Nomisma
SOCIETÀ DI STUDI ECONOMICI

nomisma.it

L'INDUSTRIA DELLA CYBER SECURITY PER LA COMPETITIVITÀ DEL SISTEMA IMPRENDITORIALE ITALIANO

29 settembre 2015

Lo studio è stato commissionato da Itway SpA e realizzato da:

- **Piera Magnatti (Coordinatrice)**
- **Francesco Capobianco**
- **Paola Piccioni**
- **Luigi Scarola**

La direzione scientifica è stata realizzata da Giulio Santagata.

Anna Bellotti ha curato gli aspetti editoriali della ricerca.

Indice

1. INTRODUZIONE. EVENTI CRITICI IN AMBITO CYBER: DAL “SE” AL “QUANDO”

Eventi critici/anomalie in ambito cyber

- La settima edizione del Rapporto CLUSIT evidenzia come il rischio teorico di essere colpiti da un attacco informatico di qualche genere per tutte le tipologie di soggetti interessati (cittadini, aziende, istituzioni, Governi) sia diventato, in pratica e nel breve-medio termine, una certezza.

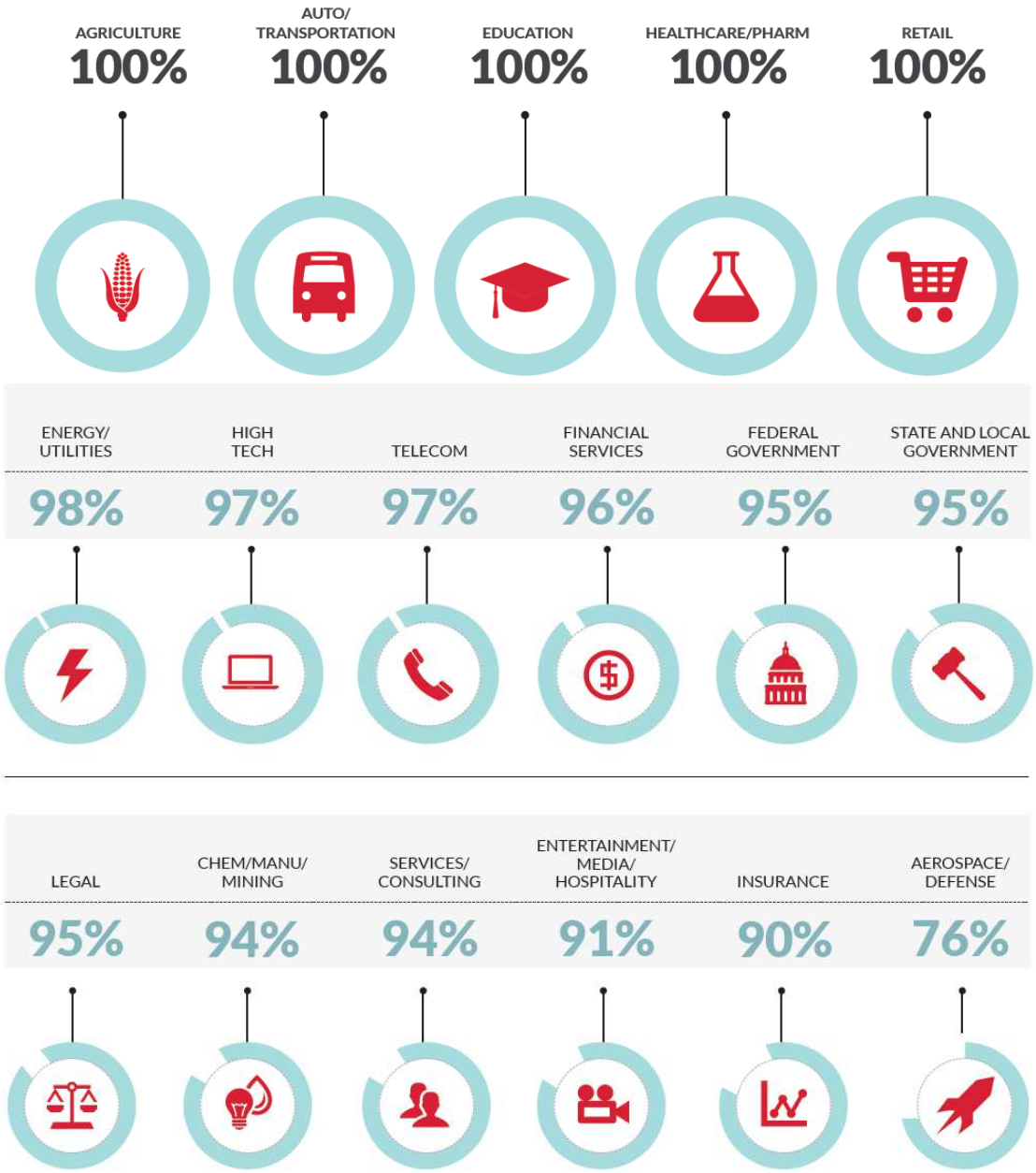
- Lo scenario cambia: non è più "se", ma "quando" si subirà un attacco informatico (dalle conseguenze più o meno dannose), e quali saranno gli impatti conseguenti.

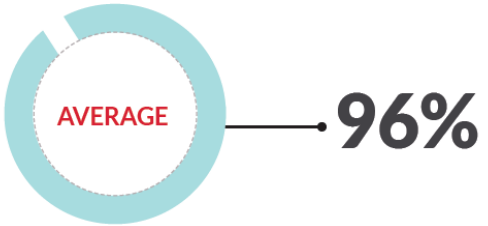
- Un cambiamento di scenario sostanziale, che mettendo in discussione tre decenni di progettazione e di gestione dell'ICT, inclusi i più recenti sviluppi in materia di Cloud, Mobile, Social Media e Internet of Things, non solo rende obsolete prassi consolidate, ma minaccia di far saltare i budget di spesa allocati e gli obiettivi di business prefissati, cogliendo in contropiede sia la società nel suo complesso che le istituzioni e, cosa più grave, trovando impreparati la maggior parte dei vendor di tecnologie e degli addetti ai lavori.

- In uno studio condotto nel corso del 2014 da FireEye ("*Maginot Revisited: More Real World Results from Real World Tests*") sono state monitorate su scala globale 1.600 aziende appartenenti a 20 diversi settori merceologici.

- In media, la percentuale di organizzazioni compromesse è stata superiore al 95%, con alcuni particolari settori (Legal, Healthcare e Pharma, Retail) che hanno avuto un tasso di compromissione del 100%.

