



L'Internet Delle Cose: Evoluzione o Rivoluzione?

Parte 1 di una serie

Prefazione di:

Shawn DuBravac, Ph.D.

Economista capo presso, Consumer Technology Association (CTA)

New York Times Best-Selling Author, "Digital Destiny: How the New Age of Data Will Transform the Way We Work, Live, and Communicate"

Carlo Ratti, Ph.D.

Direttore MIT SENSEable City Lab e curatore del Future Food District all'Expo Milano 2015



Consumer
Technology
Association™



Ringraziamenti

Il seguente documento è stato reso possibile grazie ad una partnership innovativa con la Consumer Technology Association (CTA) ® e il suo capo economista ,oltre che autore del best-seller *New York Times*, Dr. Shawn DuBravac.

Vorremmo anche ringraziare i seguenti esperti di AIG per il loro prezioso contributo a redigere la seguente relazione:

David Bassi
Lex Baugh
Nicolas Berg
Julien Combeau
Jason Kelly
Erik Nikodem
Garin Pace
Matthew Power
e
Joe Trotti



Sommario

PREFAZIONES.....	2
PROSPETTO RIASSUNTIVO	4
CHE COSA È L' "INTERNET DELLE COSE" ?	6
UNA NUOVA ERA PER L' ECONOMIA.....	9
RISCHI DELL' IoT	15
STATO DELL' IoT IN EUROPA, STATI UNITI E ASIA.....	19
CONCLUSIONI.....	21
CITAZIONI	22

Prefazione

Dr. Shawn DuBravac

è economista capo presso la Consumer Technology Association e autore del libro best seller nella lista del New York Times "Digital Destiny: How the New Age of Data Will Transform the Way We Work, Live, and Communicate".

Si può affermare con certezza che siamo all'inizio di una nuova rivoluzione industriale. L'avvento di macchinari e oggetti connessi a internet, fenomeno noto come "internet delle cose" (Internet of Things, IoT), farà concorrenza a meraviglie tecnologiche del passato come la macchina da stampa, il motore a vapore e l'elettricità. Dal mondo sviluppato a quello in via di sviluppo, ogni angolo del pianeta sperimenterà una profonda rinascita economica. Ancora più stupefacente, però, sarà la velocità con cui si verificherà questo cambiamento. Un decennio fa, i dispositivi connessi a internet erano circa 500 milioni. Oggi, il numero va dai 10 ai 20 miliardi. Fra cinque anni, potrebbero essere dai 40 ai 50 miliardi.

A differenza delle precedenti rivoluzioni industriali, però, siamo in grado di prevedere questo cambiamento. L'IoT non è costituito da una sola, colossale invenzione come accadde, ad esempio, per la sgranatrice di cotone. I settori industriali non verranno colti impreparati da un congegno migliore che rende obsoleti i loro sistemi di produzione e i loro prodotti. Infatti, tutti i settori e le singole aziende trarranno benefici e prospereranno grazie all'implementazione di oggetti IoT all'interno del proprio modello aziendale e, di conseguenza, scopriranno modi nuovi e migliori per fare affari. Il che non significa, però, che non ci saranno problemi o un rischio consistente. Man mano che si fanno strada nuovi settori e i vecchi modelli perdono sempre più terreno, le aziende dovranno confrontarsi con un contesto economico e di rischio completamente nuovo. Tuttavia, il fenomeno IoT è unico, in quanto consente alle aziende più proiettate verso il futuro di preparare, adattare e minimizzare il rischio in questa nuova epoca economica.

L'avvento dell'IoT, inoltre, significa anche che siamo all'inizio di una nuova era di dati. I due componenti principali di un "oggetto IoT" sono la capacità di catturare dati tramite sensori e di trasmetterli attraverso internet. Come questo white paper dimostra, il calo nel prezzo dei sensori a partire dall'inizio del nuovo millennio è stato uno dei volani principali nella crescita dell'IoT. Per farla breve, i sensori al giorno d'oggi hanno prezzi irrisori. Questo ci ha permesso di catturare quantitativi enormi di dati che, in passato, erano fuori dalla nostra portata.

Secondo l'organizzazione di ricerca norvegese SINTEF, il 90% dei dati al mondo è stato generato negli ultimi due anni. Ogni secondo, vengono creati oltre 205.000 nuovi gigabyte, ossia l'equivalente di 150 milioni di libri. Questo è il quantitativo di dati che viene generato in un mondo che presenta da 10 a 20 miliardi di oggetti connessi e dotati di sensori. Il mondo sta producendo più dati che mai e, cosa ancora più importante, noi spostiamo questi dati e li utilizziamo con sempre più frequenza. Pensiamo quindi a un mondo che abbia dai 40 ai 50 miliardi di oggetti IoT.

L'efficacia con cui un settore o una singola azienda utilizza il notevole afflusso di dati creato dagli oggetti IoT ne determinerà in maniera significativa il vantaggio concorrenziale e il successo futuro. In un modo o nell'altro, tutte le organizzazioni dovranno assumere un approccio e una mentalità incentrati sui dati. Saranno i dati a informare il responsabile di una catena di fornitura in merito alle inefficienze o ai problemi di sicurezza presenti nella catena stessa. Saranno i dati a comunicare all'operatore di mercato se i consumatori stanno rispondendo come previsto alla campagna più recente. E, infine, saranno i dati che offriranno alle aziende una consapevolezza più profonda che mai rispetto ai propri processi e prodotti.

Il settore delle assicurazioni si trova al centro di questa nuova rivoluzione industriale e dei dati. Di certo, le compagnie assicurative multinazionali utilizzano da decenni quantitativi incredibili di dati per comprendere e mitigare il rischio. Man mano che gli oggetti IoT permeeranno tutti i livelli dell'economia globale, le compagnie assicurative si troveranno in una posizione ideale per analizzare questi dati ed estrarre prospettive significative e concrete, prospettive che potrebbero rendere il mondo un luogo più sicuro e produttivo di quanto avremmo mai potuto immaginare.

Dott. Carlo Ratti, direttore
MIT SENSEable City Lab e
curatore del Future Food District
all'Expo Milano 2015.

Per decenni siamo stati impressionati da gadget nuovi e migliori. Computer migliori, lettori di musica migliori, televisori migliori e telefoni migliori. Questo trend ha fatto sembrare la tecnologia una lunga serie di congegni miracolosi mai vista prima d'ora. Potremmo aspettarci che continui, che troveremo la prossima tecnologia rivoluzionaria in un altro contenitore di plastica o metallo. Ma potrebbe non essere così.

Infatti, c'è un'altra rivoluzione tecnologica alle porte, ma è molto più semplice e al contempo potenzialmente più innovativa di qualsiasi singolo dispositivo. È una rivoluzione basata sui dati che potrebbe cancellare molte inefficienze, seccature, pericoli e prassi pericolose della vita moderna. Il settore assicurativo globale promette di giocare un ruolo fondamentale al centro di questa rivoluzione tecnologica.

Chiamata "Internet delle Cose" o "Internet del Tutto", tale trasformazione ha a che fare con il lento ma inesorabile aumento di oggetti connessi e dotati di sensori: in breve, la digitalizzazione online del nostro mondo fisico. Oggetti autonomi possono costantemente acquisire, analizzare e trasmettere quantità di dati acquisiti dalle aree circostanti. A loro volta, economie, città, imprese e persone risponderanno a questo flusso di informazioni, aprendo una serie di opportunità senza precedenti.

L'Internet delle Cose sta generando reti digitali pervasive nello spazio fisico: la linfa vitale in rete della "smart city". Non solo una rete di servizi comunali, quali elettricità e acqua, le vere città "intelligenti" combineranno elementi di tutte le parti interessate urbane, quali cittadini, governo e imprese. E, ancora una volta, un ampio spettro di modelli di implementazione sta emergendo in diverse parti del mondo.

Negli Stati Uniti, l'idea generale di spazio urbano intelligente è stata al centro dell'attuale generazione di start-up di successo. La progettazione stessa ha un impatto positivo nel rivoluzionare la maggior parte degli aspetti della vita urbana: dal pendolarismo al consumo energetico e alla salute personale. Queste nuove iniziative stanno ricevendo un forte supporto dai fondi di venture capital.

In Sud America, Asia ed Europa, tutti i livelli di governo stanno identificando i potenziali vantaggi di costruire città "intelligenti" e stanno lavorando per sbloccare investimenti significativi in quell'area. Rio de Janeiro sta sviluppando capacità nel suo centro "Smart Operations"; Singapore si sta per imbarcare in un impegno ambizioso, la "Smart Nation"; il programma Horizon 2020 dell'Unione Europea ha stanziato 15 miliardi di dollari nel periodo 2014-2016 – un impegno significativo di risorse per il concept di città intelligente, specialmente in un momento di vincoli fiscali.

Il futuro mostrerà come si evolveranno i diversi modelli esposti sopra. Nel frattempo, non c'è alcun dubbio che il settore assicurativo globale abbia la possibilità di giocare un ruolo da protagonista. Come valuteremo i rischi associati al territorio inesplorato dell'Internet delle Cose? Come possiamo comprendere le sfide che potrebbero scatenare spostamenti fondamentali nella responsabilità e nella gestione dei rischi attualmente noti? E dove possono portare gli assicuratori: non solo nell'interesse del loro settore, ma per fornire una guida ad altri settori, governi e, soprattutto, cittadini.

