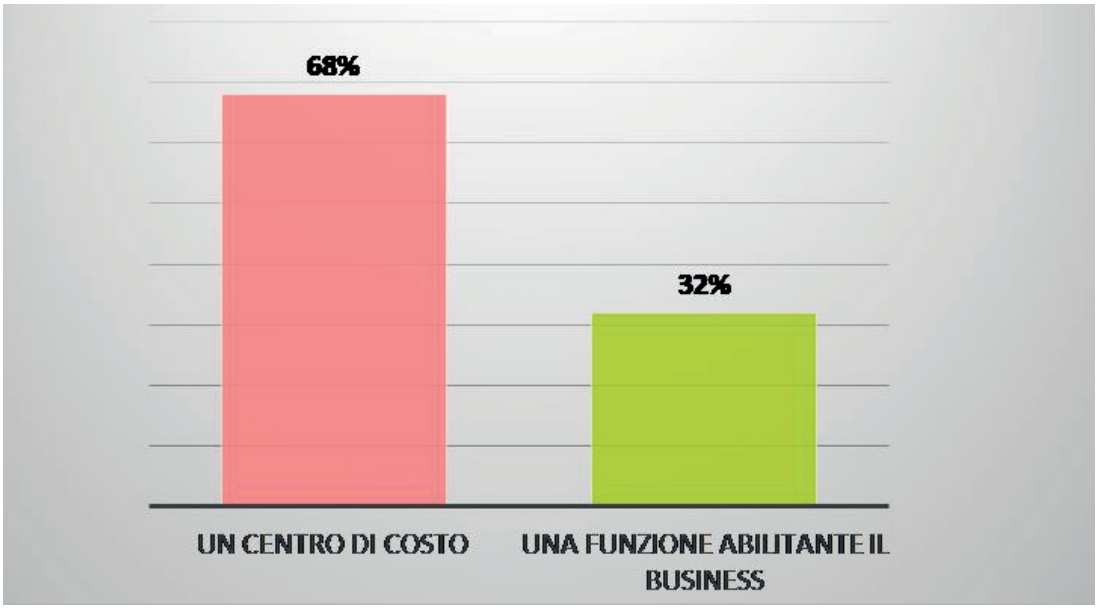
- "Sviluppo di un'efficace strategia e roadmap implementativa" (49% delle risposte); "Risposta più efficace in un contesto di minacce cyber più sofisticate" (37%) e "Sviluppo di metriche efficaci per descrivere lo stato interno" (30%).
  Queste tre risposte vanno attribuite alla più ampia necessità, che tutti i responsabili hanno, di dotarsi di un disegno e di un PROGRAMMA EFFICACE DI CYBER RISK MANAGEMENT. Fanno riferimento alla difficoltà che soprattutto

le aziende di alcuni settori (meno toccati rispetto ad altri da regolamentazioni e da iniziative di settore) hanno nell'individuare i processi, le metodologie e le best practice specifiche per la propria realtà. Un supporto andrebbe previsto per queste realtà, e dovrebbe arrivare da un maggiore coinvolgimento delle istituzioni a livello nazionale su queste tematiche, dall'istituzioni di CERT specifici per i diversi settori.

- "Tenere il passo con i requisiti richiesti da norme/regolamentazioni" è avvertito come una priorità del Security Manager dal 48% delle aziende – conseguenza di un numero sempre maggiore di norme che hanno e avranno impatto sulla cybersecurity.
- Un numero altrettanto elevato di aziende (49%) ritiene anche che "Far comprendere il ruolo abilitante della cybersecurity per l'innovazione" sia oggi un compito critico del CISO.
- L'accesso a risorse finanziarie sufficienti per investimenti in cybersecurity è un problema solo per circa un terzo delle aziende intervistate – segnale che dove oggi l'approccio al cyber risk management è già avanzato, l'accesso ai budget non è più il primo problema di un security manager.
- "Disponibilità di cyber threat intelligence "actionable" e in near real-time" è un problema prioritario solo per un'azienda su 4.
- "Information sharing con organizzazioni del proprio settore / CERT di settore" è invece indicato come un aspetto prioritario solo da una minoranza di organizzazioni. Segnale che su questi aspetti solo poche aziende sono oggi sufficientemente pronte, li considerano ancora una sfida per il medio lungo termine, non di immediata rilevanza.

Il problema è che per ottenere una risposta a molte delle problematiche che i Security Manager e i CISO oggi incontrano (dal miglior collegamento con il top management e con la strategia aziendale, all'evoluzione della sicurezza verso una funzione perfettamente allineata con i reali bisogni dell'azienda) serve innanzi tutto un CAMBIO DI PASSO su un aspetto fondamentale: la CULTURA DELLA SICUREZZA nella propria organizzazione e fuori da essa. Fintanto che – come mostra la seguente figura – la sicurezza informatica sarà percepita più come un costo che non come un elemento che abilita l'innovazione e la trasformazione del business in chiave digitale, sarà molto difficile trovare una soluzione a tutti i problemi che oggi ancora limitano il potenziale valore della sicurezza.