INTRODUZIONE





Fonte: FireEye

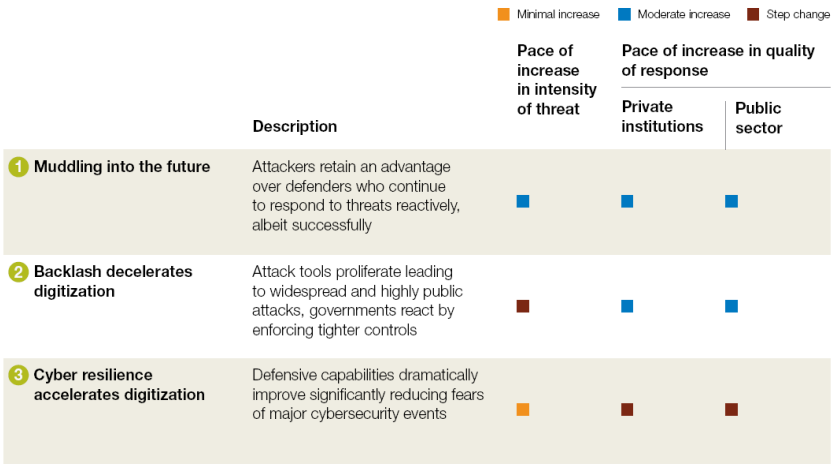
Cyber Resilience

- Il tema è, quindi, come prepararsi all'evento.
- "Cyber Resilience" è la (relativamente) nuova parola d'ordine, tanto che il World Economic Forum ha dedicato nel 2012 il suo rapporto "*Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience"* a questo tema.
- La "Cyber Resilience" intesa come dimensione aggiuntiva della gestione del rischio informatico, è – secondo il WEF - la capacità dei sistemi e delle organizzazioni di resistere a eventi critici informatici, misurata dalla combinazione di tempo medio di crisi e il tempo medio di recupero.
- Gli Stati Uniti ne hanno fatto uno dei pilastri della loro strategia di Cyber Security nel 2013. Il Dipartimento per la Sicurezza nazionale americano definisce il termine "resilience" come la capacità di adattarsi ai cambiamenti e di resistere e recuperare rapidamente da eventi distruttivi che generano situazioni di emergenza. Che si tratti di atti di terrorismo, attacchi informatici, pandemie o catastrofi naturali, la preparazione nazionale è ritenuta responsabilità comune di tutti i livelli di governo, del settore privato e senza scopo di lucro e dei singoli cittadini.
- L'Unione Europea sta lavorando sul tema fin dal 2009 con il progetto dell'ENISA "*European Public-Private Partnership for Resilience*".
- L'Italia ha incluso il tema nell'ambito del suo Quadro Strategico Nazionale e ha organizzato in merito un evento durante il semestre italiano di Presidenza Europea.

Tendenze 2015

- CLUSIT delinea le principali tendenze per il 2015:
  - Social Networks al centro del mirino
  - POS, il tallone d'Achille del Retail
  - Mobile, strategie da rivedere velocemente
  - Ricatti ed estorsioni nei confronti di aziende, PA ed Infrastrutture Critiche
  - Diffusione di strumenti assicurativi contro rischi "cyber"

- Come illustrato dal World Economic Forum nel Rapporto "*Risk and Responsibility in a Hyperconnected Word*" del 2014, nei prossimi cinque anni gli scenari che si prefigurano sono tre. Il WEF sottolinea come sia necessario impegnarsi affinché sia il terzo a realizzarsi, con il pubblico e il privato proattivi per limitare la proliferazione di strumenti di attacco, costruire capacità istituzionale e stimolare l'innovazione e l'efficienza economica.



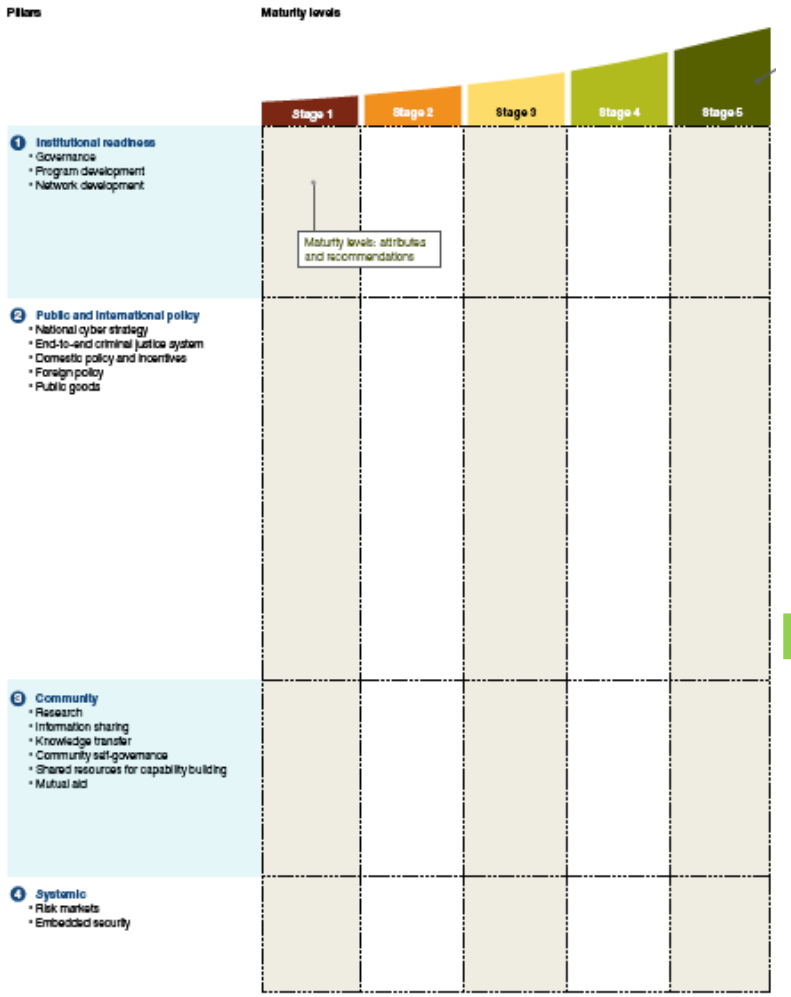
	Description	Pace of increase in intensity of threat	Pace of increase in quality of response: Private institutions	Pace of increase in quality of response: Public sector
1 Muddling into the future	Attackers retain an advantage over defenders who continue to respond to threats reactively, albeit successfully	■	■	■
2 Backlash decelerates digitization	Attack tools proliferate leading to widespread and highly public attacks, governments react by enforcing tighter controls	■	■	■
3 Cyber resilience accelerates digitization	Defensive capabilities dramatically improve significantly reducing fears of major cybersecurity events	■	■	■

nomisma.it

WEF - Roadmap

- Da CLUSIT una nota di cauto ottimismo: uscire dalla "trappola" dell'insicurezza informatica applicando estesamente logiche di Cyber Resilience è non solo necessario, ma anche certamente possibile. Riallocazione di risorse (economiche ed umane), valutazione puntuale dei rischi ed ottimizzazione della spesa in sicurezza, che deve crescere non solo in quantità ma anche e soprattutto in qualità ed efficacia.