Prospetto riassuntivo

Secondo gli analisti di settore, a oggi sono connesse a Internet tra 10 e 20 miliardi di entità. Questo ecosistema di oggetti connessi forma la base dell'“Internet delle Cose” (Internet of Things, IoT). Nonostante la tecnologia che forma l'IoT sia disponibile da anni, oggi siamo solo all'inizio del suo sviluppo. Il numero di oggetti attualmente connessi è solo una parte ridotta del valore previsto tra soli cinque anni. Le stime variano, ma nel 2020 sono previsti tra 40 e 50 miliardi di oggetti connessi; e comprende oggetti di qualsiasi genere, dalle tazze alle penne, fino a case, automobili e apparecchiature industriali.

L'IoT offre incredibili nuove opportunità di fare affari, molte delle quali risultano incomprensibili ai non esperti. I media scelgono di concentrare la propria attenzione sul lato consumer dell'IoT, ad esempio sul mercato dei dispositivi indossabili. È indubbio che questi prodotti occupano una posizione prominente nell'universo dell'IoT, tuttavia essi rappresentano un settore di nicchia. Le attività che non fanno parte del mercato consumer possono essere erroneamente indotte a creare che l'IoT non abbia nulla da offrire loro. Tuttavia, indipendentemente dal settore, le implicazioni che l'IoT avrà a tutti i livelli delle operazioni aziendali andranno dal mondano al profondo. Problemi che hanno afflitto le attività per secoli diminuiranno drasticamente, in molti casi scomparendo del tutto. Abbinato ad altri sviluppi tecnologici come il cloud computing, le smart grid, le nanotecnologie e la robotica, il mondo dell'IoT in cui stiamo per entrare rappresenta un passo gigantesco verso una maggiore efficienza di economia, produttività, sicurezza e utili.

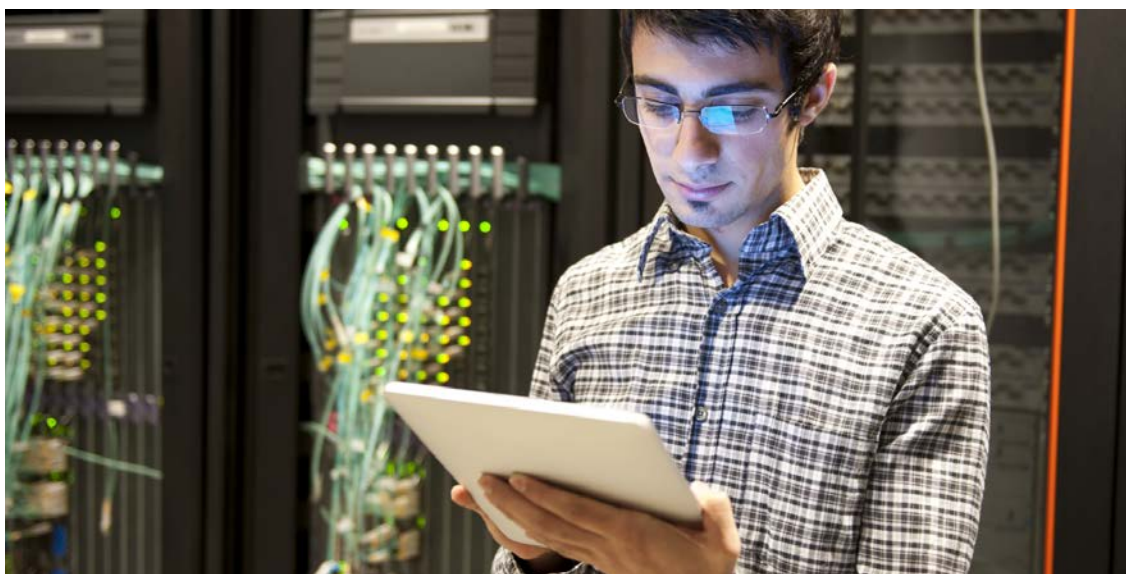
Secondo uno studio di RAND Europe, per il 2020 le maggiori valutazioni del potenziale economico globale annuo dell'IoT in tutti i settori interessati passerà da 1,4 trilioni di USD (circa 1,09 trilioni di €) a 14,4 trilioni di USD (circa 11,2 trilioni di €), pari all'incirca al PIL attuale dell'Unione europea. In effetti per allora l'IoT non sarà più un segmento isolato del mondo dell'IT, ma la forza propulsiva alla base di molte attività economiche a livello mondiale. Tra cinque anni, saranno rari i settori che non passeranno all'IoT. Già oggi sono rimasti pochi quelli che non traggono alcun guadagno dall'uso di oggetti IoT nei propri processi o prodotti. Inoltre vi sono svariati settori all'avanguardia in cui l'IoT è diventata indispensabile per le operazioni. Come vedremo, questi settori aiutano a fare luce sulle promesse dell'IoT nei prossimi anni.

Tali opportunità comportano tuttavia qualche rischio, e nel mondo dell'IoT i rischi hanno la stessa importanza dei risultati ottenuti. Dalle violazioni informatiche alle controverse questioni riguardanti proprietà e responsabilità sui prodotti, le attività non possono permettersi di entrare impreparate in questo nuovo mondo tecnologico. Ad esempio, ogni oggetto che si connette a Internet è un altro punto di accesso attraverso il quale i criminali informatici possono accedere al sistema aziendale di un'attività. In un mondo in cui le macchine sostituiscono gli esseri umani nel processo decisionale e i sensori rilevano continuamente dati, ugualmente pericolosi sono i gravi problemi di responsabilità, danni fisici e privacy che si presentano.

Lo scopo di questa serie di White Paper è informare i lettori delle opportunità e dei potenziali rischi dell'IoT. Anche se non possiamo dire con certezza cosa attende le attività tra cinque anni, possiamo predire i problemi che diventeranno importanti. Un mondo di IoT comporta una crescente complessità economica e a lungo termine l'infrastruttura che settori e governi hanno adottato per promuovere la crescita e la competizione risulterà inadatta. L'IoT avrà effetto su ogni paese ed economia del pianeta, anche nel mondo in via di sviluppo cui sono storicamente stati negati i benefici del progresso tecnologico. Come Dr. Shawn DuBravac capo economista della Consumer Technology Association di Arlington, Va., sostiene nel suo best-seller "Digital Destiny: How the New Age of Data Will Transform the Way We Work, Live, and Communicate":

**Questo non è ciò che potrebbe accadere se scegliessimo questa strada rispetto a un'altra.
Questo è ciò che accadrà indipendentemente da quale strada prendiamo.**

Per realizzare completamente il grande potenziale dell'IoT, le attività dovranno essere preparate ai rischi che si troveranno ad affrontare. Il settore assicurativo è particolarmente bene posizionato per aiutare le attività a navigare in questo nuovo mondo tecnologico. Infatti molti degli elementi che si sono uniti nell'IoT sono utilizzati da molto tempo dagli assicuratori per comprendere meglio i rischi e migliorare la sicurezza. Inoltre, così come le assicurazioni aiutano le altre attività ad adattarsi, esse si adatteranno in modo da migliorare i propri processi e le proprie funzioni base.



Che cosa è l'“Internet delle Cose”?

Il termine “Internet delle Cose” non è nuovo. È stato coniato nell'ormai lontano 1999 dal pioniere della tecnologia inglese Kevin Ashton, il quale al tempo lavorava come vicedirettore marchio presso Procter & Gamble. Nel 2007, Ashton estese il concetto in un articolo:

“Se avessimo computer in grado di conoscere tutto ciò che c'è da sapere sulle cose, utilizzando dati raccolti senza alcun aiuto da parte nostra, saremmo in grado di monitorare e conteggiare ogni cosa e di ridurre notevolmente sprechi, perdite e costi. Potremmo sapere quando le cose devono essere sostituite, riparate o richiamate, e se sono fresche o hanno superato il loro momento migliore.

“Dobbiamo mettere i computer in condizione di raccogliere informazioni con mezzi propri, in modo che possano vedere, sentire e odorare da sé il mondo in tutto il suo casuale splendore. Le tecnologie RFID e dei sensori consentono ai computer di osservare, identificare e comprendere il mondo senza le limitazioni dei dati inseriti dagli esseri umani.”ⁱ

In seguito, nel 2012, Rand Europe cercò di definire ulteriormente l'“Internet delle Cose” in un rapporto di ricerca per la Commissione europea. Il rapporto affermava che:

“L'Internet delle Cose si basa sull'Internet odierna attraverso la creazione di un network molto diffuso e organizzato in modo autonomo di oggetti fisici connessi, identificabili e indirizzabili che permettono lo sviluppo di applicazioni in e tra settori verticali chiave mediante l'uso di chip, sensori, attuatori e miniaturizzazione low-cost incorporati ”.ⁱⁱ

Le definizioni di Ashton e di RAND sono entrambe vere. Tuttavia la versione di RAND prende il concetto originale di Ashton di “computer abilitati” e lo estende per includervi gli “oggetti fisici”. In altre parole, per esistere l'“Internet delle Cose” non si basa principalmente sui computer, ma ogni oggetto può diventare una parte dell'IoT se dotato di specifiche parti elettroniche, compreso il corpo umano. Ovviamente queste parti variano a seconda della funzione che l'oggetto deve svolgere, ma rientrano tutte in due ampie categorie: 1.) L'oggetto deve essere in grado di rilevare dati, in genere tramite sensori; e 2.) L'oggetto deve essere in grado di trasmettere tali dati a un'altra ubicazione attraverso Internet. Di conseguenza, sensore e connessione sono le due “parti” elettroniche principali di un oggetto IoT.



