DICEMBRE 2019

IL CAFFÈ DIGITALE

THE INNOVATION GROUP NEWSLETTER

I TEMPORALI SULL'INDUSTRIA BANCARIA CONTINUANO

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Andrea GUANCI
Direttore Marketing, MSC Crociere

CYBERSEC E DINTORNI

Quali saranno le tendenze della Cybersecurity nel 2020

Sommario

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Andrea GUANCI
Direttore Marketing
MSC Crociere

Pag. **4**

L'EDITORIALE

I TEMPORALI SULL'INDUSTRIA BANCARIA CONTINUANO

Ezio Viola | Managing Director, The Innovation Group

La recente presentazione del piano industriale di Unicredit conferma e prosegue la direzione del cambiamento in cui è impegnata una delle più grandi banche italiane, tenendo presenti due fattori condizionanti: l'invasività e pervasività delle tecnologie digitali e un perimetro normativo in evoluzione.

Cercare di continuare ad essere competitivi e fare banca al tempo dei tassi negativi, con margini stretti, con una attenzione febbrile verso i requisiti di capitale è alla base del piano, che punta a focalizzarsi sulla clientela, offrendo servizi più evoluti, con un maggior contenuto digitale e un approccio consulenziale alle esigenze della clientela.

Completate le operazioni di de-risking, il focus è su una gestione prospettica del rischio, non solo alla luce delle previsioni economiche, ma soprattutto delle evoluzioni normative che negli anni scorsi hanno fortemente impattato i bilanci dell'industria del bancaria.

Uno dei temi caldissimi posti dal piano riguarda l'occupazione. Le prospettate uscite di 8 mila dipendenti nei prossimi 4 anni, di cui 5.500 in Italia, a cui andranno ad aggiungersi i 500 che usciranno da qui a fine anno in forza di accordi già raggiunti, portando il totale a 6 mila, che costituiscono circa il 15% del lavoratori delle banca, hanno scatenato le reazioni dei sindacati e della politica e non poteva essere diversamente.

Vanno però considerate due variabili: le probabili assunzioni di nuove figure professionali che andranno a dare corpo alla banca delineata dal piano e il fatto che in una realtà di queste dimensioni ogni anno si avvieranno alla pensione un numero di lavoratori significativo; diventa però strategico capire quindi quante assunzioni il gruppo prospetterà in arco di piano.

L'annuncio di Unicredit non è inaspettato e arriva poco dopo l'uscita di un rapporto dal titolo "Banche Italiane su un piano inclinato" di Oliver Wyman in cui si prospettano 5 miliardi di costi da tagliare a livello di sistema bancario nei prossimi 5 anni per mantenere l'attuale redditività che come sappiamo è più bassa della media europea e meno del costo del capitale.

Se le banche italiane volessero cercare di raggiungere la media

“I sistemi legacy e di core banking oggi rappresentano un vincolo strutturale verso l’evoluzione completamente digitale dei processi bancari, sono sempre più inefficienti, costosi e difficili da gestire per connettere i nuovi layer digitali basati su API.”

europea allora il taglio dei costi potrebbe essere di circa 10 Miliardi di Euro.

La contrazione del margine di intermediazione è imputabile a 3 fattori: la compressione della redditività degli impieghi che porterà a ridurre il margine di interesse del 15%, la compressione dei ritorni sui titoli di debito con un’altra riduzione del margine di interesse del 5% e la riduzione dei ricavi commissionali che tenderanno a diminuire per la maggiore concorrenza sui prezzi.

Le banche si trovano di fronte a dievrse discontinuità non più rimandabili anche di fronte ad un eventuale ed auspicabile consolidamento che avverrà con tempi più lunghi ma che non sarà sufficiente a rilanciare la profittabilità dell’industria bancaria.

Sono quindi necessari:

- un radicale e veloce cambiamento dei modelli di business per allineare la base dei costi e dei ricavi prevedibili
- una gestione più dinamica e proattiva della struttura degli attivi e dei passivi di bilancio
- un utilizzo delle tecnologie avanzate per la gestione dei dati e dell’AI nella gestione end-to-end del processo del credito: dalle politiche creditizie, all’erogazione, monitoraggio e recupero
- l’utilizzo dei canali digitali consistente al ridisegno del modello distributivo e di servizio

Questo può significare una ulteriore riduzione di circa 7000 filiali e di 70.000 risorse: le banche diventeranno meno labour intensive ma sarà necessario riqualificare in chiave digitale circa la metà del personale attuale.

Inoltre, ancora di più, sarà fondamentale rivedere i processi di relazione con la clientela sfruttando anche qui i sistemi di advanced analytics per segmentare i clienti con offerte personalizzate e una customer experience semplice e coinvolgente come quella dei new player digitali e delle nuove banche che sono sempre menzionate come esempio.

I sistemi legacy e di core banking oggi rappresentano un vincolo strutturale verso l’evoluzione completamente digitale dei processi bancari, sono sempre più inefficienti, costosi e difficili da gestire per connettere i nuovi layer digitali basati su API.

La loro evoluzione e modernizzazione accelereranno l’adozione di soluzioni comuni in partnership con fornitori di tecnologia e servizi.

La ricerca di soluzioni comuni sarà anche spinta nell’ambito della necessità di utilizzare sistemi avanzati di AI e machine learning per automatizzare e rendere più efficiente il sistema dei controlli.

Anche i ricavi le banche devono andarle a cercare in modo innovativo con l’utilizzo delle tecnologie digitali nelle aree più ad alto margine e quindi sarà necessario maggiore focus sui business del wealth management/bancassurance e consumer credit che offrono cost/income, ritorni sul capitale e livelli di assorbimento migliori della banca commerciale universale classica.

Come già ripetuto in altre occasioni e in diversi dei nostri appuntamenti siamo di fronte ad una trasformazione veloce e profonda dell’industria bancaria che richiede un supporto da parte di tutti gli stakeholder e un dialogo che sia rivolto al futuro.

Aspettiamo quindi con attenzione i prossimi piani industriali che saranno presentati da alcune importanti banche nei prossimi mesi.

QUESTO MESE ABBIAMO FATTO COLAZIONE CON

La crociera diventa un viaggio anche digitale per MSC

Intervista di **Roberto Bonino** a
Andrea Guanci
Direttore Marketing di MSC Crociere

Il marketing è probabilmente il settore nel quale la trasformazione digitale sta avendo gli effetti più evidenti e tangibili. La combinazione di dati e tecnologie digitali può far aumentare la rilevanza delle azioni pubblicitarie, ma anche ispirare innovazioni nell'erogazione dei servizi o nella proposizione delle offerte.

Al centro di questa evoluzione c'è la nuova centralità assunta dal cliente, pronto a esperienze di ingaggio digitale costruite su interazioni dirette, scambi di esperienze e offerte personalizzate, che siano online oppure offline.

Il concetto di customer journey, sostenuto dall'utilizzo delle tecnologie digitali, sta ispirando il percorso evolutivo di una realtà come MSC Crociere, che ha nel viaggio, innanzitutto il centro nevralgico del proprio business.

Delle nuove modalità di contatto, ingaggio e relazione con il cliente, abbiamo parlato con Andrea Guanci, direttore marketing di MSC Crociere.

Quanto pesa oggi la componente digitale sulla vostra attività?

Dobbiamo innanzitutto sottolineare come il mercato delle crociere continui a essere fortemente intermediato anche in altri paesi, più avanzati del nostro, come per esempio gli Stati Uniti o la Gran Bretagna. I volumi commerciali generati non sono ancora troppo significativi, ma la componente digitale è ormai fondamentale per costruire una strategia omnicanale, senza più confini stretti fra un mondo e l'altro, a supporto di un customer journey sempre più completo.

Come si struttura la vostra relazione con i consumatori?