- Il World Economic Forum indica la seguente roadmap per un'azione collaborativa



INTRODUZIONE

WEF - Raccomandazioni 1

- **Governance**
  - Dare priorità ai patrimoni informativi sui rischi aziendali
  - Integrare la resilienza informatica nei processi di gestione del rischio e di governance a livello aziendale
  - Coinvolgere i vertici aziendali

- **Sviluppo di programmi e network**
  - Fornire una protezione differenziata in base all'importanza del patrimonio
  - Sviluppare una profonda integrazione della sicurezza in ambiente tecnologico per gestirne la scalabilità
  - Attivare difese attive per scoprire gli attacchi in modo proattivo
  - Effettuare test continui per migliorare la risposta agli incidenti
  - Mobilitare il personale front-line - aiutandolo a comprendere il valore del patrimonio informativo

- **Strategia cyber nazionale**
  - Definire una strategia informatica nazionale globale e trasparente, che si integri con le strategie e le procedure di tutti i domini della politica
  - Le strategie dovrebbero incorporare il settore privato e civile e tener conto delle questioni economiche e di sicurezza
  - Creare una istituzione competente per l'attuazione della strategia nazionale

- **Il sistema di giustizia penale**
  - Le forze dell'ordine hanno la capacità e le risorse per indagare i crimini informatici
  - Lo Stato ha un codice giuridico adeguato, completo e agile per indagare e perseguire i crimini informatici
  - I legali comprendono l'ecosistema della sicurezza informatica in modo tale da realizzare un giusto processo

WEF - Raccomandazioni 2

- **Politica interna ed incentivi**
  - Il privato, il pubblico e la società civile dialogano per sviluppare un'adeguata e coerente combinazione di meccanismi politici e di mercato
  - Il governo sostiene gli sforzi delle forze dell'ordine

- **Politica estera**
  - Stabilire una dottrina nazionale in ambito Cyber
  - Identificare le persone a livello locale e nazionale responsabili della sicurezza informatica
  - Stabilire canali formali e informali di comunicazione tra entità delle forze dell'ordine
  - Creare interoperabilità tra enti a livello nazionale responsabili per la sicurezza informatica
  - Lavorare per armonizzare le politiche nazionali e internazionali volte al perseguimento della criminalità informatica
  - Stabilire un approccio multi-stakeholder alla governance del tema

- **Beni pubblici**
  - Assicurare una capacità di risposta agli incidenti consistente e in evoluzione
  - Aumentare gli investimenti in formazione tecnica sulla sicurezza informatica
  - Finanziare un programma di ricerca sulla sicurezza informatica
  - Fornire protezione per la condivisione limitata di informazioni tra imprese e governo

WEF - Raccomandazioni 3

- **Ricerca**
  - Aumentare la formazione e la sensibilizzazione
  - Incoraggiare la ricerca sulle imprese e sull'impatto macroeconomico della sicurezza informatica per fornire priorità politiche
  - Creare un ambiente in cui la ricerca “white-hat” sia incoraggiata

- **Risorse condivise per aumentare le capacità**
  - Promuovere partnership tra i governi, le università e il settore privato per lo sviluppo delle competenze

- **La condivisione delle informazioni**
  - Dove giuridicamente fattibile, le istituzioni attuano meccanismi di condivisione delle informazioni legali
  - Migliorare la qualità dei ISACs / CERT / CIERTs e gli altri luoghi di condivisione delle informazioni
  - Promuovere un sistema interoperabile, estensibile e automatizzato per la condivisione
  - Fornire protocolli comuni per diffondere informazioni riguardanti eventi informatici

- **Mercati del rischio**
  - Espandere la portata e l'ampiezza dei mercati assicurativi sulla sicurezza informatica

- **Sicurezza integrata**
  - Esplorare modi per creare un internet più sicuro, ad esempio: il nuovo standard HTTP 2.0 ha aumentato la sicurezza attraverso il trasferimento di dati crittografati. Oppure consentendo agli ISP di bloccare i computer che partecipano a botnet o che sono comunque danneggiati
  - Sviluppare una metodologia per quantificare l'impatto di cyber

2. IL MERCATO DELLA CYBER SECURITY

Il mercato globale

- Il mercato della sicurezza informatica a livello mondiale continua a crescere e a svilupparsi. Le stime vanno da 75 miliardi di dollari nel 2015 a 170 miliardi entro il 2020, con un tasso di crescita annuo composto (CAGR) del 9,8% 2015-2020.
- Il Nord America e l'Europa sono i principali contributori al reddito del settore della sicurezza informatica.
- L'Asia-Pacifico sta rapidamente emergendo come mercato potenziale per i fornitori di soluzioni di sicurezza informatica, guidati da economie emergenti come Cina, India e paesi dell'Asia del Sud-Est.
- Secondo IDC, i settori di maggior crescita sono l'analisi di sicurezza (SIEM) (10%); le informazioni sulle minacce (10% +); la sicurezza mobile (18%); la sicurezza del cloud (50%).
- Secondo i Lloyd di Londra, la criminalità informatica sta costando alle aziende fino a 400 miliardi di dollari l'anno. Alcune previsioni parlano di 500 miliardi di dollari.
- La criminalità informatica sta alimentando la domanda di assicurazione informatica, un mercato che cresce accanto ai prodotti e ai servizi di sicurezza informatica. L'anno scorso, il settore assicurativo ha generato circa 2,5 miliardi di dollari in premi sulle politiche per proteggere le aziende da perdite a seguito di attacchi informatici.