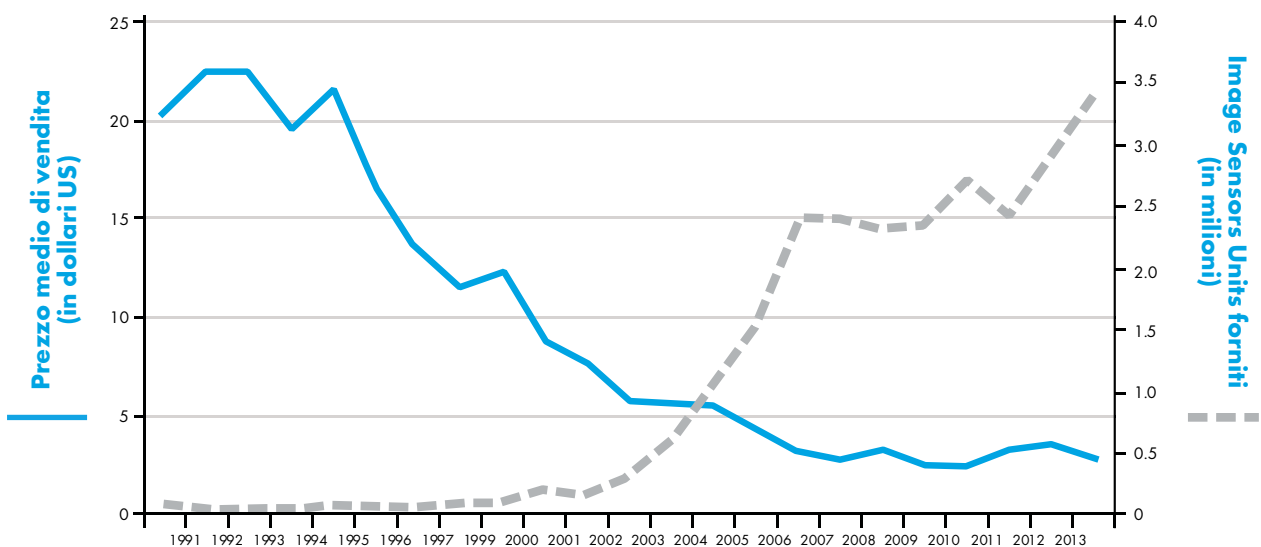
Nonostante questa tecnologia esista da oltre dieci anni, due sviluppi degli ultimi vent'anni sono il motore primario alla base dell'emersione dell'IoT come fenomeno in grado di modificare i paradigmi. Il primo è la crescita esplosiva del numero di dispositivi e applicazioni mobili e l'ampia disponibilità della connettività wireless.

Un rapporto di Cisco del 2011 faceva notare che nel 2003 erano connessi a Internet circa 500 milioni di dispositivi, quasi tutti personal computer. Dividendo il numero di dispositivi connessi per la popolazione mondiale, allora di 6,3 miliardi di

persone, vi era meno di un dispositivo (0,08) per ogni persona sul pianetaⁱⁱⁱ. Entro il 2010, l'esplosione del mercato di smartphone e tablet ha portato il numero di dispositivi connessi a 12,5 miliardi, nonostante la popolazione mondiale sia aumentata solo fino a 6,8 miliardi. In soli sette anni, nel mondo il numero di dispositivi connessi per persona era aumentato del 2.250%, passando da 0,08 a 1,8. In Europa, dove è presente una delle maggiori penetrazioni di telefoni cellulari del mondo, vi sono 1,1 miliardi di abbonamenti mobili per una popolazione di circa 800 milioni di persone^{iv}. Ciò significa circa 1,3 abbonamenti mobili per persona o, in termini più chiari, che in Europa vi sono più abbonamenti mobili che persone.

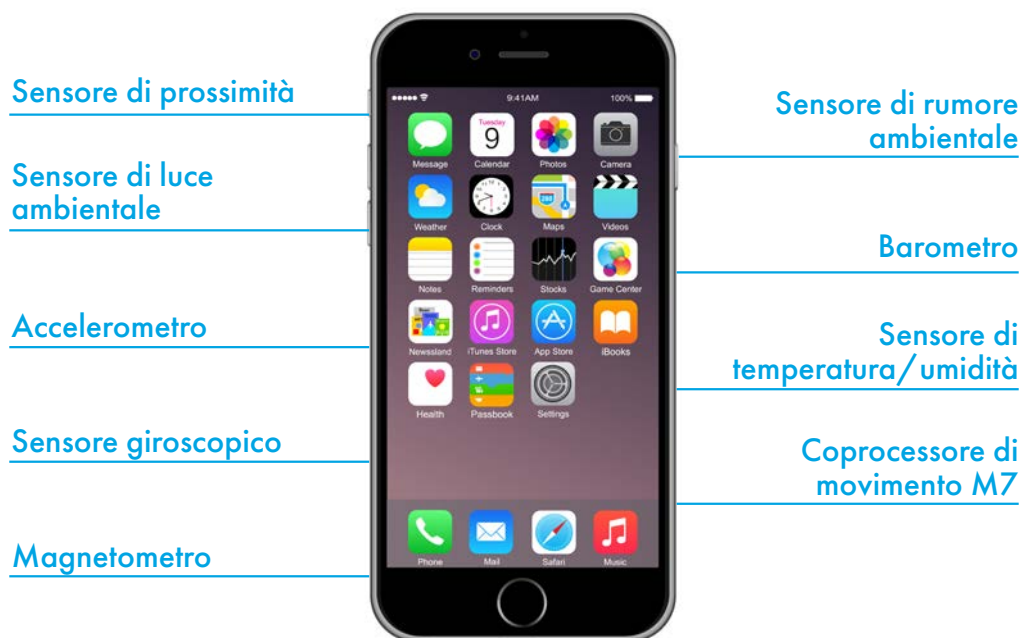
L'altro sviluppo risale ad ancora prima della tecnologia mobile: parliamo dei sensori. Tuttavia, per la maggior parte del XX secolo il costo elevato dei sensori ne ha limitato l'uso ai soli prodotti delle linee di punta. Agli inizi degli anni '90, i sensori di immagine a stato solido costavano da 20 a 25 USD. Alla fine del decennio il loro prezzo era sceso a 5 USD. Da ciò derivò una forte crescita del mercato delle fotocamere digitali. Anche gli altri sensori, ad esempio quelli presenti in un tipico smartphone, hanno seguito un percorso simile in termini di potenza e costo. Ad esempio, nel 2007 gli accelerometri che misuravano un singolo asse di movimento costavano circa 7 USD. Oggi, gli accelerometri che misurano sei assi di movimento costano meno di 0,50 USD.

Caduta dei prezzi decurtano volume di vendita



Fonte: DuBravac, Shawn. "Digital Destiny." P. 78

Naturalmente gli smartphone odierni non sarebbero altrettanto “smart” (intelligenti) senza tutti i sensori di cui sono dotati. A seconda del modello, possiamo trovarvi da un minimo di cinque a un massimo di nove sensori, tra cui:



Quindici anni fa l’inserimento di uno di questi sensori avrebbe fatto aumentare il costo di un prodotto oltre la portata del consumatore medio, figurarsi di nove. Oggi, il costo di tutti questi sensori non arriva in totale a 5,00 USD, con quelli più economici che costano solo 0,07 USD^v.

Tuttavia i sensori non si limitano a rendere possibili utili funzioni sui nostri telefoni cellulari. Infatti, essi sono l’ingrediente fondamentale che “fa muovere” l’IoT. Rilevando continuamente dati dell’ambiente circostante, un sensore sostituisce l’essere umano come modo primario attraverso cui un computer riceve dati. Ma poiché possono rilevare dati a velocità e in quantità che nessun essere umano potrà mai uguagliare, i sensori hanno portato al fenomeno chiamato Big Data, termine che indica l’acquisizione e l’analisi di gruppi di dati estremamente grandi.

Che cosa sono questi dati? Sono tutto ciò che ci circonda, di qualsiasi tipo esso sia. In termini più pratici, i dati che i sensori odierni sono in grado di acquisire (come gli esseri umani non possono fare) stanno rivoluzionando l’economia e i processi aziendali. Infatti, i produttori di automobili di tutto il mondo utilizzano i sensori non solo nelle proprie auto, ma anche negli impianti di produzione, in cui assistono macchine autonome oltre a migliorare la sicurezza dei lavoratori.

Tra gli altri fattori che hanno contribuito all’IoT, in particolare in un contesto aziendale e industriale, vi sono l’archiviazione su cloud a costi convenienti e la crescita dell’analisi dei dati che permette alle organizzazioni di trattare ed estrarre informazioni da grandi quantità di dati^{vi}. Tuttavia non ci si discosta mai molto dai due fattori principali. Si tratta sempre di un sensore che rileva i dati e la connettività mobile che li trasmette a un altro dispositivo o al cloud.

Dobbiamo ricordare che l'IoT non è un fenomeno semplice e facilmente definibile. Esiste un gran numero di segmenti e mercati che formano l'IoT. Per il consumatore, IoT significa tecnologia indossabile e apparati "smart", come termostati e televisioni. Nel settore industriale, IoT significa macchine autonome e apparecchiature dotate di sensori. Nello spazio commerciale, IoT significa Big Data e analisi di marketing. In breve, dalla produzione ai prodotti di consumo, l'IoT è varia come l'economia globale stessa.