Nel nostro settore, il concetto di viaggio identifica tanto il nostro prodotto quanto il concetto marketing della relazione con il cliente. Su questo abbiamo lavorato per costruire una strategia che mira a far vivere a ogni cliente il viaggio già molto prima della sua realizzazione e farlo proseguire anche una volta terminato. In fase di decisione, inizia a costruirsi nelle persone un sogno, che culminerà nella crociera. Qui iniziamo ad agire sul cosiddetto decision journey tramite la componente social, dove si cercano informazioni sulla destinazione o testimonianze di chi già provato un'esperienza simile. Il percorso continua poi tra il momento dell'acquisto e quello della partenza, un tempo speso per organizzare al meglio il viaggio.

In questo modo, alimentiamo le aspettative del cliente, per rendere ancor più memorabile la

settimana che trascorrerà su una delle nostre navi. Finita la vacanza, poi, occorre mantenere vivi i ricordi e anche qui supportiamo i clienti nel processo di alimentazione della memoria, gratificante per chi ha vissuto un'esperienza, ma utile anche per creare advocacy per noi e magari innescare un nuovo sogno nella mente di chi ha già viaggiato con noi.

E le tecnologie digitali come supportano questo processo circolare?

Sono molto utili soprattutto nella prima fase, quella dell'ispirazione e dell'esplorazione, in un mix che passa anche dalla pubblicità tradizionale, ma attinge anche alla ricerca e alla comunicazione via Web, per arrivare alla consultazione del nostro catalogo, sul quale abbiamo lavorato per integrare la componente di realtà virtuale. Chi si reca in un'agenzia, può utilizzare un visore per provare in anticipo l'esperienza che poi vivrà di persona. Nella fase di esplorazione, vediamo un differenziale per la nostra proposta, grazie a un sito che offre numerose possibilità di visualizzare il prodotto nei minimi particolari. Se la scelta vera e propria ancora oggi si concretizza in un'agenzia, anche la crociera integra componenti tecnologiche a supporto dell'esperienza del cliente, ad esempio il digital signage per prenotare la cena da qualsiasi touchpoint sulla nave o un assistente virtuale sempre a disposizione. Nella fase della memoria, entra in gioco lo spazio personale riservato ai clienti per poter condividere quanto vissuto, conservare i ricordi ma anche dialogare con gli altri.

Quali strumenti utilizzate per profilare e ingaggiare i clienti?

Già da tempo lavoriamo sulle informazioni ricavate da ciò che i clienti fanno sulle navi per comprendere attitudini e gusti, in modo da creare cluster omogenei e costruire così azioni specifiche. Ora stiamo iniziando a fare qualcosa di simile anche sui prospect, per esempio analizzando come vengono sfogliati i cataloghi digitali per capire gli interessi dominanti e costruire versioni più personalizzate del catalogo stesso. Il nostro lavoro si basa molto più sui comportamenti che sulle ricerche di mercato e i big data aiutano a ottenere preziose informazioni, se naturalmente trattati e gestiti in modo da ottenere polarizzazioni credibili. Naturalmente, tutto si svolge in perfetta osservanza della normativa GDPR, per cui possiamo lavorare solo su dati aggregati, comunque essenziali per fare analisi e creare modelli predittivi.

Qual è il vostro rapporto con il dipartimento IT?

La tecnologia è ormai oggetto specifico delle strategie di marketing. Quando si vende il nostro prodotto in un certo senso si vende anche tecnologia come strumento primario di supporto. Pertanto, siamo noi del marketing a identificare esigenze e problematiche, ma anche fornire input sulle soluzioni da adottare. L'IT è abilissima nel portare a compimento i progetti costruiti sulla base delle nostre necessità, quindi il lavoro è molto condiviso, ma anche noi abbiamo acquisito, inevitabilmente, competenze tecnologiche.

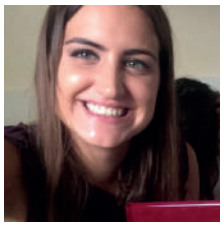
Come evolverà la vostra strategia?

Resterà centrale la commistione fra digitale e reale. Abbiamo da poco terminato un progetto legato all'interrelazione fra agenzie di viaggio e social media, per fare in modo che oltre alla vetrina fisica i nostri partner ne abbiano anche una digitale su Facebook. Procederemo nello sviluppo di ulteriori attività volte a arricchire soprattutto la fase iniziale l'elaborazione del sogno e quella successiva di memoria del nostro cliente. Nel giro di un paio d'anni, l'obiettivo e vendere un viaggio esperienziale, che ha comunque il suo culmine nella crociera, ma comprende numerosi elementi in più. Nel luogo ideale che stiamo creando ci sarà spazio soprattutto per gli user generated content e in questo senso il digitale è il supporto migliore per crearli.

Credit: MSC website

NUMERI E MERCATI

Qual è il livello di maturità digitale delle aziende italiane?



Carmen Camarca
Analyst, The Innovation Group

All'interno del Rapporto annuale "Digital Italy 2019 – Per il governo dell'innovazione digitale nel Paese", presentato a Roma lo scorso 26 novembre in occasione del Digital Italy Summit, è stata sviluppata un'analisi per comprendere la percezione delle aziende sullo stato dell'arte dell'innovazione al loro interno. Al campione, composto da 202 aziende estratte casualmente dal database utenti di The Innovation Group, è stato chiesto di esprimere un giudizio in una scala da 1 (pessimo) a 10 (ottimo) sul grado di "innovatività" raggiunto dalla propria azienda rispetto a:

- le iniziative sviluppate dalla funzione IT aziendale,
- gli investimenti in tecnologia,
- la capacità della divisione IT e delle tecnologie di supportare le attività aziendali e di "portare" innovazione al Business,
- la diffusione e la qualità degli strumenti di gestione e analisi di dati,
- la capacità di innovazione del software utilizzato in azienda.

Nel complesso l'analisi sullo stato dell'innovazione digitale in Italia mostra la fotografia di una situazione ancora non particolarmente definita, in cui risulta complesso individuare dei trend generali.

Tuttavia, in linea di massima emerge uno stato dell'IT in Italia tendenzialmente ancora tradizionale, in cui le aziende hanno iniziato a intraprendere un percorso di trasformazione digitale volto principalmente alla riorganizzazione dei propri processi interni più che allo sviluppo di attività che potrebbero essere ritenute più "innovative", come appunto l'utilizzo e la gestione del dato in azienda e che potrebbero impattare in maniera più significativa, ad esempio, nell'approccio e nella relazione con il cliente.

Per quanto riguarda l'analisi per dimensione e settore aziendale, le aziende grandi (oltre 500 dipendenti) risultano più avanti (appartenendo in misura maggiore agli "Attivi"[1]) in ambiti quali l'analisi dei dati e la capacità innovativa del software aziendale, oltre ad essere anche quelle che hanno una migliore percezione del ruolo propulsore dell'IT in azienda di stimolare l'innovazione verso il Business. Le aziende medio-piccole (fino a 99 dipendenti) hanno espresso, invece, una valutazione più negativa (rientrando principalmente negli "Immobili") sul livello di innovazione delle iniziative e degli investimenti IT.

Dall'analisi è, infine, emersa una posizione d'interesse sia per il campione della Pubblica Amministrazione sia per quello della Finanza.

Nel caso della Pubblica Amministrazione è stata rilevata una posizione positiva con riferimento al livello di innovazione delle iniziative e degli investimenti IT e alla capacità innovativa degli strumenti tecnologici, mentre è emersa una

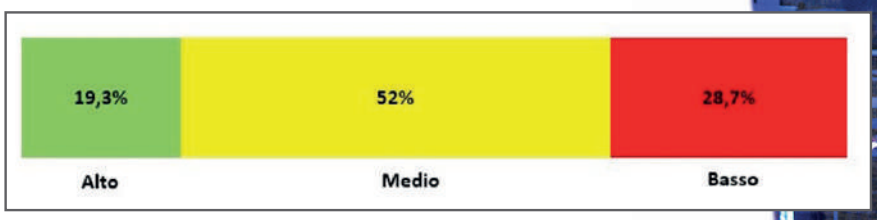
valutazione negativa sulla collaborazione con l'IT e sull'utilizzo di dati e strumenti volti a gestirli. Tali risultati mettono in mostra come all'interno degli enti pubblici abbiano iniziato lo sviluppo di attività innovative che però ancora non si basano su strategie data driven né sono supportate da un'adeguata collaborazione con la divisione IT.