Dati e prospettive da Cybersecurity Ventures

- Il mercato Europeo è destinato a crescere a 35,53 miliardi di dollari entro il 2019, del 7,2% nel periodo 2013-2019. Questo mercato contribuisce per il 26.95% al mercato globale e scenderà al 22,81% entro il 2019.
- Il Medio Oriente e l'Africa sono destinati a crescere fino a 13,43 miliardi di dollari entro il 2019, con un CAGR del 13,7% per il periodo 2013-2019. Questo mercato contribuisce per il 7,19% al mercato globale e crescerà fino al 8,62% entro il 2019.
- L'area Asia-Pacifico è destinata a crescere fino a 32,95 miliardi di dollari entro il 2019, con un CAGR del 14,1% per il periodo 2013-2019. Questo mercato contribuisce per il 17.21% al mercato globale e aumenterà fino al 21.16% entro il 2019.
- L'America Latina è destinata a crescere fimo a 11,91 miliardi di dollari entro il 2019, con un CAGR del 17,6% per il periodo 2013-2019. Questo mercato contribuisce per il 5,18% al mercato globale e crescerà fino al 7,65% entro il 2019.
- "La richiesta per la forza lavoro è prevista in aumento a 6 milioni di unità (a livello globale) entro il 2019, con un deficit previsto di 1,5 milioni", ha dichiarato Michael Brown, CEO di Symantec, il più grande fornitore di software di sicurezza al mondo.

Il mercato italiano

- L'edizione 2015 del Rapporto ASSINFORM rileva come il mercato italiano della sicurezza nel 2014 abbia continuato il percorso di crescita intrapreso già nel 2013, registrando un'espansione del 2% per un valore pari a 772 milioni di euro (750 meuro nel 2012, 757 meuro nel 2013), a conferma dell'importanza crescente data dalle aziende alla tematica, e anche della spinta derivante dalla compliance normativa.

- A livello di singoli segmenti il software è la componente che ha registrato l'andamento più vivace (+3,5%), spinto da progetti volti a mettere in sicurezza sia i sistemi tradizionali che quelli "innovativi" come mobile, network, cloud.

- In crescita è stato anche il segmento dei servizi (+1,6%) in cui, oltre che per la componente di system integration, si è registrato un trend di crescita per le attività a supporto della revisione delle strutture organizzative e alla definizione di policy e per i servizi di audit.

- Anche nel 2014, così come già accaduto l'anno precedente, l'unico segmento in contrazione è stato quello dell'hardware, in flessione dell'1%, per effetto del calo progressivo dei costi degli apparati che, a parità di capacità, scontano un differenziale in negativo rispetto all'anno precedente.

Digital Security per la PA

- Nella Pubblica Amministrazione, sia Centrale che Locale, gli investimenti digitali hanno continuato nella dinamica negativa che caratterizza il settore ormai già da diversi anni.
- La Pubblica Amministrazione Centrale ha registrato una contrazione dei budget maggiore di quella Locale, anche se nel 2014 il calo è risultato molto più contenuto rispetto all'anno precedente, lasciando intravedere i primi segnali di una ripresa.
- Nel 2014, infatti, nelle Amministrazioni Centrali si è rilevato un calo della spesa del 2,6% (contro il -11,6% del 2013), imputabile prevalentemente alle componenti di servizi ICT, situazione generalizzata all'intero mercato IT, e dei dispositivi e sistemi, che ha riflesso la progressiva riduzione dei prezzi di acquisto e l'allungamento dei tempi di sostituzione.
- La spesa relativa al mercato digitale della Pubblica Amministrazione Locale ha continuato, anche nel 2014, a evidenziare una dinamica negativa, registrando un calo del 2,1%, per un valore complessivo del mercato pari a 1.237 milioni di euro.
- Il calo più consistente ha riguardato la componente di dispositivi e sistemi, seguita da quella relativa ai servizi ICT. Anche nel 2014, infatti, il Patto di Stabilità e la Spending Review hanno pesato sui budget destinati agli investimenti ICT traducendosi, soprattutto nei Comuni, in tagli lineari che hanno colpito anche la spesa ICT.

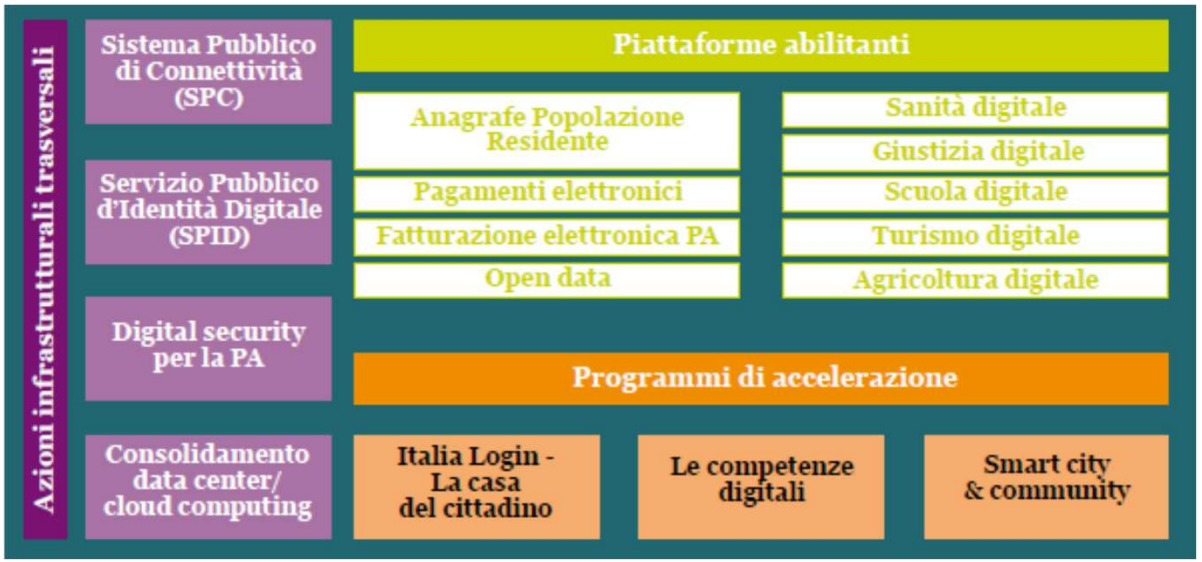
Il Piano Crescita Digitale

- A marzo 2015 il Consiglio dei Ministri ha approvato il Piano Nazionale Banda Ultralarga e il Piano Crescita Digitale 2014-20207, due strategie sinergiche per il perseguimento degli obiettivi dell'Agenda Digitale Europea al 2020. I due piani strategici sono stati definiti dall'Agenzia per l'Italia Digitale e dal Ministero dello Sviluppo Economico, con l'obiettivo primario di colmare il ritardo digitale del Paese sul fronte infrastrutturale e dei servizi per i cittadini e le imprese.

- La strategia per la Crescita Digitale integrerà quanto già realizzato o in progress, in piena sinergia con altre iniziative pubbliche in essere, per mettere a sistema obiettivi, processi e risultati.