In generale, l'ICT è vista nella vostra azienda come:



VOCI
DAL MERCATO

La sfida della Trasformazione Digitale per il nuovo CISO

Intervista di **Elena Vaciago** a
Francesco Di Maio, Head Security Department, ENAV

Quali sono oggi le principali sfide con cui deve confrontarsi il Responsabile della sicurezza informatica, e come sta evolvendo il suo ruolo, con l'obiettivo di favorire la strategia di digitalizzazione scelta dalla sua azienda?

Ne abbiamo parlato con chi vive quotidianamente queste problematiche e che può quindi indicare la direzione giusta da intraprendere, ossia, direttamente con Francesco Di Maio, Head Security Department, ENAV e parte dell'Advisory Board del Programma 2018 sulla Cybersecurity di The Innovation Group.

Quali sono oggi le problematiche più avvertite dai Chief Information Security Officer?

Il principale tema con cui deve confrontarsi oggi un Responsabile della sicurezza informatica è l'aspetto culturale, la necessità di diffondere maggiore consapevolezza su questi rischi.

Sappiamo infatti che la principale debolezza di un'architettura di sicurezza rimane l'elemento umano: è quindi necessario far crescere l'awareness e avere una maggiore cultura.

I modi per farlo sono diversi, e alcuni risultano essere più efficaci della formazione tradizionale, introducendo ad esempio aspetti legati alla gamification.

Secondo problema: riuscire a collegare l'intera supply chain sui temi della cybersecurity. Tutti i fornitori di beni e servizi esterni devono possibilmente adeguarsi al modello interno di gestione: bisogna avere un modello di sicurezza basato sul trust, sulla fiducia da parte di tutti delle capacità altrui.

Essendo l'ENAV un'infrastruttura critica, ci aspettiamo da tutti i nostri fornitori un'elevata professionalità nell'erogazione dei rispettivi servizi.

Anche i produttori di software dovrebbe ro dotarsi di metodologie di sviluppo sicuro, processi di verifica interni, modelli di patching basati su standard internazionali oggettivi e misurabili.

Terza sfida: semplificare. Le organizzazioni sono sempre più complesse. Lo sforzo di tutti i CISO deve quindi essere quello di ridurre i silos, eliminare le complicazioni. Bisogna disporre di una mappatura dei sistemi più critici e di un processo di security governance nella sua interezza, comprensivo di aspetti di Security by design e anche di un approccio sicuro lungo tutto il ciclo di vita dei prodotti/servizi erogati.

In pratica come assicurare la sicurezza della Supply Chain?

Si tratta di impostare un "Security through evidence" ed essere così in grado di dimostrare secondo vari modelli che il codice rilasciato è sicuro, che sono rispettate le linee guida base (come la verifica di processi di routine, il superamento di stress test, la gestione dell'autorizzazione dell'utente).

Noi prevediamo nei processi di procurement

la fornitura di linee guida base: il cliente deve fornire nei contratti specifiche tecniche e requisiti base. Anche ai nostri provider chiediamo appropriati livelli di sicurezza: sia per quanto riguarda i processi e l'organizzazione, sia garanzie di continuità operativa, misurate sulla base di specifici SLA.

In molte aziende il Responsabile della Sicurezza lamenta la difficoltà di coinvolgere il Board/Top Management e renderlo partecipe delle criticità della cybersecurity: è anche il vostro caso?

Non direi: per noi la sicurezza informatica è un elemento critico del business.

La nostra azienda è totalmente tecnologica: disponibilità, integrità e riservatezza dei dati sono aspetti assolutamente critici e prioritari, e l'alta direzione dà risposte consistenti. Non avvertiamo questo problema.

Parliamo di ottimizzazione della Governance della Cybersecurity: quale struttura di governance deve essere scelta da ogni azienda?

Una struttura ideale non esiste, dipende dalla singola organizzazione e dai suoi scopi.

Ognuno deve effettuare una valutazione interna e quindi disegnare la governance partendo dal concetto che tutto deve essere risk based. Da questa analisi iniziale derivano output specifici per ogni singola organizzazione.

Nel mondo dell'aviazione civile abbiamo anche norme specifiche in tal senso, l'EASA (l'agenzia europea per la sicurezza aerea, European Aviation Safety Agency) ha avviato un programma con regolamenti di grande impatto.

Inoltre ci sono linee guida comuni per salvaguardare la fear competition tra tutti gli attori, in modo che tutti i provider di servizi di navigazione aerea abbiano misure comparabili.

Oltre alle varie iniziative dell'EASA per rispondere ai rischi di cybersecurity, va ricordato poi l'avvio dell'European Strategic Coordination Platform for cybersecurity, un'iniziativa voluta invece da una serie di attori pubblici, privati e vari rappresentanti dell'aviazione (linee aeree, aeroporti, aviazione commerciale).

Si tratta di un modello condiviso e coordinato di risposta, con l'obiettivo di elevare il livello di intelligence e information sharing nell'aviazione.