Per quanto riguarda la Finanza è emersa una posizione positiva sulle iniziative e gli investimenti IT e sulla capacità del Business di sollecitare l'IT: tali valutazioni risultano in linea con i cambiamenti che stanno impattando il settore negli ultimi anni e che richiedono una rivisitazione del proprio business model in chiave digitale.

Il Digital Transformation Index

Sommando le singole valutazioni emerse dai rispondenti per ciascuna domanda è stato ricavato un indice, definito "Digital Trasformation Index" e suddiviso nei tre cluster "Basso" (intervistati che hanno ottenuto un punteggio complessivo nelle risposte da 1 a 33), "Medio" (da 34 a 66) e "Alto" (oltre 66).

L'indice ha rilevato che oltre la metà del campione (52%) ritiene che la propria azienda si trovi in una fase intermedia del processo trasformativo, contro il 28,7% che ne è solo all'inizio e il 19,3% che si reputa in una fase avanzata. In modo particolare, la maggior parte del campione attribuisce una valutazione intermedia al livello di innovazione delle iniziative e degli investimenti in IT che la propria azienda sta sviluppando così come al rapporto tra l'IT e il Business. Soprattutto in relazione a quest'ultimo aspetto è emerso come sia ancora molto forte il ruolo del Business nel sollecitare le attività innovative, una tendenza confermata anche dal fatto che, con riferimento alla capacità innovativa delle figure IT e delle tecnologie in azienda, la maggior parte del campione ha ritenuto di appartenere agli "Immobili".



[1] Per ogni domanda la distribuzione dei voti ottenuta è stata suddivisa in tre cluster:

immobili, con voto da 1 a <=4; comprendente le aziende che non hanno ancora iniziato il processo di trasformazione digitale o che sono in procinto di farlo.

In mezzo al guado, con voto >4 e <=8; comprendente le aziende che hanno iniziato o stanno iniziando il processo di digitalizzazione delle proprie attività.

Attivi, con voto >8; comprendente le aziende che sono in una fase avanzata del proprio percorso di digitalizzazione e che si sono dotate di una vera e propria "digital strategy".

LA TRASFORMAZIONE DIGITALE

Svolta Green del Piano Industria 4.0

Vincenzo D'Appollonio
Partner, The Innovation Group

Il MiSE annuncia la 'svolta green' del Piano Industria 4.0: si è svolto recentemente al Ministero dello Sviluppo Economico il tavolo su Transizione 4.0, presieduto dal Ministro Stefano Patuanelli, con la partecipazione delle associazioni che rappresentano le Imprese che operano nel nostro Paese.

L'incontro ha avuto l'obiettivo di avviare un confronto sui risultati raggiunti in questi anni dalle misure previste dal Piano Impresa 4.0, al fine di migliorare gli strumenti già esistenti e individuare un nuovo assetto, che attraverso una programmazione pluriennale possa supportare PMI e Grandi imprese verso una transizione tecnologica che premi lo sviluppo dell'economia circolare ('green economy') da parte delle Aziende italiane: si punta ad incentivare di più rispetto agli anni precedenti gli investimenti in formazione 4.0 e in trasformazione tecnologica e digitale, se finalizzati alla sostenibilità ambientale.

La Commissione Brundtland, Commissione mondiale per l'ambiente e lo sviluppo indetta dalle Nazioni Unite nel 1987, diede una definizione precisa di sostenibilità ambientale, più precisamente di sviluppo sostenibile, affermando come questo sia "la condizione di uno sviluppo in grado di assicurare il soddisfacimento dei bisogni della generazione presente senza compromettere la possibilità delle generazioni future di realizzare i propri."

> Il concetto di sostenibilità ambientale ha fatto registrare una profonda evoluzione che, partendo da una visione centrata prevalentemente sugli aspetti ecologici, è giunta nel tempo ad un significato più globale, che tenesse conto delle dimensioni sociale ed economica, oltre che ambientale.

Il concetto di sostenibilità ambientale ha fatto registrare una profonda evoluzione che, partendo da una visione centrata prevalentemente sugli aspetti ecologici, è giunta nel tempo ad un significato più globale, che tenesse conto delle dimensioni sociale ed economica, oltre che ambientale.

La ‘green economy’ è dunque un modello di sviluppo economico che valuta un’attività produttiva non solo in base ai benefici derivanti dalla crescita ma anche dal suo impatto ambientale. In particolare l’obiettivo degli investimenti pubblici e privati è ridurre l’inquinamento, aumentare l’efficienza di energia e risorse e preservare la biodiversità.

Riteniamo questi aspetti strettamente legati alla pratica dell’Innovazione nelle aziende, ed alla Responsabilità Sociale d’Impresa: infatti Innovazione applicata alle imprese non significa solo adozione di tecnologie ICT avanzate nei processi di produzione, ma anche trasformazione dei comportamenti aziendali nei confronti dell’ambiente, del risparmio energetico, del territorio, della formazione dei giovani, in generale della società in cui viviamo.

Nelle nostre attività di consulenza direzionale per le PMI lombarde notiamo come siano sempre più numerose le Piccole e Medie Imprese che hanno comportamenti virtuosi in termini di Responsabilità Sociale d’Impresa, cioè l’ambito riguardante le implicazioni di natura etica all’interno della visione strategica d’impresa; ci confrontiamo con una sempre più ampia manifestazione della loro volontà di gestire efficacemente le problematiche d’impatto sociale ed etico al loro interno e nel contesto operativo che le circonda, nel rispetto di tutta la collettività nel Territorio; coniugando le giuste istanze economiche con le attenzioni sociali e ambientali nell’ottica di uno sviluppo sostenibile, con lo scopo di migliorare la qualità della vita della Comunità.

E questo testimonia non solo una sempre maggiore sensibilità delle Imprese agli aspetti ‘green’ ed a comportamenti eticamente corretti verso colleghi, fornitori e clienti, ma ispira anche il comportamento dell’Impresa nella Comunità: l’Impresa mette le proprie competenze tecniche al servizio di associazioni di categorie, scuole, enti pubblici e servizi territoriali.

Questo impegno virtuoso verso la società, l’ambiente e gli stakeholder in generale, personale, clienti, fornitori, comunità locali, diventa alla fine ‘premiante’ per la ‘Brand Reputation’ aziendale, ed importante per lo sviluppo del Business sul Mercato indirizzato.

LA TRASFORMAZIONE DIGITALE

Skill gap, l'ostacolo sul percorso della trasformazione

Valentina Bernocco
Giornalista, Technopolis e IctBusiness

Quello delle competenze, o meglio del gap di competenze da colmare nelle aziende affinché la trasformazione digitale possa pienamente realizzarsi, è un ritornello che risuona da tempo. Ne parlano i media, i vendor tecnologici, le ricerche di mercato.

La lacuna è in parte comprensibile: l'impetuosa evoluzione della tecnologia crea continuamente necessità nuove, traducendosi in un carico di sapere teorico e pratico in buona parte ancora da costruire. Le università del mondo stiano tentando di stare al passo con nuovi corsi di laurea e master, ma intanto nelle aziende è scoppiata la richiesta di figure specializzate, soprattutto nei campi degli analytics e dunque della data science, nell'intelligenza artificiale, nella robotica, nella cybersicurezza in tutte le sue declinazioni, nell'industria 4.0, senza dimenticare lo sviluppo software in ottica DevOps.

Si può dire, forse, che questi fenomeni si stiano affermando sul mercato Ict (nell'offerta, innanzitutto, e secondariamente nell'adozione da parte delle aziende) più rapidamente di quanto non stiano producendo nuove competenze.