- Il Piano per la Crescita Digitale traccia una roadmap per la digitalizzazione del Paese. Gli obiettivi strategici che si pone sono:
  - il progressivo switch-off verso la completa digitalizzazione della Pubblica Amministrazione, in un'ottica centrata sull'utente, coordinando e mettendo a sistema le diverse azioni avviate da tutte Amministrazioni - entro il 2016 gli Enti della PA dovranno essere in grado di gestire tutti i documenti in elettronico;
  - lo sviluppo di competenze digitali nelle imprese e la diffusione di cultura digitale fra i cittadini, in modo da innescare un circolo virtuoso tra crescita della domanda e crescita dell'offerta, in chiave innovativa;
  - una maggiore efficienza del Sistema Paese, coordinando la programmazione e gli investimenti pubblici in innovazione digitale e ICT.

Il Piano Crescita Digitale



Digital Security per la PA

- Il Progetto di Digital Security per la PA nasce per aumentare il livello di sicurezza delle informazioni e delle comunicazioni digitali per consentire nuovi livelli di servizi per i cittadini e le imprese. Il fine ultimo è di tutelare la privacy, l'integrità e la continuità dei servizi della PA, vera e propria infrastruttura critica per il paese. In questo progetto rientra anche il CERT-PA.

- Il Governo Italiano attraverso l'Agenzia per l'Italia Digitale definisce gli Standard e le linee guida di sicurezza per tutta la pubblica amministrazione. L'aderenza agli standard di servizio e di processo sarà obbligatorio per tutte le Amministrazioni Pubbliche. La Cabina di Regia per la Cybersecurity, presieduta dal Consigliere Militare del Presidente del Consiglio assicura il coordinamento fra tutti i soggetti pubblici. Il ministero dello Sviluppo Economico attraverso l'Organo di Certificazione della Sicurezza Informatica, verifica l'aderenza delle soluzioni agli standard. Il settore privato avrà il compito di sviluppare prodotti e soluzioni allineati agli Standard.

- Nel progetto sono coinvolte tutte le Amministrazioni Pubbliche, nonché tutti quegli attori del settore privato che forniscono soluzioni e servizi alla PA.

- Il Settore Privato ricopre un ruolo chiave, in quanto sarà l'attore principale al fianco delle Pubbliche Amministrazioni per l'innalzamento della sicurezza e la privacy dei servizi digitali. Questo tipo di coinvolgimento avrà risvolti positivi anche al di fuori della PA, poiché stimolerà il settore privato a sviluppare servizi e soluzioni con più alti standard di sicurezza, che potranno essere messi a disposizione all'intero mercato Italiano ed Europeo.

- Tempistica 2015 – 2020; fabbisogno finanziario 30 milioni di euro fino al 2020

3. L’ATTORE PROTAGONISTA: L’INDUSTRIA DELLA CYBER SECURITY

L'offerta

- Nell'ambito dei numerosi approfondimenti realizzati a livello nazionale e internazionale sul tema della cyber security un protagonista della vicenda - il settore delle imprese che offrono tecnologie e servizi avanzati nel campo della sicurezza informatica – è ancora poco tracciato.

- È soprattutto poco evidenziato il ruolo che tali imprese possono giocare nel garantire la sicurezza del dato in una prospettiva in cui questo obiettivo deve essere perseguito al pari della tutela della concorrenza, in una visione integrata tra domanda, offerta e diffusione delle conoscenze a livello nazionale, integrazione che possa portare ad aumentare il livello di consapevolezza del sistema industriale italiano nel Paese.

- C'è ancora ampio spazio di azione e sperimentazione su un fronte molto delicato volto a coniugare la tutela della concorrenza con la sicurezza del dato.

- L'Agenda Digitale italiana, anche con il supporto delle risorse comunitarie della nuova programmazione, può rappresentare il contesto ideale attraverso cui avviare una efficace collaborazione pubblico-privato in tale direzione.

Il settore ICT

- Il settore dell'ICT è di assoluto rilievo nel sistema economico nazionale. Conta più di 75.400 imprese e 456 mila addetti, concentrati nelle PMI, la maggior parte operanti nell'ambito dei servizi (all'incirca 70%), a fronte, sempre all'incirca, del 23% nel software, del 5% nelle telecomunicazioni e dell'1,5% nella produzione di hardware.

- L'andamento del numero delle imprese fra il 2010 e il 2013 evidenzia l'effetto della crisi: un impatto forte nel 2011 e una leggera ripresa nel 2012 che non è stata mantenuta nel 2013. Nel complesso, dal 2010 al 2013, il settore ha subito la perdita di più di 7 mila imprese attive. I comparti più penalizzati sono stati quello dell'hardware e quello dei servizi. Significativo è il fenomeno delle startup.

- Il settore è nel pieno di un grande cambiamento e la crisi si è sentita, ma la digital trasformation sta aprendo a grandi opportunità.

- Al calo del numero delle imprese si associato un calo dell'occupazione. Hanno contato anche le riorganizzazioni delle imprese che, anche attraverso riduzioni di organico, hanno cercato di contrastare la congiuntura negativa. Dal 2010 al 2013 il settore ha perso più di 34 mila addetti.

- Le carenze di competenze continuano a manifestarsi: alcune imprese del settore già da diversi anni hanno iniziato a realizzare partnership con Atenei ed enti di formazione superiore. Lo scopo è di colmare le lacune della preparazione accademica attraverso una formazione focalizzata alle esigenze del mercato.

- L'indagine Cepis e-Competence Benchmark evidenzia come in Europa la carenza di professionisti qualificati nel settore ICT freni la capacità di rilanciare la crescita economica e la competitività. Nel 2020 in Europa vi saranno 900 mila posti vacanti nell'ICT.

Il mercato della sicurezza ICT

- Nonostante i venti di crisi, il mercato della sicurezza ICT conferma anche per il 2013 un trend, seppure timido, di crescita, confermando il dato registrato fin dalla prima edizione del Rapporto CLUSIT.

- In particolare, per quando riguarda il 2013, i fornitori hanno pressoché confermato i dati previsionali forniti nel Rapporto CLUSIT 2013, con una lieve preponderanza di coloro i quali hanno rilevato una crescita (42%), rispetto alle aziende che hanno riscontrato un mercato stazionario rispetto all'anno precedente (40%).

- Tale mercato, tuttavia, si sta ampliando grazie ad una maggiore ricerca e specializzazione dei fornitori che, complice la crisi, adattano la propria offerta alla pluralità di esigenze delle nicchie di mercato o delle aree geografiche fino a poco tempo fa scarsamente raggiunte.