La domanda quindi diventa: come possono le attività utilizzare questi oggetti connessi per migliorare i propri processi, aumentare la produttività, ridurre i costi ed evitare i rischi?

Una nuova era per l'economia

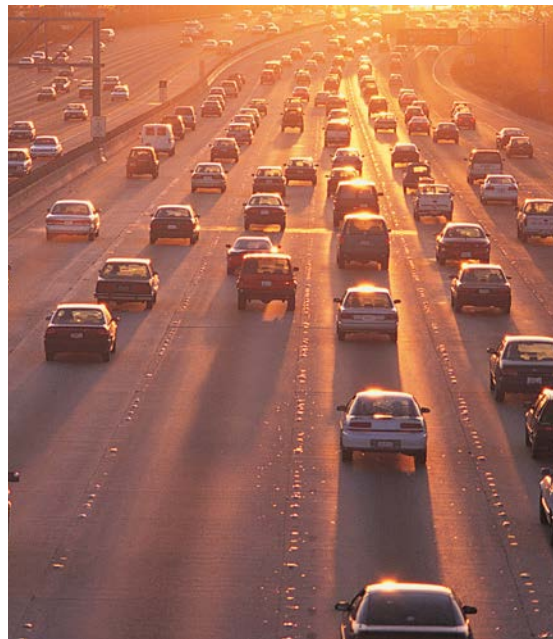
Per apprezzare le opportunità che l'IoT offre alle attività, iniziamo comprendendo il suo impatto a livello macroeconomico. In un documento di politica per la Commissione europea, RAND Europe pone le stime più elevate del potenziale economico dell'IoT da 1,4 trilioni di USD l'anno (circa 1.09 trilioni di €) a 14,4 trilioni di USD (circa 11.2 trilioni di €) tra tutti i settori a livello globale^{vii}. Inoltre, nel 2020 la vendita di dispositivi e servizi connessi arriverà a circa 2,5 trilioni di USD, mentre gli investimenti accumulati indicati per la connessione di miliardi di dispositivi connessi raggiungerà almeno i 2 trilioni di € a prezzi attuali. Ad esempio, lo studio di RAND fa notare che la Cina ha già accantonato 625 milioni di € (775 milioni di USD) per investimenti nell'IoT^{viii}.

È certo che tra cinque anni non vi sarà alcun settore su cui l'IoT non avrà effetti diretti. Il ritmo di adozione combinato con le aspettative e le richieste dei consumatori trasformerà rapidamente qualsiasi industria non-IoT in una reliquia da museo, per non parlare delle aziende individuali. Detto ciò, molti settori hanno tempo per comprendere l'IoT e dove questo può migliorare i loro obiettivi strategici a lungo termine. Come primo capitolo di questa serie, questo White Paper intende fornire ai lettori esempi attuali del modo in cui alcuni settori hanno iniziato a utilizzare l'IoT. La nostra speranza è che i lettori siano in grado di iniziare ad implementare una strategia per le proprie attività basata sugli esempi forniti di seguito. Dal momento che l'IoT ha impieghi che coprono l'intero spettro delle attività umane, abbiamo diviso in quattro categorie il modo in cui ogni settore utilizza l'IoT:

**Sicurezza, Efficienza,
Processo decisionale guidato
dai dati e Infrastruttura.**

SETTORE AUTOMOBILISTICO

Sicurezza: Nel 2010, l'Organizzazione Mondiale della Sanità ha comunicato che 1,24 milioni di persone nel mondo è deceduta in conseguenza di incidenti con veicoli a motore^{ix}. Ogni anno, in Europa circa 30.000 persone rimangono uccise in incidenti automobilistici^x. Un valore molto simile si presenta anche negli Stati Uniti. In Asia il problema è di gran lunga più grave. Solo in Cina e India, ogni anno muoiono in incidenti automobilistici più di 400.000 persone^{xi}. La tecnologia IoT, in particolare la crescita di sensori dedicati alla sicurezza sulle automobili, promette di ridurre drasticamente il tasso globale di decessi causati da incidenti automobilistici. Poiché gran parte degli incidenti automobilistici sono dovuti a errori umani, lo scopo dei veicoli autonomi è sostituire la componente decisionale umana nella guida.



A maggio 2015, Daimler Trucks North America (una società di proprietà tedesca con sede negli Stati Uniti) ha annunciato di essere pronta a testare il suo Freightliner Inspiration Truck senza conducente sulle strade del Nevada^{xii}. Tuttavia le auto senza conducente, quali quelle in fase di sviluppo da parte di società come Google^{xiii} e Tesla^{xiv}, stanno appearing lentamente. Molte di queste sono sotto forma di sensori di sicurezza che danno all'automobilista una vista a 360 gradi della propria auto, mentre altre lavorano in modo autonomo proteggendo l'auto senza alcuna azione diretta da parte del conducente. Le società produttrici di automobili utilizzano i dati acquisiti da questi sensori anche per produrre automobili più sicure ed efficienti. Anche se comportano qualche preoccupazione per la privacy, questi dispositivi di raccolta dati sono il prossimo passo nell'evoluzione delle auto.

SETTORE BANCARIO

Efficienza: Il settore finanziario ha avuto un ruolo di pioniere nell'uso della tecnologia mobile per facilitare le operazioni bancarie al consumatore medio. Un esempio evidente in cui l'IoT e il settore bancario si incontrano sono gli sportelli Bancomat, i quali possono essere dotati di tecnologia basata sull'uso di sensori. Un utente con dati identificativi biometrici corretti potrà un giorno prelevare del denaro da un Bancomat dotato di appositi sensori senza dover più estrarre di tasca la propria carta. In prospettiva futura, l'IoT promette di collegare le attività finanziarie di un consumatore con altri aspetti della sua vita. Un esempio è il collegamento del monitor sanitario dell'utente con il suo portafoglio finanziario. Come ha fatto notare Deloitte, un problema di salute rilevato dal monitor potrebbe segnalare alla banca dell'utente di riequilibrare automaticamente il suo portafoglio per minimizzare la sua esposizione finanziaria^{xv}.

In un rapporto del 2014 sulla "Banca delle Cose", Accenture faceva notare che: "La Banca delle Cose anticiperà le esigenze dei clienti e risponderà alle variazioni delle circostanze, offrendo soluzioni tempestive e pertinenti in grado di aiutarli a raggiungere i propri obiettivi. La banca rimarrà per i propri clienti un consigliere di fiducia, un facilitatore e un aggregatore di valore, ma lo farà con una comprensione quasi intima delle necessità e delle preferenze di ogni cliente."^{xvi}

SETTORE MARINO

Sicurezza: Come nella maggior parte del settore dei trasporti, per decenni le società di spedizioni marittime hanno dotato le proprie flotte di un grande numero di sensori con il compito di monitorare sistemi di bordo critici, condizioni meteo e del mare e carico. Oggi la tecnologia IoT consente a questi sensori di acquisire dati che possono quindi essere analizzati per migliorare l'ottimizzazione della rotta, la sicurezza e i processi di stivaggio.

Ad esempio, un software open source impiega i sensori di bordo per fornire informazioni in tempo reale sul movimento della nave ad altre imbarcazioni e ai centri di coordinamento del traffico marittimo a terra. Il software IoT "supporta un processo decisionale collaborativo tra le principali parti interessate coinvolte per garantire operazioni marittime più sicure, efficienti e sostenibili per l'ambiente", ha affermato un esperto^{xvii}.

Processo decisionale guidato dai dati: All'International CES 2015, la società svedese Ericsson ha presentato una soluzione IoT avanzata per i trasporti marittimi. La piattaforma basata sul cloud può collegare le navi in mare con "operazioni basate a terra, fornitori di servizi di manutenzione, centri di assistenza clienti, partner di flotta/trasporto, operazioni portuali e autorità". La soluzione può consentire agli operatori in mare e a terra di monitorare consumo di carburante, prestazioni dei motori, condizioni meteo, traffico e navigazione per ottimizzare la rotta, tracciare posizione e condizioni di carichi specifici e, mediante comunicazioni migliorate, opzioni di intrattenimento e telemedicina, aumentare anche il benessere dell'equipaggio della nave^{xviii}.

PROPRIETÀ IMMOBILIARI

Efficienza: A livello di immobili, esistono già oggetti "smart" come termostati e altri apparati che aiutano i proprietari a migliorare l'efficienza energetica e ridurre i costi dei consumi. È possibile prevedere che questi prodotti prolifereranno mentre le case diventeranno sempre più "connesse". Tuttavia il valore reale dell'IoT nelle case si presenterà quando questi apparati connessi e altri oggetti domestici comunicheranno tra loro. Ad esempio il termostato intelligente di una casa conosce la temperatura esterna e comunica questi dati al sistema di armadi di casa, il quale suggerisce gli abiti più adatti alla giornata. Un altro esempio è un sistema di casa, anche in questo caso un armadio, che si sincronizza con l'agenda di un utente. In questo modo l'armadio "sa" se quel giorno l'utente ha una riunione e sceglie l'abito appropriato.

Processo decisionale guidato dai dati: Nel settore immobiliare, una casa dotata di sistemi IoT può arrivare anche a prendere il posto di un agente umano. Essa può inserirsi autonomamente negli elenchi delle proprietà in vendita e pianificare le visite, poiché "sa" quando i proprietari saranno fuori^{xix}. Alcune società di mediazione stanno già sperimentando la tecnologia e gli avvisi "In vendita" iBeacon^{xx} di Apple. Il concetto prevede che il potenziale acquirente che passa in prossimità della casa in vendita riceva da iBeacon un messaggio sul proprio smartphone che fornisce istantaneamente i dettagli relativi alla proprietà. All'interno della casa, la tecnologia iBeacon può essere utilizzata per offrire ai potenziali acquirenti planimetrie, testimonianze video del proprietario precedente e persino proposte di ristrutturazione, ad esempio in collaborazione con un negozio di fai da te e ferramenta^{xxi}.