Ad aggravare il divario c'è il fatto che le vecchie generazioni di dipendenti e di manager raramente ricevano una formazione specifica su temi che impattano sulla vita lavorativa quotidiana e sulla tranquillità dell'azienda: il sapersi difendere da tentativi di phishing, per esempio, o utilizzare servizi cloud da remoto senza favorire attacchi informatici e fughe di dati.

L' EVOLUZIONE DELLA TECNOLOGIA CREA CONTINUAMENTE NECESSITÀ NUOVE, TRADUCENDOSI IN UN CARICO DI SAPERE TEORICO E PRATICO IN BUONA PARTE ANCORA DA COSTRUIRE

Citiamo a tal proposito una recente ricerca di Trend Micro, condotta da Opinium su 1.125 responsabili della cybersicurezza di 12 Paesi: il 44% degli intervistati (e il 49% di quelli italiani) sostiene di avere difficoltà a spiegare ai colleghi esterni al dipartimento IT questioni complesse come quelle di sicurezza informatica.

Per quanto la cybersicurezza non sia di per sé un veicolo di Digital Transformation, allo stesso tempo è un requisito per le società che affrontano progetti di rinnovamento tecnologico o adottano nuove applicazioni.

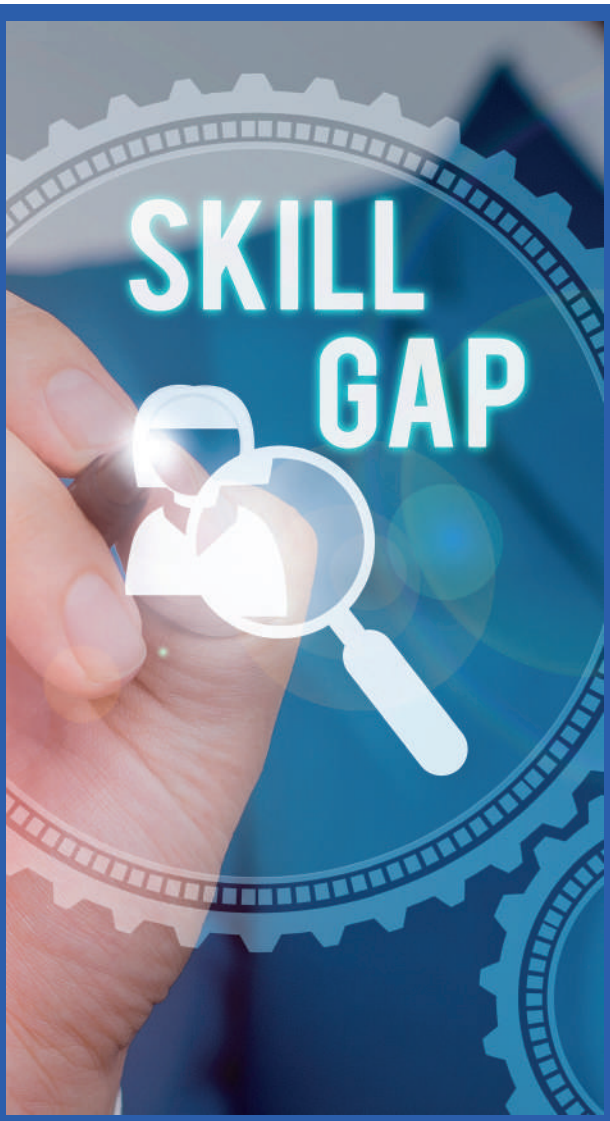
Allargando lo sguardo al quadro generale delle competenze, la situazione non migliora. Nel "The Future of Jobs Report 2018" (studio che prende in considerazione oltre 15 milioni di lavoratori di imprese di 12 settori di tutto il mondo), il World Economic Forum prevede che l'85% delle aziende da qui al 2022 farà progressi nell'adozione dei Big Data analytics. Corposi investimenti saranno diretti anche all'Internet of Things, all'intelligenza artificiale, alla realtà aumentata e virtuale.

L'automazione e la robotica inevitabilmente impatteranno sulla forza lavoro: dunque il reskilling per molti dipendenti sarà una questione di sopravvivenza, per potersi ricollocare su posizioni più qualificate all'interno della medesima azienda o in altre. "Le lacune di competenze, sia tra i lavoratori sia tra i dirigenti aziendali senior, potrebbero ostacolare in modo significativo l'adozione di nuove tecnologie e dunque la crescita del business", si legge nel report.

L'Organizzazione per la Cooperazione e lo Sviluppo Economico ha stimato che in Europa esistano almeno 80 milioni di lavoratori male accoppiati al ruolo professionale svolto, o perché troppo o perché troppo poco qualificati.

In estrema sintesi, sembra di poter dire che oggi abbiamo a disposizione numerosi strumenti di trasformazione digitale, ma spesso non sappiamo come maneggiarli. Tutto sommato, alcuni studi concedono qualche ragione di ottimismo: dal sondaggio "The Future of Work", sponsorizzato da Ricoh e condotto da Arup su tremila dipendenti d'azienda europei, è emerso che più di tre su quattro (77%) credono di possedere le competenze necessarie per rimanere aggiornati e assecondare la trasformazione da qui ai prossimi dieci anni.

Otto su dieci (81%) hanno fiducia nel fatto che saranno i loro datori di lavoro a procurare sia la formazione sia gli strumenti necessari per adattarsi ai futuri ruoli professionali. L'ottimismo è forse eccessivo, ma possiamo accoglierlo come un buon augurio e come un'esortazione, per le aziende, a fare la loro parte.



L'automazione e la robotica inevitabilmente impatteranno sulla forza lavoro: dunque il reskilling per molti dipendenti sarà una questione di sopravvivenza, per potersi ricollocare su posizioni più qualificate all'interno della medesima azienda o in altre

DIRITTO ICT
IN PILLOLE

Proprietà Intellettuale: un'occasione per le PMI

Giulia Rizza
Senior Consultant, Colin & Partners

Il report annuale della Property Rights Alliance analizza il livello di tutela della proprietà in oltre 129 nazioni, pari al 98% del PIL mondiale e il 93% della popolazione, basandosi su tre ambiti di analisi:

- L'ambiente giuridico e politico, inteso come la capacità di una nazione di far rispettare un sistema dei diritti di proprietà.
- Il livello di protezione dei diritti di proprietà fisici, analizzando in particolare l'efficienza e l'efficacia della giustizia civile.
- Il livello di tutela dei diritti di proprietà intellettuale, valutato tenuto conto delle normative in tema di brevetti e dei livelli di pirateria.

L'Italia si aggiudica un punteggio di 6.1 su 10, assestandosi al 46mo posto, e pagando in particolare l'inefficienza del sistema giudiziario e gli ampi livelli di corruzione percepiti. Dal report emergono anche alcune preoccupazioni in merito all'apertura della "Nuova Via della Seta", atteso che la sola contraffazione in Cina di prodotti e brand italiani causa 24 miliardi di perdite per l'Italia e le sue aziende.

Nonostante questo, nel nostro Paese, la tutela dell'innovazione è percepita come un efficace strumento di promozione della crescita sostenibile, in quanto offre a coloro che investono tempo, impegno e denaro nell'innovazione un meccanismo per proteggerla e trarne vantaggio.

Il World Intellectual Property Indicators 2019, analisi annuale svolta dalla WIPO (Organizzazione Mondiale della Proprietà Intellettuale) che riporta i dati dei depositi di domande di brevetti, marchi e design internazionali dell'anno precedente, evidenzia come l'Italia sia tra i 10 Stati aderenti al sistema internazionale in cui si brevetta di più. Nel 2018, infatti, l'aumento delle domande di marchio internazionali depositate è stato del 16,6%.

Inoltre, dalla recente indagine EUIPO (Ufficio UE della Proprietà Intellettuale) sulle piccole e medie imprese e sulla proprietà intellettuale, emerge come per oltre il 60% delle aziende titolari la registrazione abbia avuto un effetto positivo sull'attività, migliorando la propria reputazione e credibilità, ed aumentando fatturato e prospettive di espansione sul mercato.