- La proiezione del mercato per il 2014 resa dai fornitori mostra previsioni nettamente orientate alla crescita, quasi un plebiscito per un valore superiore al 70% degli intervistati.

4. FOCUS SULLE PERFORMANCE DI UN CAMPIONE DI IMPRESE

LA COSTRUZIONE DEL CAMPIONE

•**Identificazione delle imprese attraverso key words analysis**. Non essendo le aziende che operano nella sicurezza informatica riconducibili a settori codificati ATECO, la costruzione del campione è avvenuta attraverso un approccio analitico qualitativo basato sul posizionamento web delle singole realtà aziendali per le quali la cyber security rappresenta il core business o uno dei prevalenti mercati;

• **Definizione dei parametri campionari**. Al fine di avere una rappresentazione robusta delle dinamiche evolutive, si è ricorsi all'analisi attraverso «modalità panel». Tra le imprese identificate sono state selezionale le realtà per le quali risulta annualmente depositato il bilancio d'esercizio per tutto il periodo analizzato. Sono state inoltre eliminate dal campione le imprese con un volume di affari, al 2013, superiore a 100 milioni di euro, al fine di evitare una distorsione dell'analisi;

• **Il campione di imprese**. L'analisi è stata dunque sviluppata analizzando le performance economiche di un campione di 87 società di capitali;

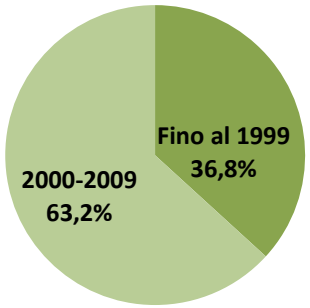
• **La significatività del campione.** La presente analisi pur non avendo obiettivi di rappresentatività statistica, si ritiene che possa considerarsi una proxy dei comportamenti del sistema nazionale. Si è deciso di focalizzare lo studio sulle società di capitali in quanto il presumibile maggior grado di strutturazione può rappresentare una più elevata capacità di intercettare gli elementi di sistema dell'intero settore.

LE CARATTERISTICHE DEL CAMPIONE

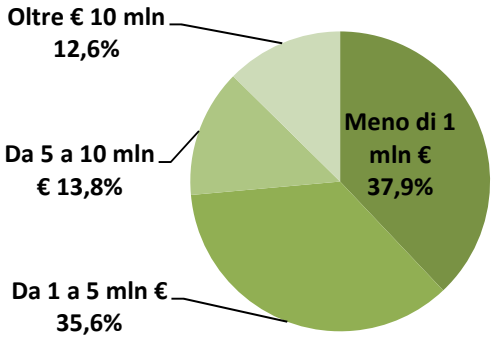
- Il campione oggetto di analisi risulta, per la maggior parte (63,2%), composto da imprese «giovani», costituite a partire dall'anno 2000;

- Segmentando il campione per classi di ricavi al 2013, si evidenzia una preponderanza marcata di imprese di piccole e medie dimensioni: le imprese che al 2013 presentavano un valore dei ricavi al di sotto dei 5 milioni di euro costituiscono il 73,5% del campione.

Campione di imprese analizzato per anno di costituzione



Campione di imprese analizzato per classe di ricavi delle vendite al 2013

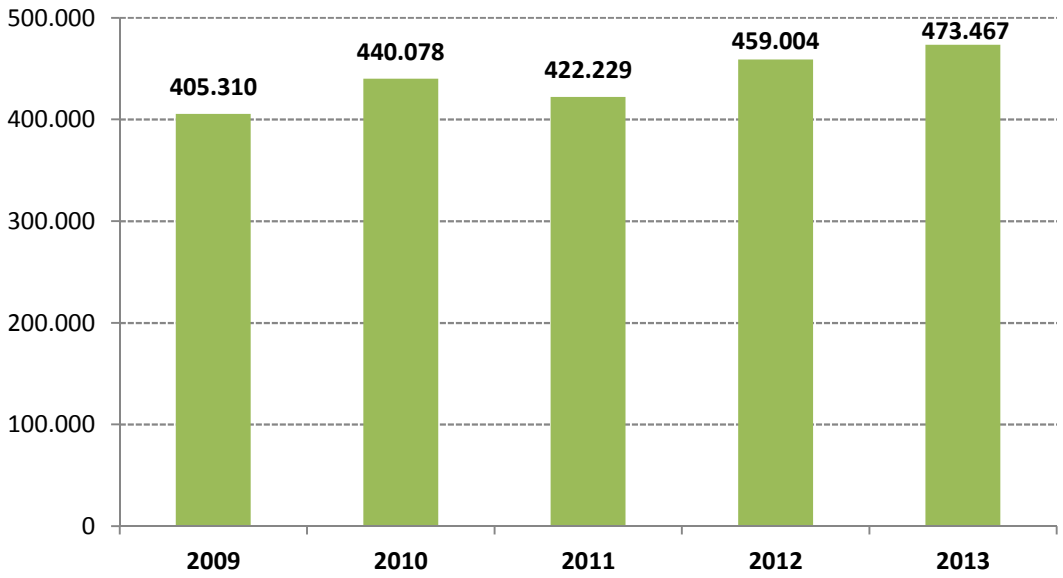


Fonte: elaborazioni Nomisma su dati Aida - Bureau van Dijk

I ricavi delle vendite

• I ricavi delle vendite mostrano un andamento crescente, evidenziando nel quadriennio 2009-2013 un aumento pari al 16,8%, con una sola fase di arretramento nel corso dell'anno 2011, il che sottolinea una sostanziale 'tenuta' anche nel periodo di congiuntura negativa

I ricavi delle vendite: serie storica dal 2009 al 2013
(valori espressi in migliaia di euro)