Queste iniziative fanno anche sì che vengano adottate da tutte le parti delle prassi comuni, come la nomina di un CISO, l'analisi del rischio secondo modelli standard, una cybersecurity governance comprensiva degli aspetti di monitoraggio e reporting del rischio.

Le aziende si confrontano oggi con l'arrivo di numerose innovazioni Disruptive, dal Cloud, all'Internet of Things, all'intelligenza artificiale. Quale impatto avranno queste innovazioni sulla Cybersecurity aziendale?

Viviamo un momento notevole di trasformazione: la nostra vita sta diventando via via sempre più digitale, con qualche problema di privacy in più. Le nuove tecnologie offrono livelli più elevati di condivisione e una disponibilità immediata dei dati, ma spesso sono fornite con scarsa capacità di sicurezza, come si è visto nel 2017 con l'attacco Denial of service tramite la botnet Mirai che sfruttava appunto le vulnerabilità dell'IoT.

Si rende quindi necessario indirizzare principi più generali e comuni di sicurezza: ciascuno deve cioè partecipare aggiungendo un proprio layer di sicurezza.

Quali saranno quindi i problemi di cybersecurity che le aziende dovranno affrontare il prossimo anno? In quale direzione bisognerà puntare nel 2018 per ridurre i rischi?

Bisogna passare da una gestione generica delle minacce a una fortemente incentrata sulle proprie vulnerabilità. Essere in grado di capire al momento se una minaccia in corso può avere conseguenze dirette sulla propria organizzazione. Si tratta principalmente di applicare il principio "Conosci te stesso", che nel nuovo mondo delle minacce cyber riguarda tutti, le grandi organizzazioni ma anche i singoli individui, perché oggi i rischi sono collegati ai vari utilizzi non consapevoli degli strumenti digitali. Il fattore della responsabilità deve coinvolgere innanzi tutto un'analisi delle vulnerabilità.

Quale sarà quindi in futuro, sempre di più, il ruolo del CISO?

La security sarà sempre di più uno dei principali driver del business. Per chi vive di digitalizzazione, valori come l'integrità, la disponibilità e la riservatezza dei dati stanno diventando importantissimi, non solo per la difesa dell'azienda, della sua continuità operativa e della sua reputazione, ma, nel caso di aziende produttrici, anche per quanto riguarda la qualità dei propri prodotti, che devono avere sempre di più caratteristiche intrinseche di sicurezza digitale. Il CISO quindi non sarà più in futuro soltanto chi protegge gli asset critici dell'azienda, come le informazioni critiche contenute nei sistemi, ma dovrà dotarsi di skill e capacità per rendersi proattivo nei confronti della security del prodotto o servizio erogato. Per ENAV lo sbarco in Borsa nel 2016 ha significato impegnarsi ancora di più, adottando un approccio olistico per cui i rischi cyber sono compresi in una visione completa su tutti i rischi, e puntando a valori etici con il fine ultimo della salvaguardia delle dinamiche produttive ma anche dell'impegno nei confronti degli investitori.

THE INNOVATION GROUP
ACCREDITATA DAL MISE

Ministero dello sviluppo economico

The Innovation Group
Innovating business and organizations through ICT

Da diversi anni The Innovation Group è attiva in decine di progetti di Consulenza Direzionale con le PMI per lo sviluppo del Business: grazie alla sua comprovata esperienza ed alle testimonianze soddisfatte dei nostri Clienti, The Innovation Group è stata accreditata dal Ministero dello Sviluppo Economico come società di Temporary Export Manager, secondo le direttive del Decreto Direttoriale MISE del 20 dicembre 2017, ed iscritta all'Albo delle società fornitrici esclusive, sul territorio nazionale, di servizi consulenziali nell'ambito del progetto finanziato 'Voucher per l'internazionalizzazione'.

Questo prestigioso riconoscimento del MISE certifica che The Innovation Group è in grado, nei fatti, di fornire tutti i servizi consulenziali necessari ed appropriati per raggiungere obiettivi strategici di crescita in Mercati Nazionali ed Internazionali: assistenza organizzativa, contrattuale, sviluppo di competenze, ricerche e analisi SWOT di mercato, identificazione e/o acquisizione di nuovi clienti, sviluppo nuovi mercati, ricerca di potenziali partner industriali e/o commerciali.

Siamo a disposizione di tutte le aziende PMI italiane per portare avanti Progetti Consulenziali per lo Sviluppo di Mercati Nazionali ed Internazionali, con un approccio win-win, per raggiungere insieme il successo finale.

CONTATTACI PER CAPIRE COME COGLIERE QUESTA OPPORTUNITÀ!

IL CAFFÈ DIGITALE

ISCRIVITI ALLA NEWSLETTER MENSILE!

RICEVI GLI ARTICOLI
DEGLI ANALISTI DI THE
INNOVATION GROUP
E RESTA AGGIORNATO
SUI TEMI DEL MERCATO
DIGITALE IN ITALIA!

QUESTO MESE ABBIAMO
FATTO COLAZIONE CON...

ING

COMPILA IL FORM DI REGISTRAZIONE SU
www.theinnovationgroup.it