Dallo studio emerge come la maggioranza delle PMI intervistate sia stata motivata a registrare le proprie privative per impedire di essere copiate da parte dei concorrenti (59%), incrementare la certezza del diritto (58%) e migliorare l'immagine e il valore dell'impresa (36%).

Tuttavia, hanno allo stesso tempo lamentato una mancanza di informazione in merito agli strumenti di tutela del proprio patrimonio intellettuale, nonché scarsa conoscenza dei benefici fiscali ed economici riconosciuti alle PMI in materia di marchi, brevetti e design.

Come dichiarato dal Direttore esecutivo dell'EUIPO, questa tipologia di imprese svolge un

ruolo fondamentale nell'economia dell'innovazione e la proprietà intellettuale contribuisce a proteggere preziose risorse aziendali. Offrire loro un solido supporto è essenziale per una crescita economica intelligente e sostenibile.

Diventa fondamentale, quindi, un'adeguata formazione ed informazione in materia, non soltanto per aumentare la consapevolezza delle PMI in merito al valore strategico del proprio patrimonio intellettuale, ma anche per far conoscere efficaci strategie e strumenti di tutela delle proprie attività inventive.

A fronte della conclamata inefficienza del sistema giudiziale italiano, con procedimenti civili che durano anni e dall'esito e costo incerti, esistono soluzioni che consento ai titolari di privative intellettuali di azionarsi prontamente ed ottenere risultati in tempi brevi e con costi contenuti. Servizi di monitoraggio degli usi non autorizzati delle proprie privative industriali, quali ad esempio la sorveglianza dei siti di aste online e/o dei canali social, garantiscono – ad esempio – di essere informati prontamente e di impostare efficaci soluzioni stragiudiziali volte a eliminare prontamente le violazioni occorse.

CYBERSEC
E DINTORNI

Quali saranno le tendenze della Cybersecurity nel 2020

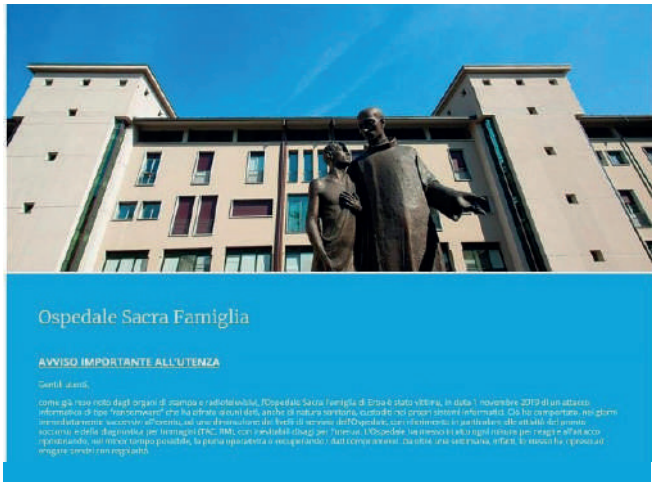
Elena Vaciago
Associate Research Manager, The Innovation Group

Per chi sta lavorando oggi al budget e alla programmazione di quelle che saranno le azioni del 2020, per garantire una protezione efficace di dati, applicazioni, infrastrutture e, non ultima, la reputazione aziendale, guardare alle evoluzioni previste per i rischi di cybersecurity nel prossimo anno significa considerare uno scenario molto mutevole, che prenderà le mosse da quanto abbiamo appreso quest'anno ma comporterà anche nuove complessità da gestire. Di seguito i trend 2020 della cybersecurity.

Ransomware, attacchi mirati e richieste di riscatto in crescita

Quest'anno abbiamo vissuto una vera epidemia da ransomware, il malware che una volta infettato un PC o una rete, crittografa tutti i dati e chiede un riscatto in cambio della chiave per ripristinarli. Abbiamo visto attacchi ransomware molto più mirati a singole organizzazioni, con il malware nascosto in mail di spear phishing indirizzate a singole persone. Negli USA in soli 10 mesi sono stati presi in ostaggio 140 amministrazioni locali, stazioni di polizia e ospedali. In agosto, 23 municipalità del Texas – che dipendevano per i propri servizi dal Texas Department of Information Resources (DIR) – hanno subito un blackout informatico a causa di un'infezione da ransomware. In luglio invece il Governatore della Louisiana ha dichiarato lo stato di emergenza in risposta a un incidente di questo tipo che ha coinvolto 3 distretti scolastici.

Numerosissimi poi gli attacchi con cancellazione di dati sanitari rivolti contro gli ospedali, tra cui il caso recente dell'Ospedale Sacra Famiglia di Erba, facente capo al Fatebenefratelli, che lo scorso primo di novembre è caduto vittima di un attacco ransomware con cifratura di dati di natura sanitaria. Questo ha comportato, nei giorni immediatamente successivi all'evento, ad una diminuzione dei livelli di servizio dell'Ospedale, con riferimento in particolare alle attività del pronto soccorso e della diagnostica per immagini (TAC, RM). In seguito all'attività di ripristino, è emerso però che non era stato possibile recuperare le immagini radiologiche relative ad alcune prestazioni erogate negli ultimi 12 mesi.



Fake News e AI Deep Fakes

Se nelle elezioni del 2016 si è assistito alla prima, massiccia e preoccupante diffusione di Fake News sui social (notizie fittizie contro avversari politici in grado di influenzare il voto e mettere quindi in crisi il funzionamento di una moderna democrazia), il 2020 sarà l'anno in cui le Fake News potranno avvantaggiarsi di nuovi strumenti di intelligenza artificiale per diventare ancora più credibili e quindi pericolose. Sono diventati famosi i video DeepFake costruiti ad arte per risultare credibili, con celebrità come il Presidente Trump, Mark Zuckerberg, gli attori Nicholas Cage, George Clooney e Robert De Niro, Elon Musk, cui sono messe in bocca parole in realtà mai pronunciate. Secondo gli esperti, oggi si può ancora istruire le persone a capire se un video è un DeepFake: ad esempio, quando un viso viene sostituito con quello di un'altra persona, nei punti di "aggancio" dell'immagine permangono delle scollature. Però è anche probabile che gli algoritmi sviluppati in futuro siano così avanzati da rendere assolutamente credibile qualsiasi video fake, e – soprattutto – che il loro utilizzo sia reso accessibile a chiunque, permettendo quindi una diffusione sempre più virale e potenzialmente malevola. Già quest'anno si ha avuto notizia di una frode realizzata utilizzando una finta voce – sintetizzata con strumenti AI – che ha comportato una perdita pari a 243mila dollari per un'azienda energy del Regno Unito. La voce copiata era quella dell'AD della capogruppo tedesca, che ha chiesto al CEO della controllata britannica di effettuare un versamento urgente – su un conto che è poi risultato fasullo – a un fornitore ungherese. In sostanza, con la finta voce (alterata in modo da sembrare credibile) è stata creata una variante della classica CEO Fraud (BEC, business email compromise).

Vulnerabilità delle nuove reti 5G

Anche l'implementazione delle reti 5G – prevista per il 2020 – comporterà nuove sfide legate alla sicurezza cyber. In questo caso le vulnerabilità dipenderanno proprio dal fatto che si tratta di una tecnologia nuova, e su alcuni aspetti i provider saranno impreparati a gestire alcuni aspetti. Ad esempio, gli analisti della cybersecurity hanno predetto che trattandosi di una rete software-defined, avrà delle debolezze intrinseche legate al disegno del software, e richiederà continue patches di sicurezza così come avviene oggi per i nostri smartphone. Un attaccante potrà quindi in alcuni casi individuare degli zero-days, che potenzialmente potrebbero metterlo in condizione di prendere il controllo di ampie porzioni della rete.