Var. % 2013/2009: +16,8%

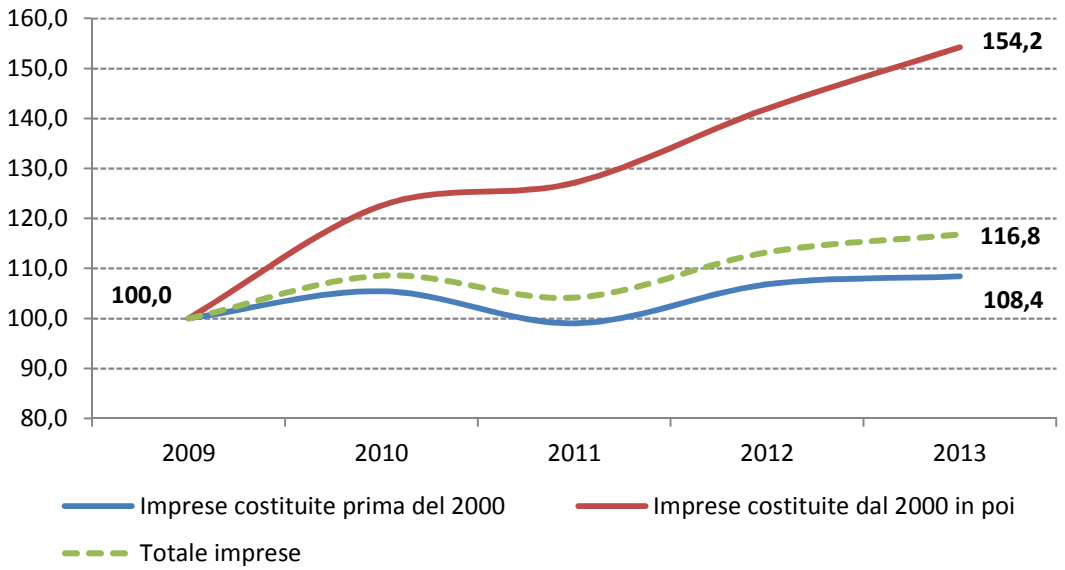
Fonte: elaborazioni Nomisma su dati Aida - Bureau van Dijk

FOCUS SULLE PERFORMANCE DI UN CAMPIONE DI IMPRESE

nomisma.it

I ricavi

Dinamica dei ricavi delle vendite per periodo di costituzione aziendale– Anno base 2009=100. *Anni 2009-2013*



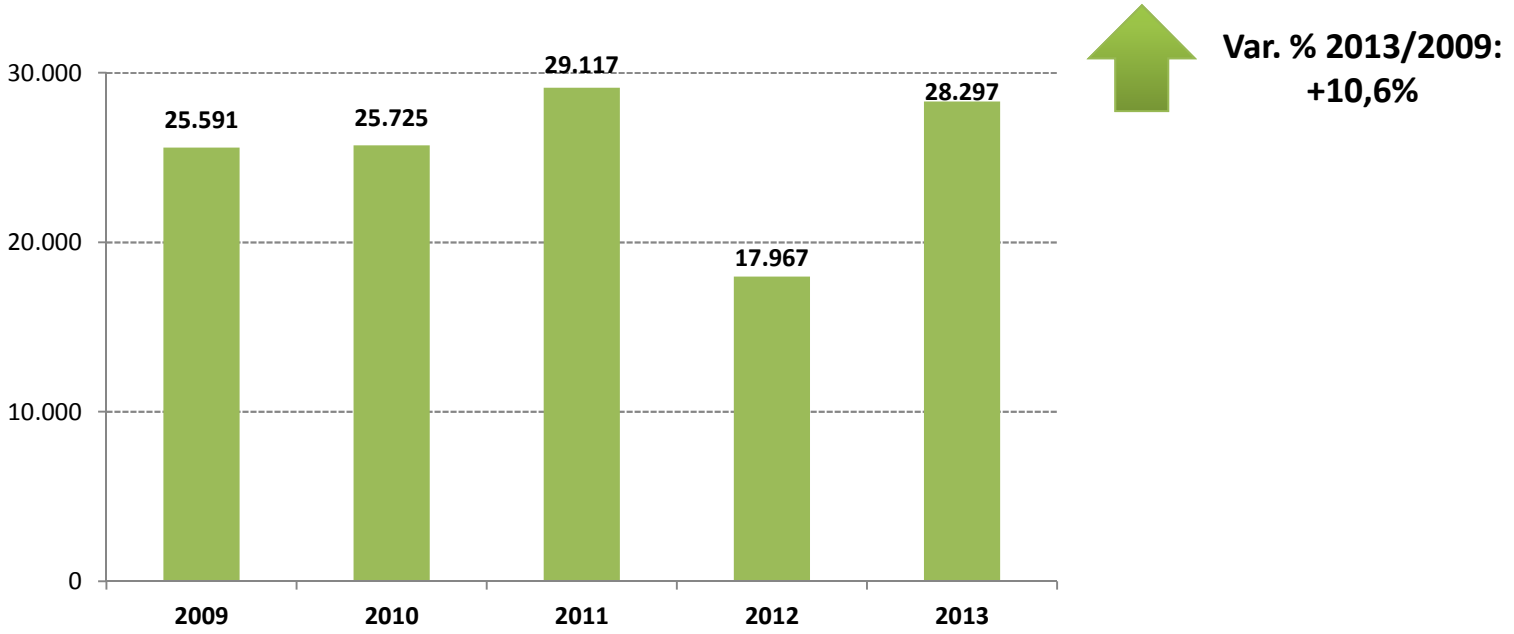
Fonte: elaborazioni Nomisma su dati Aida - Bureau van Dijk

- Scomponendo il campione per periodo di costituzione delle imprese, si osserva come la crescita del volume di affari sia attribuibile in misura maggiore alle imprese che sono state costituite a partire dall'anno 2000, che dal 2009 al 2013 hanno visto aumentare i propri ricavi del 54,2%. Più contenuta la crescita delle imprese nate prima dell'anno 2000, che si attesta al +8,4%;
- Tale dinamica può ricondursi ad un maggiore grado di adattabilità al mercato (decisamente mutevole);
- È necessario anche considerare che alcune aziende del campione sono frutto di fusioni/incorporazioni di realtà preesistenti, alle quali è utile prestare particolare attenzione soprattutto rispetto all'esigenza di innalzamento delle competenze.

Il risultato operativo

- Come per il fatturato, anche per il risultato operativo la dinamica 2009-2013 mostra un trend in crescita, con una incremento complessivo a fine periodo pari al +10,6%;
- Risulta necessaria una riflessione sull'esigenza di un'ottimizzazione dei processi riorganizzativi al fine della riduzione dell'incidenza dei costi della produzione.