Infrastructure: Tra i rischi che ogni attività deve accettare vi sono inondazioni, incendi e decadimento strutturale. Tuttavia, la tecnologia IoT, in particolare i sensori incorporati in specifiche aree di rischio, possono aiutare e diminuire e in alcuni casi eliminare questi problemi. Ad esempio, i sistemi elettrici possono essere dotati di sensori che monitorano il flusso di elettricità attraverso un edificio. Quando un cavo o un collegamento subiscono un danno o stanno per avere un malfunzionamento con conseguente aumento della probabilità di incendio, i sensori possono avvisare immediatamente i tecnici. Le società immobiliari possono utilizzare i sensori IoT nelle loro proprietà per monitorare un'ampia gamma di incidenti legati a rischi, tra cui la presenza di gas pericolosi, le infestazioni di termiti, i malfunzionamenti di sistemi HVAC/caldaie e lo stato di usura generale. Anche quando una particolare struttura sembra essere in condizioni perfette, gli analisti possono esaminare l'enorme quantità di dati raccolti da questi sensori incorporati per trovare indizi di problemi futuri.



ENERGIA

Efficienza: Il settore dell'energia fa già un grande uso della tecnologia IoT. A livello di consumatore, gli utenti possono utilizzare apparati avanzati e dispositivi "smart" per ridurre l'uso di energia e i relativi costi. Anche le aziende possono utilizzare queste tecnologie, ma a un livello molto più avanzato. Ad esempio, un palazzo di uffici con più inquilini può rilevare e monitorare l'uso di energia di ciascun piano. Analizzando i dati, l'edificio può identificare le aree in cui si verificano sprechi di energia e tagliare i costi.

Nel frattempo, il settore dell'energia è da tempo all'avanguardia della tecnologia IoT, principalmente con società di servizi che introducono modi innovativi di leggere da remoto i consumi di energia di clienti commerciali, industriali e residenziali. Infatti, secondo Ericsson, dal 2013 al 2020 si prevede una crescita da 485 milioni a 1,53 miliardi nel numero di dispositivi connessi che vengono gestiti da società di servizi a livello globale. In effetti, il settore dei servizi è la seconda fonte di fatturato per i fornitori di servizi "machine-to-machine", subito dietro al settore automobilistico e dei trasporti. "Questi dispositivi possono andare da contatori, sensori di griglia e attuatori a quadri e apparati elettrici. Questi dispositivi sono utilizzati per applicazioni come monitoraggio e controllo della griglia, misurazione dei consumi, gestione e traccia delle risorse e comunicazione con la forza lavoro sul campo", afferma Ericsson^{xxii}.



APPLICAZIONI AEROSPAZIALI

Sicurezza: I sistemi “fly-by-wire” sono da decenni un caposaldo del settore aerospaziale. In parole povere, i sistemi “fly-by-wire” consentono al pilota di concentrare l’attenzione sul monitoraggio del velivolo, mentre sensori e sistemi automatizzati si prendono cura del resto. Infatti, i sistemi “fly-by-wire” stanno diventando così avanzati che per molti aspetti gli aeroplani sono mezzi pressoché autonomi. Ad esempio, quando capitano Chesley B. “Sully” Sullenberger fece un ammaraggio di emergenza nel fiume Hudson pochi minuti dopo il

decollo dall’aeroporto LaGuardia di New York, stava pilotando un Airbus A320, sui cui primi modelli era stato introdotto l’uso di sistemi “fly-by-wire” digitali. Senza sminuire il capitano Sullenberger, possiamo affermare che il “Miracolo sull’Hudson” sarebbe stata una tragedia senza gli avanzati sensori del velivolo che gli hanno permesso di concentrarsi su come posare l’aereo sul fiume in sicurezza^{xxiii}.

Efficienza: A terra, le società aerospaziali stanno impiegando la tecnologia IoT per migliorare la manutenzione e le misure di sicurezza. Ad esempio, l’attività di manutenzione dei motori per aeroplani di General Electric utilizza sensori montati sui motori a getto per rilevare dati in tempo reale sulle loro prestazioni. Il volume di dati prodotto da questo processo consente a GE di migliorare l’efficienza dei motori, ridurre i consumi di carburante e abbreviare i tempi di viaggio^{xxiv}.

SANITÀ

Processo decisionale guidato dai dati: Non esiste alcun settore della sanità che non impieghi o stia per impiegare la tecnologia IoT. A livello di paziente, i dispositivi indossabili con tecnologia IoT consentono ai medici di rilevare i dati sanitari che altrimenti rimarrebbero ignoti. Gli esami medici annuali potrebbero diventare obsoleti, poiché i medici dispongono già di grandi quantità di dati sui singoli pazienti che indicano se è necessario un check-up di persona. Similmente, i pazienti con condizioni di salute problematiche che potrebbero non presentare sintomi sarebbero rilevati dal medico prima che insorgano problemi più gravi. I medici possono utilizzare questi dati non solo per comprendere meglio la salute del singolo paziente, ma anche per creare insiemi di dati dettagliati di sottogruppi di pazienti, con l’obiettivo di curare e prevenire le patologie più antiche dell’umanità.

Nel frattempo gli ospedali, i quali producono e archiviano da sempre enormi quantità di dati, possono impiegare la tecnologia IoT per trovare informazioni utili nei dati raccolti. Ad esempio, molti ospedali acquistano intenzionalmente quantità di farmaci superiori alle normali esigenze per evitare carenze nelle forniture critiche. Gli scanner dotati di tecnologia IoT permettono agli amministratori ospedalieri di conoscere le scorte e di sapere quando si verificheranno tali carenze. Inoltre, i dispositivi IoT possono migliorare notevolmente le cure ospedaliere, in particolare in situazioni di emergenza. I paramedici possono utilizzare i dispositivi IoT per rilevare i segni vitali dei pazienti e altri dati statistici che vengono quindi immediatamente trasmessi al pronto soccorso. Una volta arrivato il paziente, i medici non devono più perdere tempo prezioso per comprendere le condizioni del paziente, poiché queste sono già note.

PRODUZIONE

Sicurezza: L'IoT promette anche di ridurre notevolmente il tasso di infortuni e decessi sul posto di lavoro. Secondo l'Organizzazione internazionale del lavoro, a livello globale ogni anno 2,3 milioni di persone muoiono per incidenti e malattie dovute al lavoro^{xxv}. Secondo la Commissione europea, ogni anno più di tre milioni di lavoratori sono vittima di incidenti gravi sul lavoro, e 4.000 muoiono in incidenti sul posto di lavoro^{xxvi}. L'IoT può aiutare a garantire la sicurezza dei dipendenti, in particolare di quelli che lavorano da soli in aree pericolose come i cantieri edili. Ad esempio, la tecnologia indossabile può essere dotata di sensori incorporati in grado di stabilire quando un lavoratore può mettersi in condizioni pericolose o svolgere una manovra insicura. I sensori possono anche monitorare condizioni ambientali pericolose, come ad esempio temperature estreme e presenza di sostanze tossiche. Inoltre, i dati comportamentali raccolti da questi sensori indossabili possono aiutare i responsabili della sicurezza a comprendere quando un lavoratore è esposto alla probabilità di avere un incidente. Anche se per molti versi ancora teorico, questo elemento premonitore dell'IoT è una delle sue funzioni più interessanti (oltre che potenzialmente sfruttabili).

Processo decisionale guidato dai dati: Le società possono anche utilizzare i prodotti IoT per garantire integrità e sicurezza di qualità e componenti nelle proprie complesse catene di approvvigionamento. Gartner, Inc., una società di ricerca e consulenza del settore IT, stima che "entro il 2020, un aumento di 30 volte dei dispositivi fisici connessi a Internet modificherà significativamente l'accesso alle informazioni e l'esposizione ai rischi informatici per i leader delle catene di approvvigionamento"^{xxvii}. I dispositivi IoT incorporati nella catena di approvvigionamento daranno ai responsabili la più approfondita visione dei loro processi di sempre. Dalla visibilità delle merci in transito alla sicurezza dei magazzini, gli oggetti IoT promettono di rivoluzionare il modo in cui le società progettano, proteggono e gestiscono le proprie catene di approvvigionamento sensibili.

SETTORE ALIMENTARE

Efficienza: Le società di recapito offrono già ai consumatori la possibilità di tracciare i propri ordini imballati presso ogni stazione di trattamento, ma la tecnologia è di gran lunga più utile se applicata alle attività. Sensori IoT incorporati nel posto e al momento giusti possono aiutare le aziende a tracciare le proprie risorse in tempo reale. I dati raccolti possono consentire alle organizzazioni di identificare le inefficienze e i colli di bottiglia delle catene di approvvigionamento. Altrettanto importante, i sensori posti in strutture o mezzi di immagazzinamento, ad esempio su autocarri dotati di congelatore, possono avvisare una società quando il meccanismo refrigerante presenta un malfunzionamento o sta per guastarsi. Ciò toglie il compito del monitoraggio al conducente, il quale potrebbe non controllare la merce per svariate ore dopo il malfunzionamento dell'unità refrigerante, e dà alle organizzazioni la possibilità di preservare carichi preziosi impedendone il deterioramento. In agricoltura, i contadini possono impiegare la tecnologia IoT incorporata nei campi per monitorare informazioni critiche come l'utilizzo di acqua. Ad esempio, un sensore può informare l'agricoltore dove vi sono perdite nel sistema di sprinkler, oppure se sta utilizzando troppa acqua su un particolare appezzamento. In particolare, applicati al mondo in via di sviluppo, i miglioramenti dell'IoT in materia di produzione e distribuzione degli alimenti promettono di essere rivoluzionari.