In aggiunta, è stato già notato che una debolezza delle reti 5G (utilizzate su larga scala in ambienti pubblici, come hotel, centri commerciali, aeroporti) potrebbe essere legata allo switch automatico che essa abilita tra reti cellulari e reti wifi presenti nella singola location. Secondo i ricercatori di sicurezza ci sarebbero delle vulnerabilità in questo processo di handover cellular-to-wifi, tali da permettere ad eventuali hacker di accedere a dati o trasmissioni voce su telefoni cellulari 5G.

Attacchi alle reti industriali

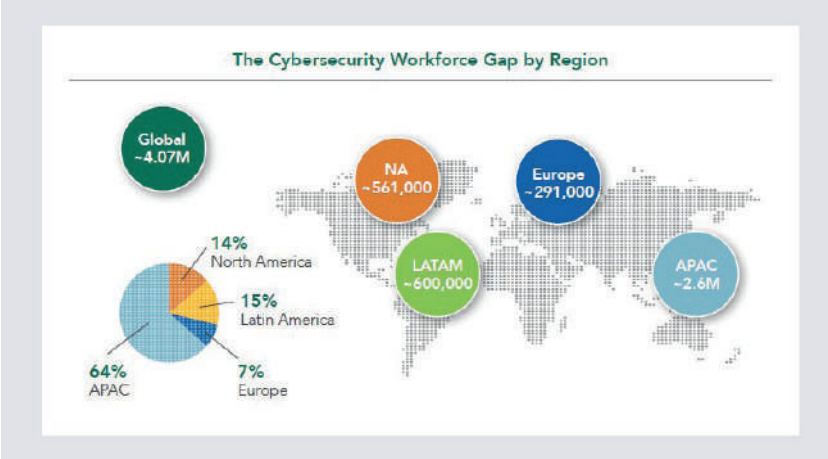
Un ambito che nel 2019 si è dimostrato estremante vulnerabile è quello dei sistemi OT (Operational Technologies) impiegati per infrastrutture critiche, reti di distribuzione dell'energia, del petrolio e del gas, acquedotti, infrastrutture di trasporto, catene di montaggio in fabbrica e quant'altro. Le tecnologie OT sono impiegate in tutti questi ambiti principalmente per il monitoraggio (PLC, DCS), la supervisione e il controllo (ICS/SCADA) di sistemi complessi, per l'automazione dei processi e il mantenimento dei parametri produttivi entro i range pianificati. Si tratta di ambiti che non possono soffrire alcun arresto senza incorrere in gravi danni e perdite elevate in termini di produttività degli impanti, motivo per cui l'Availability è un parametro fondamentale di funzionamento, molto più che non gli aspetti di Integrity e Confidentiality che sono invece elementi centrali nella protezione dei sistemi informativi.

Oggi attacchi ransomware, Denial of Service, APT, hanno raggiunto anche questi sistemi, con conseguenze molto gravi. Ad esempio, a metà ottobre scorso, la società tedesca di automazione Pilz è stata infettata dal ransomware Bitpaymer: tutte le macchine, i PC, i server, i sistemi di comunicazione, sono rimasti in breve tempo irraggiungibili. A dichiararlo è stata la stessa Pilz, informando di aver sconnesso in via precauzionale tutti i sistemi informativi; avviato una procedura di gestione dell'incidente; avvisato le autorità (in particolare l'Ufficio federale tedesco per la sicurezza informatica). Il livello di gravità dell'evento è stato eccezionale: tutte le sedi della società, in 76 paesi nel mondo, hanno subito conseguenze e sono state sconnesse dalla rete aziendale principale, quindi non più in grado di inviare ordini o di verificare lo stato delle transazioni dei clienti. Anche la durata del ripristino è stata lunga: 3 giorni per riottenere l'accesso ai servizi di posta elettronica, altri 3 giorni per ripristinare la posta nelle sedi internazionali. Positivo invece il fatto che le capacità produttive – di fabbrica – non abbiano subito arresto, se non per l'incapacità di processare ordini che o non arrivavano, o giungevano ma a ritmo molto rallentato. Un incidente di questo tipo, se si aggiunge un fermo alla produzione, può avere un impatto economico enorme.

Skill Gap

La cultura della sicurezza informatica avrà una necessaria crescita nei prossimi anni, se non altro, per l'esperienza di attacchi che andranno a segno e colpiranno le singole persone. Misure come il cambio delle password o la multifactor authentication, backup e data protection, stanno entrando nell'uso quotidiano. Quello che invece rimarrà come un problema irrisolto ancora per lungo tempo sarà la mancanza di personale esperto in grado di gestire il tema della mitigazione e della gestione del rischio

cyber. Nel 2018 la domanda inevasa di professionisti di cybersecurity era pari a 3 milioni. A fine 2019 (ISC)[2] ha stimato che nelle prime 11 economie globali ci siano 2,8 milioni di professionisti di cybersecurity, ma che sarebbe richiesta una crescita del 145% (un gap per 4 milioni di persone). La regione in cui la domanda di questi professionisti, sarebbe quella dell'Asia Pacific (fino a 2,6 milioni di esperti che non si trovano). Il problema è come fare a recuperare questo gap, una forbice tra domanda e offerta che, se non si interviene con azioni decise, continuerà a crescere e a rendere sempre più difficile alle aziende il tema della messa in sicurezza delle infrastrutture e dei dati.



Data Privacy e utenti finali

Infine, quello a cui stiamo assistendo è una sempre maggiore consapevolezza da parte degli utenti del valore del proprio dato. Negli ultimi anni abbiamo assistito ad alcuni dei più grandi scandali e data breach: i top player del mondo digitale, Apple, Google, Facebook, Amazon, hanno tutti dovuto in qualche modo "riguadagnarsi" la fiducia degli utenti e fornire maggiori garanzie sul proprio uso sicuro dei loro dati. Ci possiamo aspettare che in futuro gli utenti chiederanno di poter controllare come sono gestite le proprie informazioni personali, e questo sarà uno dei maggiori driver per investimenti in cybersecurity.

Come migliorare nella Preparazione e nella Risposta?

In ultima analisi, il 2020 si avvicina e preannuncia sfide ancora più elevate sul fronte della gestione della sicurezza. Quali le raccomandazioni che ci sentiamo di dover indirizzare, sia ai professionisti del settore, sia in generale al management delle aziende che cominciare a occuparsi di un tema – per molto tempo ritenuto per "addetti ai lavori" – come quello della cybersecurity?

- Lo scenario delle minacce, i requisiti della compliance, il diffondersi delle iniziative di trasformazione digitale: tutto concorre ad aumentare la pressione sui responsabili della cybersecurity. Come rispondere nel migliore dei modi se non si dispone di un team e di tutti gli skill per una gestione olistica della cybersecurity? Le organizzazioni devono oggi prendere in considerazione la possibilità di affidarsi a partner esterni specializzati (es. Managed Security Service Provider), dialogando con i quali riusciranno più facilmente a predisporre piani end-to-end di monitoraggio, detection, gestione dell'incidente e risposta.
- Sempre di più il tema della cybersecurity dovrà diventare parte integrante della cultura aziendale, e per far questo, i manager di quest'area dovranno imparare a parlare il linguaggio del business, confrontarsi con quelli che sono le priorità e i principali rischi per il business. Inoltre, dovranno misurare qual è il migliore contributo che possono dare alla stessa sostenibilità del business. Devono quindi sedere al tavolo dei nuovi sviluppi – soprattutto dove questi coinvolgono componenti digitali – e avere un approccio propositivo, in cui la cybersecurity diventa valore effettivo e componente abilitante la crescita del business.
- Le aziende che affrontano con successo il tema della gestione del rischio cyber non lo fanno da sole, ma facendo leva su una rete di partner esterni: da un lato come dicevamo sopra le società specializzate su questi aspetti, ma non solo. Servono esperienze esterne, condivisione in real time di informazioni sugli attacchi, una risposta coordinata con il law enforcement: tutto questo si può fare solo collaborando con peer e agenzie di cybersecurity, università e centri di ricerca, e i confini nazionali oggi sono stretti … Serve guardare anche a quanto viene fatto all'estero, partendo dal proprio settore ma non solo questo. Assisteremo sempre di più alla creazione di ecosistemi per la cybersecurity che saranno basati su tutte queste relazioni e legami.
- Cybersecurity e Innovazione Digitale. Il tema della sicurezza non deve frenare la migrazione verso il cloud o l'uso innovativo di tecnologie IoT e AI, anzi, deve favorirle il più possibile. L'AI poi sarà un'arma in più a disposizione della protezione: secondo quanto affermato da Capgemini, il 63% delle aziende prevede di utilizzare tecniche AI nel 2020 per migliorare la propria cybersecurity (in particolare negli ambiti della network security, data security, endpoint security, identity e access management).
- Infine, quello a cui dovranno puntare i responsabili della cybersecurity, dal prossimo anno in avanti, sarà di disegnare una roadmap che porti nel tempo a incrementare sempre più la maturità della propria security posture, su più fronti: dall'incident handling, alla risposta, al security-by-design, al monitoraggio, alla detection, prevenzione e remediation. Sono molte le fasi da considerare, lo sforzo deve essere quello di disegnare un percorso di maturazione coerente con l'as-is e con gli obiettivi che si vuole raggiungere.