Rischi dell'IoT

In effetti, le promesse e il potenziale della nuova era dell'IoT sono enormi. Per molti aspetti, le possibilità dell'IoT sono limitate solo dalla nostra immaginazione. In particolare, se consideriamo tutti i dati che non vengono registrati, tutti i pezzi di informazioni che ci scivolano tra le dita e come l'IoT ci permetterà infine di rilevare e utilizzare questi dati in un modo finora ignoto all'umanità, è facile ignorare il lato oscuro del nuovo mondo dell'IoT. Tuttavia le attività non possono permettersi di investire nei propri sistemi IoT senza prima comprendere i principali rischi insiti in qualsiasi sistema connesso a Internet. Dal giorno in cui abbiamo acceso il primo computer, sappiamo che la nostra fiducia nella tecnologia può condurre al disordine, grande e piccolo. Questa affermazione non ha lo scopo di scoraggiare le società dall'adottare l'IoT; le opportunità superano di gran lunga i rischi. Tuttavia ogni società deve comprendere che per ogni problema che l'IoT risolve, un altro viene creato. Ecco quattro dei maggiori rischi derivanti dall'adozione dell'IoT:

PRIVACY

Con miliardi di sensori sparsi nel mondo che acquisiscono costantemente dati da ciò che li circonda, compresi gli esseri umani, la preoccupazione per la privacy diventa fondamentale nel mondo dell'IoT. La maggior parte dei Paesi sviluppati ha tentato di proteggere i consumatori dall'uso illegale di informazioni riservate, ma in molti casi le leggi non sono in grado di gestire l'enorme numero di nuovi modi in cui le informazioni personali vengono rilevate e impiegate. Il recente tentativo dell'UE di aggiornare la legge sul copyright (vedere di seguito) è un sintomo della natura obsoleta di molte leggi dei Paesi sviluppati.



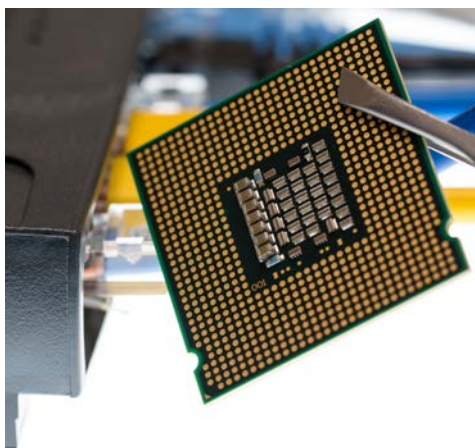
In una fase precedente di Internet, i consumatori hanno fatto la conoscenza, non sempre gradita, dei software di tracciatura altrimenti noti come cookie. Dal momento che non esiste alcuna legge specifica che limiti l'uso di cookie da parte di un sito Web per tracciare il comportamento dell'utente durante la navigazione, molte società ne hanno semplicemente adottato l'impiego senza preoccuparsi molto dell'opinione degli utenti. In effetti, i browser hanno reagito ai dubbi dei consumatori fornendo loro strumenti per limitare l'uso di cookie ed eliminarli dopo una sessione di navigazione. Oggi la legislazione dell'UE regola il modo in cui vengono usati i cookie e quale tipo di dati degli utenti possono raccogliere^{xxviii}, ma con la crescita della tecnologia mobile, la quale non necessita dei cookie per monitorare il comportamento dell'utente, molte di queste leggi stanno rapidamente diventando obsolete e inadeguate nel mondo dell'IoT.

Similmente, anche gli Stati Uniti si basano su modelli normativi vecchi per nuovi dispositivi e sistemi IoT. Tuttavia non esiste alcuna singola legge federale che regoli la raccolta e l'utilizzo di dati personali. Per proteggere la privacy dei consumatori, gli Stati Uniti si affidano invece a un misto di leggi federali e statali esistenti. Lo scalpore pubblico nei confronti del governo federale, in particolare della National Security Agency, per le attività di "data-mining" connesse all'applicazione della legge e alla lotta al terrorismo fanno presagire futuri dibattiti politici pubblici.

A gennaio 2015, la Federal Trade Commission statunitense ha rilasciato un rapporto sullo stato dell'IoT negli Stati Uniti e suggerito le "pratiche migliori" che le società devono seguire in materia di dati e sicurezza dei consumatori. Tuttavia, il rapporto dell'FTC prosegue la "linea morbida" del governo federale per quanto riguarda la regolamentazione di Internet, e pertanto dell'IoT. Ad esempio, il rapporto conclude "che in questo momento qualsiasi legge specifica per l'Internet delle Cose sarebbe prematura, alla luce della natura in rapido sviluppo della tecnologia. Il rapporto sottolinea tuttavia il ripetuto appello della Commissione per una forte legge sulla sicurezza dei dati e la segnalazione delle violazioni."^{xxix}

Le preoccupazioni per la privacy riguardano anche il posto di lavoro. Sul mercato esistono numerosi programmi che consentono ai datori di lavoro di monitorare il comportamento dei dipendenti, solitamente tramite i loro PC. Ma l'IoT consente ai datori di lavoro di posizionare sensori in pressoché ogni angolo dell'ufficio per monitorare le abitudini dei dipendenti. Ad esempio, in California una ex dirigente alle vendite ha avviato un'azione legale contro il datore di lavoro, sostenendo di essere stata forzata a scaricare sul proprio smartphone un'app di monitoraggio usata dal datore di lavoro per controllarla sia durante il lavoro, sia nel suo tempo libero^{xxx}. La capacità dell'IoT di monitorare e rilevare le azioni umane fa sorgere numerose domande etiche cui non è ancora stata data una risposta esauriente, come ad esempio:

- Un lavoratore può essere punito sulla base dei dati raccolti da un oggetto IoT?
- I datori di lavoro devono informare i propri dipendenti dei sensori che ne rilevano il comportamento?



SICUREZZA INFORMATICA

Oggi, le violazioni informatiche rappresentano una delle principali minacce per le attività. Secondo una stima, i reati informatici costano alle attività 400 miliardi di USD l'anno^{xxxi}. Dal punto di vista dell'IoT, la cosa più preoccupante è il fatto che i criminali informatici stanno violando sistemi apparentemente sicuri dotati di livelli di protezione multipli. La complessità di garantire la sicurezza dei dispositivi IoT è un'area di miglioramento per le attività, specialmente in vista del giorno in cui prenderà vita un "ecosistema IoT" in cui miliardi di oggetti saranno connessi a Internet e tra loro.

È necessario ricordare che qualsiasi dispositivo con una connessione a Internet è un potenziale punto di accesso per gli hacker. Ad esempio, nel 2014 un hacker è riuscito a violare un baby monitor per molestare una bambina di due anni. Una successiva ricerca sul prodotto, realizzato dalla società cinese Focsam, ha rilevato che 40.000 dei 46.000 dispositivi non erano stati aggiornati con una misura di sicurezza che avrebbe impedito la violazione.^{xxxii}

È necessario anche ricordare che più automatizziamo e connettiamo taluni sistemi, in particolare quelli industriali, più esposti questi saranno alle pratiche di hacking. Una città che realizza una griglia elettrica “smart” può ottenere forti risparmi grazie alla semplificazione delle procedure di risoluzione dei problemi dei sistemi. Al contempo, il sistema stesso offre a un potenziale hacker un facile modo per interrompere la fornitura di elettricità all’intera città dal proprio computer.

In un altro esempio, ad aprile 2015 il Government Accountability Office statunitense ha emesso un rapporto in cui si discutono le minacce legate all’aumentata interconnettività tra velivoli e sistemi di terra. Secondo il rapporto, “questa interconnessione può potenzialmente fornire un accesso remoto non autorizzato ai sistemi avionici dell’aeromobile”^{xxxiii}. In altre parole, un hacker-terrorista potrebbe impiegare il sistema per ottenere il controllo del velivolo.

A causa della natura in rete dell’IoT, in cui ad esempio ogni oggetto connesso utilizza dati provenienti da altri oggetti connessi, esiste anche il rischio che un guasto possa portare a un malfunzionamento catastrofico del sistema. Un oggetto malfunzionante può potenzialmente fornire dati errati a un altro dispositivo che funziona normalmente. Tuttavia, facendosi strada nel sistema, i dati errati iniziano a infettare un numero sempre maggiore di sistemi. Se consideriamo una calamità naturale, ad esempio un’alluvione, un malfunzionamento di sensori che monitorano l’integrità di dighe e argini può causare gravi danni alle proprietà o anche la perdita di vite umane.

Esempi come questi sottolineano i nuovi rischi che molte attività dovranno affrontare in relazione alla sicurezza informatica dell’IoT. Anche se è possibile prevedere che nel tempo i produttori di questi dispositivi migliorino le proprie misure di sicurezza, il numero totale degli oggetti connessi sta aumentando in modo esponenziale.