VOCI
DAL MERCATO

Impostare un percorso efficace per la Trasformazione Digitale

Intervista di **Elena Vaciago** a
Mario Attubato
Corporate Head of Digital Transformation di Saipem

Disegnare l'agenda digitale, individuare una Roadmap coerente comprensiva di un insieme omogeneo di iniziative; introdurre una Governance Digitale il più possibile integrata nell'organizzazione e rivolta ai vertici del business; identificare le architetture digitali del futuro. Sono molti i passaggi strategici e le sfide per le organizzazioni che hanno cominciato un percorso coerente ed esteso di digitalizzazione del business. Come impostare tutto il disegno e prepararsi ad affrontare il cambiamento? Ne parliamo in questa intervista con Mario Attubato, Corporate Head of Digital Transformation di Saipem.

Quali sono quindi i percorsi da seguire per incoraggiare l'Innovazione conservando però il controllo del cambiamento? qual è la vostra esperienza?

L'innovazione in Saipem è in primis parte integrante della cultura aziendale. Da oltre 60 anni, infatti, Saipem propone soluzioni ingegneristiche all'avanguardia a problemi di business particolarmente sfidanti. Per quanto riguarda l'innovazione tecnologica e digitale in Saipem viene perseguita ad un doppio livello: corporate e di divisione. Da alcuni anni, infatti, è stata creata la divisione XSIGHT che si occupa di quella che si definisce ingegneria concettuale e che opera nell'early engagement del cliente, fase strategica per indirizzare investimenti innovativi e sostenibili. A livello corporate esiste invece la funzione dedicata "Digital e Innovation" di cui faccio parte. Sia la Divisione XSIGHT che la funzione "Digital e Innovation" fanno capo a Mauro Piasere.

Sono integrate nella Direzione Digital e Innovation sia la Fabbrica dell'innovazione che la funzione Digital Transformation. La Fabbrica dell'Innovazione è un incubatore di idee, una fucina di sperimentazioni creata in Saipem a partire dal 2016 per affrontare i temi del settore energetico con soluzioni, tecnologie e metodologie alternative. Attraverso la collaborazione attiva con start-up e partner accademici e tecnologici, si propone di perseguire risultati innovativi facendo leva su team misti, ovvero composti sia da persone di Saipem che da esterni.

La funzione Digital Transformation è lo strumento aziendale con cui si promuove la digitalizzazione interna all'azienda e attraverso la quale offriamo ai nostri clienti soluzioni innovative. Opera ricevendo input dal business (demand bottom-up), ma anche proponendo in

autonomia soluzioni digital (demand top-down). A oggi riteniamo che per essere sempre più efficaci nei percorsi di innovazione sia utile, ad esempio:

- valutare tempestivamente quali soluzioni possono essere a beneficio di tutta l'azienda attraverso una capillare estensione;
- valutare upfront i reali benefici e stabilire le priorità;
- comprendere le implicazioni sul business e dotarsi di ottime capabilities a supporto del change management;
- verificare la disponibilità di risorse e di capabilities;
- approcciare le iniziative all'interno di roadmap sostenibili dal punto di vista funzionale, tecnologico e di costo;
- fare leva su partnership che mettano al centro concetti di value e risk sharing;
- introdurre nuove capabilities e nuove modalità di lavoro, come ad esempio il modello di lavoro agile.

Come è organizzata la vostra IT e quale modello avete identificato per portare la DT in azienda?

La funzione Digital Transformation opera in sinergia con la funzione di servizi IT condivisi a livello di corporate. Le 5 Divisioni di Saipem hanno, inoltre, ciascuna una funzione IT dedicata e lavorano in sinergia con le IT locali, dislocate nelle diverse aree geografiche in cui Saipem è presente. Per migliorare e rendere ancora più efficaci i nostri servizi, stiamo migliorando le sinergie per colmare eventuali punti di discontinuità sui processi end-to-end. Ad oggi vi sono diverse azioni in corso:

- avviare un processo di sistematizzazione e arricchimento della domanda al fine di creare l'agenda digitale di Saipem, supportata da roadmap con opportune priorità secondo logiche di valore associato a cluster omogenei di iniziative;
- introdurre una Governance Digitale che coinvolga tutte le divisioni e la corporate a più livelli dal CEO, ai direttori, ai digital champion di aree e alle delivery platform multidisciplinari;
- identificare le architetture digitali del futuro, a supporto del percorso evolutivo di Saipem;
- definire le roadmap tecnologiche delle principali piattaforme, tenendo conto di uno starting point stratificato e mediamente sub-ottimale.

Cosa comporterà tutto questo?

Stiamo parlando di un cambiamento epocale per Saipem. Per portare la DT in azienda bisogna dotarsi di un mix di competenze, verticali sul business specifico, ma anche orizzontali sulle tecnologie. Per far funzionare tutto, IT e business devono co-operare in maniera sinergica. In aggiunta, bisogna acquisire competenze sul mercato, introducendo nuove figure. Oggi è più facile perché Saipem, dopo aver cambiato pelle anche grazie alla riorganizzazione in divisioni, è un'azienda più smart, efficace ed efficiente, capace di stare al passo con un mercato competitivo. Siamo davanti a una sfida davvero stimolante, in un ambiente di lavoro in continua evoluzione.

Come state operando per ridurre la complessità dell'infrastruttura tecnologica, allo scopo di semplificare i processi, automatizzare e liberare le risorse da attività a minore valore aggiunto?

Abbiamo avviato diversi programmi. Due anni fa abbiamo avviato una trasformazione del modello di sourcing e oggi siamo nel pieno del passaggio verso il cloud e verso nuove infrastrutture per i nostri asset in giro per il mondo. Stiamo operando un'ottimizzazione dei processi e dei sistemi, con l'obiettivo di essere sempre più competitivi. Ad esempio, stiamo ridisegnando le architetture applicative e ammodernando le infrastrutture e le piattaforme a supporto del business. A valle di opportuni ridisegni dei processi di business e corporate, prevediamo di attualizzare tutti i trend tipici della trasformazione digitale (e.s. analytics, cloud, RPA, …). Una sfida nella sfida è la volontà di avviare un percorso di trasformazione sostenibile anche per chi lavora in azienda. A tale proposito saranno fondamentali le attività di change management (e.s. upskilling, reskilling).

Quali sono per Lei i trend disruptive più significativi (cloud, mobile, IoT, AI) e, nel breve/medio termine, come andranno a modificare il rapporto e l'interrelazione fra business e tecnologia?

A oggi sono già realtà il passaggio al cloud, sia infrastrutturale che applicativo. Lo sfruttamento delle grandi moli di dati e informazioni da condividere con i clienti sono un aspetto importante nel processo di digitalizzazione e trasformazione. Fondamentale è la capacità di collaborare, interagire, integrare ed analizzare i dati.