RESPONSABILITÀ

Quando si parla di veicoli autonomi, come le automobili senza conducente, ci si imbatte in un evidente dilemma etico: Nei secondi che precedono un incidente, un veicolo autonomo deve fare qualsiasi cosa possibile per proteggere i passeggeri anche ove ciò significhi danneggiare altri automobilisti o pedoni? Quando al volante si trova un essere umano, per tragici che siano, i danni collaterali non comportano grandi problemi etici. Un essere umano in pericolo non può essere criticato quando il suo istinto di sopravvivenza lo fa deviare mandandolo a investire un pedone. Ma quando le decisioni sono prese da una macchina, un pedone ferito in un incidente può fare causa al produttore dell’automobile? Il conducente può far causa al produttore dell’automobile dopo un incidente in cui ha subito delle lesioni? Come afferma il rapporto della Commissione europea sui dilemmi etici connessi alla tecnologia IoT, “le persone non sono abituate a oggetti che hanno un’identità o che agiscono autonomamente, in particolar modo se lo fanno in modi imprevedibili”^{xxxiv}.

Altri dubbi sulla responsabilità emergono quando si considera la proprietà dei dati. Con miliardi di dispositivi che raccolgono dati, i confini della responsabilità sui



dati si fanno confusi. Gli oggetti IoT operano in modo autonomo e insieme a numerosi altri. Prima di essere visti da un occhio umano, i dati vengono rapidamente condivisi, elaborati, ricondivisi e rielaborati. In altre parole, è troppo semplice associare un dispositivo a un blocco di dati, poiché gran parte del potenziale dell'IoT sta nel trasferimento senza ostacoli di questi dati tra oggetti differenti. Ad esempio, un monitor cardiaco IoT non si limita a monitorare il cuore di un paziente alla ricerca di segnali di allarme legati a un imminente attacco di cuore. Il dispositivo può accedere anche ai dati di un altro oggetto che traccia il programma di esercizio fisico seguito dal paziente, il quale a sua volta riceve dati da un dispositivo che monitora gli alimenti ingeriti. Se il paziente ha un attacco di cuore, chi è responsabile?

I dispositivi IoT fanno sorgere anche domande importanti in relazione ai loro possibili malfunzionamenti. I sensori possono essere incorporati in infrastrutture critiche come dighe, ponti e strade per monitorare l'integrità strutturale e le condizioni ambientali che potrebbero minarla. In una strada in prossimità di una zona allagata possono essere incorporati sensori che rilevano il momento in cui le piogge superano il livello che per gli ingegneri rappresenta un avviso avanzato di inondazione. Infatti, la protezione delle infrastrutture è uno degli aspetti più interessanti dell'IoT. Tuttavia quando affidiamo sempre più infrastrutture critiche e sistemi di sicurezza agli oggetti IoT, di contro ci esponiamo al rischio di una catastrofe se e quando tali oggetti smettono di funzionare.

Questo concetto può essere applicato anche al settore privato. Per citare un esempio non letale, ad aprile 2015 numerosi voli di American Airlines sono stati ritardati quando un malfunzionamento software ha reso inutilizzabili i tablet usati dai piloti per la navigazione^{xxxv}. Nonostante il malfunzionamento sia stato risolto facilmente con un aggiornamento software, gli esempi mostrano quanto siamo già esposti a causa dei nostri dispositivi connessi. Siamo pronti a reagire quando non funzionano?

Stato dell'IoT in Europa, Stati Uniti e Asia

EUROPA

Con i suoi elevati tassi di penetrazione dei dispositivi mobili, l'Europa è particolarmente adatta a sfruttare l'imminente rivoluzione dell'IoT. Tuttavia, nonostante l'inevitabilità dell'IoT, per le singole economie rimangono degli ostacoli da superare per realizzare il pieno potenziale dell'IoT. Un ostacolo è la semplice concorrenza. Ad esempio, durante una conferenza della Commissione europea tenutasi a marzo 2015 a Bruxelles, i rappresentanti europei di industria pesante, produttori di automobili ed elettrodomestici, aziende delle telecomunicazioni e legislatori si sono incontrati per discutere come migliorare la competitività del continente nel settore IoT, in particolare mentre società statunitensi come Apple e Google sembrano fare la maggior parte dei progressi.

Il risultato della conferenza è stata una nuova alleanza dell'industria europea sostenuta dall'UE, comprendente grandi aziende come Phillips, Bosch, Orange, Alcatel, Nokia, Siemens, Telefonica e Volvo, il cui scopo è promuovere l'innovazione nell'IoT. Come ha dichiarato Anne Lauvergeon, a capo della startup sulle reti francesi Sigfox e membro del Consiglio di amministrazione della nuova alleanza IoT: "La creazione di un ecosistema per l'innovazione IoT è fondamentale per affrontare la concorrenza internazionale."^{xxxvi}

Contemporaneamente, l'UE sta lavorando per creare un unico mercato digitale mediante la rivisitazione delle leggi sulle telecomunicazioni esistenti. L'obiettivo della nuova legislazione è rimuovere gli ostacoli al trasferimento dei dati, secondo il Wall Street Journal "abbattendo i silos nazionali in aree come e-commerce e leggi sul copyright"^{xxxvii}. Questa necessità di rivedere l'ambiente normativo rivela la natura mutevole della nuova economia IoT, in cui la capacità di trasferire e scambiare in modo rapido e facile grandi quantità di dati diventerà uno dei simboli del successo di una regione.

Oltre all'aggiornamento della legislazione, la nuova economia IoT richiederà anche investimenti significativi in infrastrutture tecnologiche. A marzo 2015, la Banca europea per gli investimenti (BIE) ha tenuto a Berlino una conferenza sull'argomento "Momentum for Europe-Innovation and Competitiveness".^{xxxviii} Durante il suo discorso introduttivo, Jeremy Rifkin, presidente della Foundation on Economic Trends e consulente politico di Francia, Germania e UE, ha parlato del modo in cui l'accrescimento di scala e l'introduzione dell'IoT aiuteranno l'"Europa digitale" a entrare nella "Terza rivoluzione industriale".^{xxxix}

Tuttavia, Rifkin ha fatto notare che nel 2012 gli investimenti europei in piattaforme tecnologiche superate hanno raggiunto i 741 miliardi di USD. Se il 25% di questi fondi venisse reindirizzato in ogni regione dell'Unione europea verso infrastrutture IoT, i benefici complessivi dell'"Europa digitale" potrebbero essere realizzati entro il 2040^{xl}. Vale a dire che, secondo l'opinione di un esperto, troppi euro vengono destinati a sostenere un modello economico vecchio a scapito del futuro.

STATI UNITI

Nel 2014, gli imprenditori hanno investito quasi 11,9 miliardi di USD in società direttamente collegate a Internet, il valore massimo dal 2000 e dall'apice della bolla di mercato "Dot Com"^{xli}. Anche se non tutti questi capitali sono andati in dispositivi specifici per l'IoT, l'entusiasmo per l'IoT negli Stati Uniti è certamente a un massimo storico. Ad esempio, a marzo 2015 IBM ha annunciato che investirà 3 miliardi di USD in una nuova "divisione dedicata all'Internet delle Cose"^{xlii}

In effetti il settore privato sta tentando di mantenere gli Stati Uniti all'avanguardia della rivoluzione dell'IoT. Nel 2014, i giganti di software e tecnologia, tra cui AT&T, Cisco, General Electric, IBM e Intel, hanno annunciato l'Industrial Internet Consortium, il cui scopo è creare standard tecnici riguardanti gli oggetti IoT. In questo organismo non vincolante sono coinvolti anche la Casa Bianca e altri enti governativi.^{xliii} Nonostante l'FTC abbia suggerito al governo federale di evitare di emanare norme sull'IoT per ora, le agenzie del governo hanno iniziato a lavorare insieme a imprese private per produrre applicazioni pubbliche della tecnologia IoT. Ad esempio, nel 2014 i rappresentanti di Defense Advanced Research Projects Agency (DARPA), Dipartimento dei Trasporti e Veterans Health Administration si sono incontrati a Washington per discutere le tecnologie IoT per il settore pubblico.^{xliv}

Tuttavia, per quanto riguarda l'accesso alla banda larga e la velocità, gli Stati Uniti rimangono dietro ad altri Paesi sviluppati, in particolare in Asia. Secondo la società di traffico digitale Akamai, gli Stati Uniti occupano il 14° posto per velocità della banda larga^{xlv}. Nonostante la connettività generale negli Stati Uniti sia una delle migliori del mondo, infrastrutture obsolete, ostacoli normativi locali e costi elevati per l'accesso alla banda larga limitano le possibilità degli Stati Uniti di guidare l'adozione e l'innovazione in materia di IoT.

ASIA

Secondo RAND Europe, la Cina sta investendo risorse considerevoli in investimenti di IoT. Nel 2012, il Paese ha accantonato 625 milioni di € (775 milioni di USD) per investimenti nel settore IoT, con il ministero cinese di informazioni e tecnologia che ha creato un fondo di 775 milioni di USD per supportare lo sviluppo dell'IoT nei prossimi cinque anni. Entro il 2015, questi investimenti serviranno alla costruzione di dieci parchi industriali dedicati all'IoT e andranno a più di 100 aziende base sparse in tutto il Paese. In effetti, più di qualsiasi altro Paese, gli investimenti cinesi degli ultimi anni nelle infrastrutture IoT hanno superato la concorrenza di Europa e Stati Uniti^{xlvi}.

Mentre la Cina è sicuramente il giocatore principale sul mercato IoT, l'intera regione Asia Pacifico è pronta a guadagnare moltissimo dalla recente tecnologia IoT. La società di ricerca IDC stima che il mercato dell'Internet delle Cose in Asia Pacifico, escluso il Giappone, crescerà dai 250 miliardi di USD del 2013 ai 583 miliardi di USD del 2020. Nel frattempo, il numero di cose connesse a Internet nel mercato Asia Pacifico crescerà da 2,59 miliardi nel 2013 a 8,98 miliardi nel 2020.^{xlvii}

Nonostante preveda che entro il 2020 1 oggetto connesso a Internet su 5 sarà in Cina, IDC avverte che le dimensioni del mercato non corrispondono alla sua maturità. "Anche se le opportunità del mercato cinese sono enormi rispetto ad altri Paesi leader come Corea del Sud, India, Indonesia e Australia in termini di valore in dollari, ciò non significa che sia il più maturo", ha affermato Charles Reed Anderson, VP associato, responsabile di Mobilità e Internet delle Cose per IDC in Asia/Pacifico. "Per valutare la maturità di un mercato, confrontiamo il numero totale di oggetti connessi con la popolazione complessiva per ottenere il valore di connessioni pro capite. In base a questo calcolo, abbiamo scoperto che i tre mercati più maturi sono Corea del Sud, Australia e Nuova Zelanda, mentre la Cina occupa il sesto posto tra i 13 Paesi APeJ."^{xlviii}

Ciononostante, in qualità di hub produttivo del mondo, l'Asia è pronta a ottenere enormi benefici dall'economia IoT.

Conclusioni

Non è esagerato affermare che l'IoT introdurrà una nuova era economica per l'intero mondo. Le promesse fatte dall'IoT non sono semplici miglioramenti di processi e modelli economici esistenti, ma vere trasformazioni di ambito. L'economia IoT rivoluzionerà il modo in cui le attività producono, lavorano e operano. Inoltre il cambiamento sta avvenendo più velocemente di ogni altra rivoluzione industriale precedente.

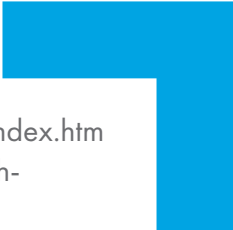
Al contempo, l'IoT comporterà grandi sfide in tutti i settori e per tutte le attività. Anche se risolve problemi che hanno afflitto le attività per decenni o addirittura secoli, essa creerà anche dilemmi completamente nuovi, sia procedurali che etici. Preoccupazioni per privacy, sicurezza informatica, proprietà e responsabilità dei prodotti diventeranno rapidamente importanti come le opportunità che l'IoT offre. Mentre devono iniziare a implementare la tecnologia IoT se sperano di sopravvivere sul lungo periodo, le attività devono anche implementare strategie che tengano conto dei molti rischi associati all'IoT.

Nel prossimo capitolo di questa serie esamineremo ulteriormente questi rischi e forniremo alle attività indicazioni pratiche per evitarli o minimizzarli. Presenteremo anche il modo in cui il settore assicurativo si prepara a aiutare le attività a navigare in questo nuovo mondo dell'IoT. Per molti aspetti, il settore assicurativo è pronto per sfruttare al massimo i sensori incorporati che producono grandi quantità di dati, cosa che fornirà informazioni più approfondite su come minimizzare i rischi per i clienti. Da tempo al centro delle pratiche di analisi guidate dai dati e riduzione dei rischi, il settore assicurativo sarà pronto per massimizzare le opportunità di IoT delle attività e minimizzarne l'esposizione.



Citazioni

- i <http://www.rfidjournal.com/articles/view?4986>
- ii RAND: Europe's policy options for a dynamic and trustworthy development of the Internet of Things, 2012
- iii CISCO: The Internet of Things How the Next Evolution of the Internet Is Changing Everything, 2011
- iv <http://www.ericsson.com/res/docs/2014/emr-june2014-regional-appendices-europe.pdf>
- v Dubravac, Shawn. "Digital Destiny." P. 68
- vi HBR-Verizon INTERNET OF THINGS: SCIENCE FICTION OR BUSINESS FACT?, 2014
- vii RAND: Europe's policy options for a dynamic and trustworthy development of the Internet of Things, 2012 p. 14
- viii ibid
- ix http://www.who.int/gho/road_safety/mortality/en/
- x http://ec.europa.eu/transport/road_safety/specialist/statistics/index_en.htm
- xi <http://morth.nic.in/writereaddata/mainlinkFile/File1465.pdf> and http://www.chinadaily.com.cn/china/2011-01/07/content_11808453.htm
- xii <http://www.forbes.com/sites/dougnewcomb/2015/05/08/daimler-autonomous-truck-has-huge-commercial-implications/>
- xiii © 2012 Google Inc. All rights reserved. Google and the Google Logo are registered trademarks of Google Inc.
- xiv Copyright 2002-2015 Tesla Motors, Inc. All Rights Reserved.
- xv <http://www2.deloitte.com/us/en/pages/finance/articles/internet-of-things-financial-services-industry.html>
- xvi <http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Bank-of-Things.pdf>
- xvii <http://osdelivers.blackducksoftware.com/2015/02/11/industrial-internet-of-things-in-the-maritime-industry/>
- xviii <http://www.rcrwireless.com/20150106/featured/ericsson-maritime-platform-targets-shipping-connectivity-tag2>
- xix <http://www.inman.com/2014/07/08/internet-of-things-could-be-most-disruptive-to-real-estate/>
- xx iBeacon is a trademark of Apple Inc., registered in the U.S. and other countries.
- xxi <http://realtormag.realtor.org/technology/feature/article/2015/03/real-estate-and-internet-things>
- xxii <http://www.ericsson.com/res/docs/2014/gtwp-op-transforming-industries-aw-print.pdf> p. 4
- xxiii <http://www.cnn.com/2009/OPINION/11/18/langewiesche.miracle.hudson.flight/index.html?iref=24hours>
- xxiv <http://www.forbes.com/sites/ptc/2014/06/23/will-the-internet-of-things-revolutionize-the-aircraft-industry/>

- 
- xxv <http://www.ilo.org/global/topics/safety-and-health-at-work/lang--en/index.htm>
 - xxvi <http://www.euractiv.com/sections/social-europe-jobs/commission-publishes-health-and-safety-strategy-eu-workers-302665>
 - xxvii <http://www.gartner.com/newsroom/id/2688717>
 - xxviii http://ec.europa.eu/ipg/basics/legal/data_protection/index_en.htm
 - xxix <https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices>
 - xxx <http://www.techweekeurope.co.uk/mobility/lawsuit-tracking-app-168043>
 - xxxi <http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/>
 - xxxii <http://www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/>
 - xxxiii <http://www.gao.gov/products/GAO-15-370>
 - xxxiv http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1752
 - xxxv http://www.nytimes.com/2015/04/30/business/several-american-airlines-flights-are-delayed-by-an-app-malfunction.html?_r=0
 - xxxvi <http://blogs.wsj.com/digits/2015/03/25/europe-wants-to-bring-its-industry-online-before-google-apple-make-it-obsolete/>
 - xxxvii <http://www.wsj.com/articles/eu-considers-new-telecom-rules-to-level-the-playing-field-1427295277>
 - xxxviii <http://www.eib.org/infocentre/events/all/momentum-for-europe.htm>
 - xxxix <http://www.automatedtrader.net/headlines/153295/digital-europe-the-rise-of-the-internet-of-things-and-the--transition-to-a-third-industrial-revolution>
 - xl *ibid*
 - xli <http://nvca.org/pressreleases/annual-venture-capital-investment-tops-48-billion-2014-reaching-highest-level-decade-according-moneytree-report/>
 - xlii <http://www.theglobeandmail.com/report-on-business/international-business/us-business/ibm-to-invest-3-billion-in-new-internet-of-things-unit/article23722378/>
 - xliii http://bits.blogs.nytimes.com/2014/03/27/consortium-wants-standards-for-internet-of-things/?_php=true&_type=blogs&_r=1
 - xliv http://www.washingtonpost.com/business/on-it/dot-va-reps-discuss-how-the-federal-government-could-use-internet-of-things/2014/08/06/d9ac6410-1d84-11e4-ae54-0cfef1f974f8a_story.html
 - xlv http://www.akamai.com/dl/akamai/akamai-soti-q114.pdf?WT.mc_id=soti_Q114
 - xlvi HBR-Verizon INTERNET OF THINGS: SCIENCE FICTION OR BUSINESS FACT?, 2014 p. 7
 - xlvii <http://www.idc.com/getdoc.jsp?containerId=prHK25553415>
 - xlviii *ibid*

The Consumer Technology Association (CTA) is the technology trade association representing the \$286 billion U.S. consumer electronics industry. More than 2,000 companies enjoy the benefits of CTA membership, including legislative and regulatory advocacy, market research, technical training and education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES – The Global Stage for Innovation. All profits from CES are reinvested into CTA's industry services. Find CTA online at CE.org, InnovationMovement.com and through social media at ce.org/social.

American International Group, Inc. (AIG) is a leading global insurance organization serving customers in more than 100 countries and jurisdictions. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: www.linkedin.com/company/aig

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds. The content contained herein is intended for general informational purposes only, and should not be viewed as a substitute for legal, regulatory, accounting or other advice on any particular issue or for any particular reason.

© American International Group, Inc. All rights reserved.

12/15 SP812T



Bring on tomorrow®