A tale proposito, riteniamo che l'IoT, le data platform supportate da AI, siano parte del nostro futuro. Non sottovaluterei anche la capacità della digital collaboration interna ed esterna, in quanto il lavoro è sempre più legato alla capacità di networking e di orchestration. Per un'azienda come Saipem, di cui fanno parte circa 32.000 dipendenti di cui circa 25.000 digitalmente abilitati, anche questo aspetto diventa sostanziale.

VOCI DAL MERCATO

Il rischio Cyber è un rischio di sistema

Intervista di **Elena Vaciago** a
Marcello Fausti
Head of Cyber Security di Italiaonline

Come deve essere gestita la resilienza di sistemi complessi caratterizzati dalla presenza di attori diversi e da un gran numero di interrelazioni? Che cosa potrebbe accadere se capitasse nel mondo cyber qualcosa di simile a un'alluvione, in senso digitale? Siamo pronti a rispondere e a sostenere l'emergenza? e le reti TLC, oggi elemento critico in ecosistemi complessi, sono effettivamente sotto attacco?
In questa intervista riportiamo i temi al centro dell'intervento di Marcello Fausti, Head of Cyber Security di Italiaonline, nel corso del Digital Italy Summit 2019, lo scorso 27 novembre a Roma.

Come cambia la valutazione del rischio considerando sistemi complessi?

Se guardiamo il grafico in cui anche quest'anno il World Economic Forum ha rappresentato lo scenario globale dei principali rischi, come al solito osserviamo che il cyber risk è posizionato in alto a destra. Il motivo è legato al fatto che, come ben sappiamo, il funzionamento delle moderne economie è fortemente dipendente dalle infrastrutture digitali. E le interrelazioni tra gli attori del mondo digitale sono tantissime e spesso sconosciute. Questo significa che – se dovesse manifestarsi un danno significativo ad un nodo di questo sistema – con probabilità molto elevata l'impatto si trasmetterebbe in modo istantaneo ai nodi circostanti.

Viviamo in un mondo di sistemi critici interconnessi, con un nucleo di «servizi essenziali» e «servizi digitali» CORE (quelli identificati dalla Direttiva NIS) a cui si interconnettono una serie di HUB di servizi digitali che hanno il compito di aggregare, semplificare, vestire con funzionalità aggiuntive i servizi digitali per determinate categorie di cittadini o profili di aziende (in particolare per le microimprese e per le PMI). In questa vasta rete, si stabiliscono interdipendenze operative, logiche e geografiche di cui bisogna tenere conto quando si valuta il rischio cyber. I percorsi di interconnessione tra le varie entità sono molteplici: il mondo dell'energy, delle TLC, il cloud, sono 3 ambienti fondamentali, collegati tra loro e sempre coinvolti nelle principali trame. Il cloud, che come sappiamo sta diventando un elemento pervasivo: è abilitatore di semplificazione e di risparmio; permette di realizzare controlli di sicurezza più semplici ed efficaci; rimane, però, un ulteriore layer anch'esso attaccabile.

Se nel 2017 abbiamo visto le conseguenze della diffusione pandemica del ransomware WannaCry (porti bloccati, un pezzo di sanità in crisi, altre parti della PA colpite), l'anno prima, il 2016, ha visto il più importante attacco sferrato da una botnet IoT

al principale service provider USA di servizi DNS, che ha avuto come conseguenza lo spegnimento completo della rete internet per 6 ore in USA. Si trattava evidentemente di una forte criticità del sistema degli Over The Top americani, e nessuno aveva previsto prima di allora che in quel nodo si potesse concentrare un rischio così elevato.

Avviene quindi che il rischio che dobbiamo considerare ha una quota che possiamo gestire con tecniche usuali di mitigazione, accettazione, trasferimento ed eliminazione, ma c'è uno stock di rischio che non dipende solo da noi, bensì dipende soprattutto dal sistema di cui facciamo parte, in cui siamo immersi. È un problema in più che si aggiunge via via che la digitalizzazione diventa elemento fondante dell'economia.

Considerando quindi anche questo rischio di sistema, come ci dobbiamo regolare?

Ci sono 3 livelli di rischio da considerare:

- Il Rischio Interno, su cui riusciamo a lavorare con controlli di sicurezza e con le regole di resilienza. Pensiamo a come un TLC provider progetta la propria rete TLC, normalmente tratte di fibra ridondate.
- Al livello successivo c'è la relazione con le proprie Upstream Infrastructure, come ad esempio con i fornitori di energia o le telco. La relazione con chi ti dà un servizio critico deve essere sempre garantita, mentre non sempre lo è.
- Shock esterno: questo livello è del tutto fuori dalla portata del singolo attore e riguardano il sistema nel suo complesso. Un esempio è costituito dagli attacchi "state sponsored", che sono più reali di quanto siamo portati a pensare e chiamano in causa un livello superiore di responsabilità costituito dai governi e dalle istituzioni preposte al presidio del rischio cyber a livello paese. Anche questo rischio va considerato, eseguendo analisi di scenario magari con il supporto delle istituzioni preposte. Sarebbe molto utile se a livello istituzionale si potesse supportare un ragionamento di sistema sul rischio cyber.

Per ridurre il rischio sistemico, si può contare su capacità di segmentazione e separazione?

Non credo, oramai è un limite travalicato, i dati saranno sempre di meno entro i perimetri nazionali. Credo però che un coordinamento nazionale e una capacità di ragionare a livello di sistema sulla resilienza singola e complessiva delle componenti che alimentano economia digitale del paese sarebbe molto utile. Abbiamo oggi tutta una serie di regolamenti, ma servirebbe in realtà un livello di coordinamento in più. I nostri problemi sono fondamentalmente i seguenti:

- la superfice digitale cresce continuamente, e mentre chi l'attacca si concentra su una parte, chi la difende deve considerarla tutta;
- cresce la velocità dei cicli tecnologici: oggi abbiamo il 5G, il 4G è già storia e il 6G è già in preparazione;
- realizzare gli attacchi è sempre più semplice e meno costoso;
- le minacce diventano sempre più complesse (fenomeno di ibridazione di cyber-armi realizzate da agenzie governative che arrivano in mano a semplici criminali) e quindi difficili da contrastare.

Le reti sono oggi particolarmente sotto attacco?

Le reti sono da sempre sotto attacco: se guardiamo i dati relativi agli attacchi DDoS, osserviamo due picchi, a 1,3 Terabit in banda (attacco a GitHub, acquistato di recente da Microsoft) e a 1,7 Terabit. Il secondo (quello avvenuto nel 2016 ai danni dell'operatore USA di DNS citato in precedenza) è di un ordine di grandezza assolutamente rilevante e sarebbe in grado di mettere in crisi moltissime reti di tlc nazionali. Oggi un operatore TLC ha circa l'80-85% degli attacchi costituiti da tentativi di DDoS e dal 2014 in avanti tutti i più rilevanti attacchi di questo tipo sono realizzati con botnet di IoT.

Quindi per la riduzione del rischio sistemico come fare?

La convinzione è che ad un rischio di sistema sia necessario dare una risposta di sistema. Non possiamo fidarci del fatto che per garantire la sicurezza dell'intero sistema sia sufficiente che ciascun attore lavori al proprio interno per garantire la sicurezza e la resilienza delle proprie infrastrutture (secure us to secure me). La resilienza del sistema non deriva (solo) dall'adozione di regole di buon senso sul perimetro interno ma dalle caratteristiche di progettazione del sistema. Dobbiamo evitare che si creino nodi in cui la concentrazione di rischio (single point of failure) è troppo elevata, ciò avviene quando elementi (che magari hanno al proprio interno un livello di ridondanza elevatissimo) non hanno un'alternativa funzionale e non possono, quindi, essere sostituiti in caso di fault/attacco.

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...

MSC CROCIERE

COMPILA IL FORM DI REGISTRAZIONE SU
www.theinnovationgroup.it