Il risultato operativo : serie storica dal 2009 al 2013
(valori espressi in migliaia di euro)



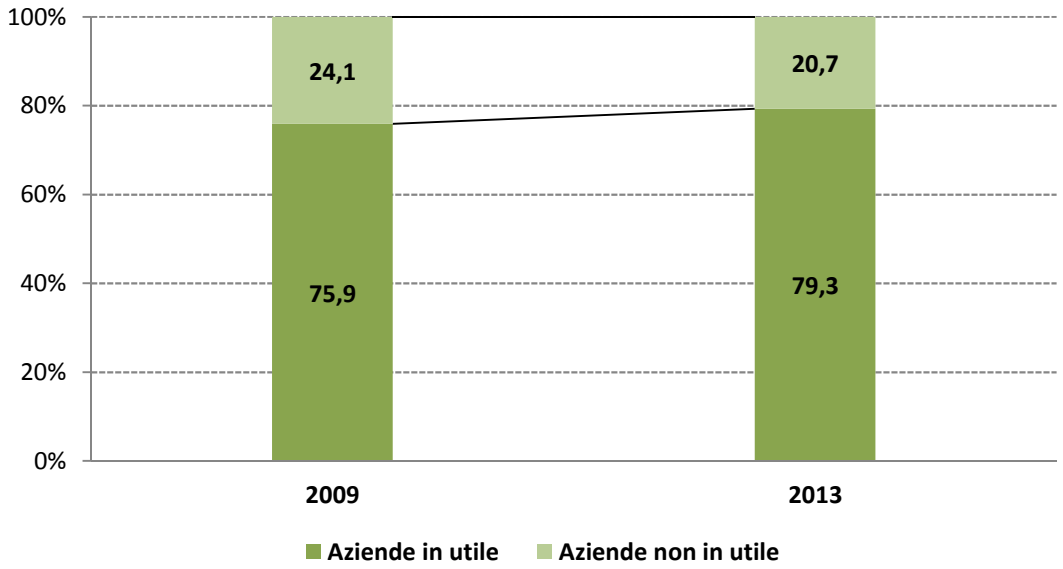
Fonte: elaborazioni Nomisma su dati Aida - Bureau van Dijk

FOCUS SULLE PERFORMANCE DI UN CAMPIONE DI IMPRESE

nomisma.it

L'utile di esercizio

Quota percentuale di aziende in utile e non: anni 2009-2013



Fonte: elaborazioni Nomisma su dati Aida - Bureau van Dijk

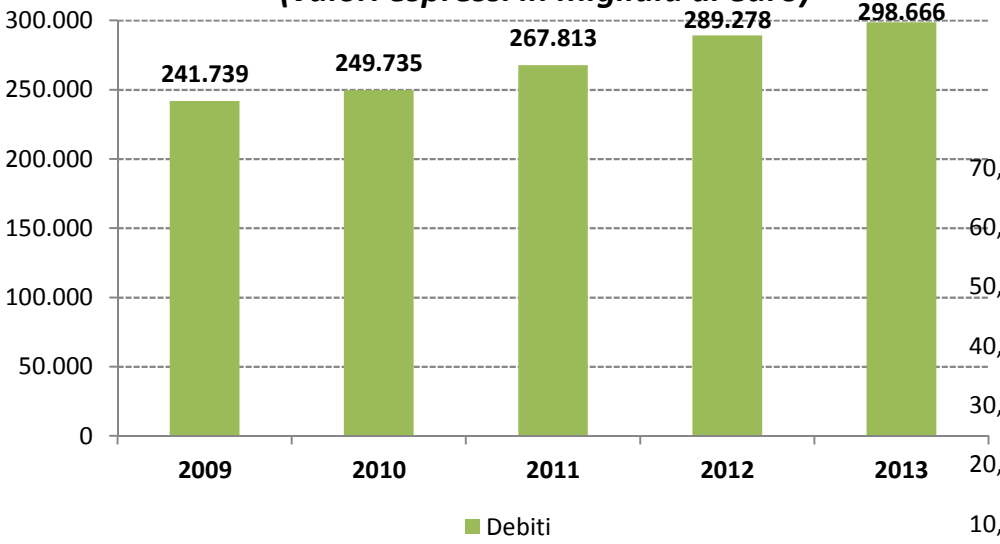
- A fronte di un incremento del volume di affari e del risultato operativo, l'utile delle imprese monitorate risulta in calo di circa 30 punti percentuali anche se, rispetto al 2009, nel 2013 la quota di aziende che ha un risultato economico positivo aumenta, passando da circa il 76% delle imprese a poco più del 79%;
- Il calo complessivo dell'utile deve leggersi come un'oggettiva difficoltà delle imprese nel guadagnare quote di mercato che consentano un adeguamento all'incidenza dell'incremento dei costi sul fatturato;
- Ciò può essere imputabile a diversi fattori tra cui: l'elevata competizione nel settore (che si gioca anche sui prezzi dei prodotti software), la gestione dei processi interni, la necessità di investimenti in risorse umane e servizi.

FOCUS SULLE PERFORMANCE DI UN CAMPIONE DI IMPRESE

I debiti

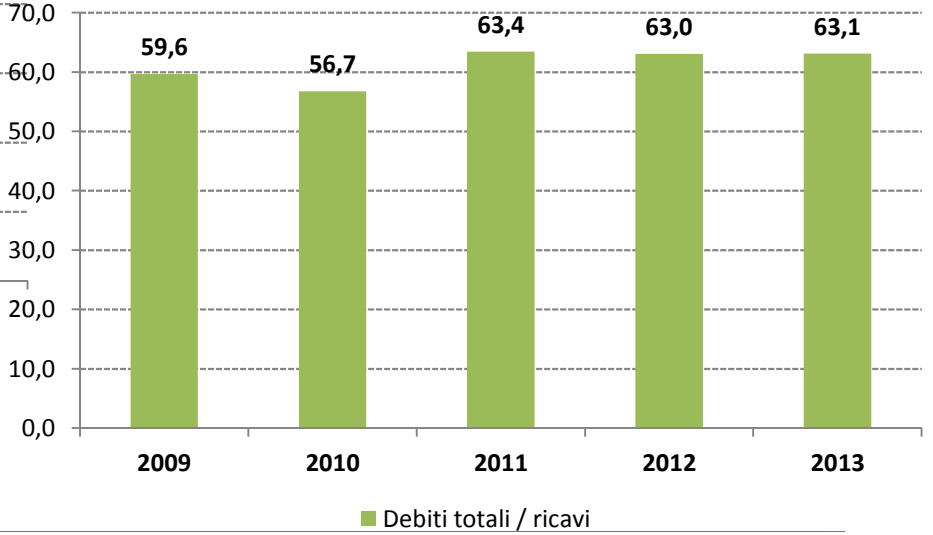
• L'analisi relativa ai debiti contratti dalle imprese evidenzia un indebitamento in aumento sia in termini assoluti che come incidenza sui ricavi delle vendite.

I debiti totali: serie storica dal 2009 al 2013
(valori espressi in migliaia di euro)



Var. % 2013/2009: +23,5%

Incidenza dei debiti sui ricavi delle vendite: serie storica dal 2009 al 2013

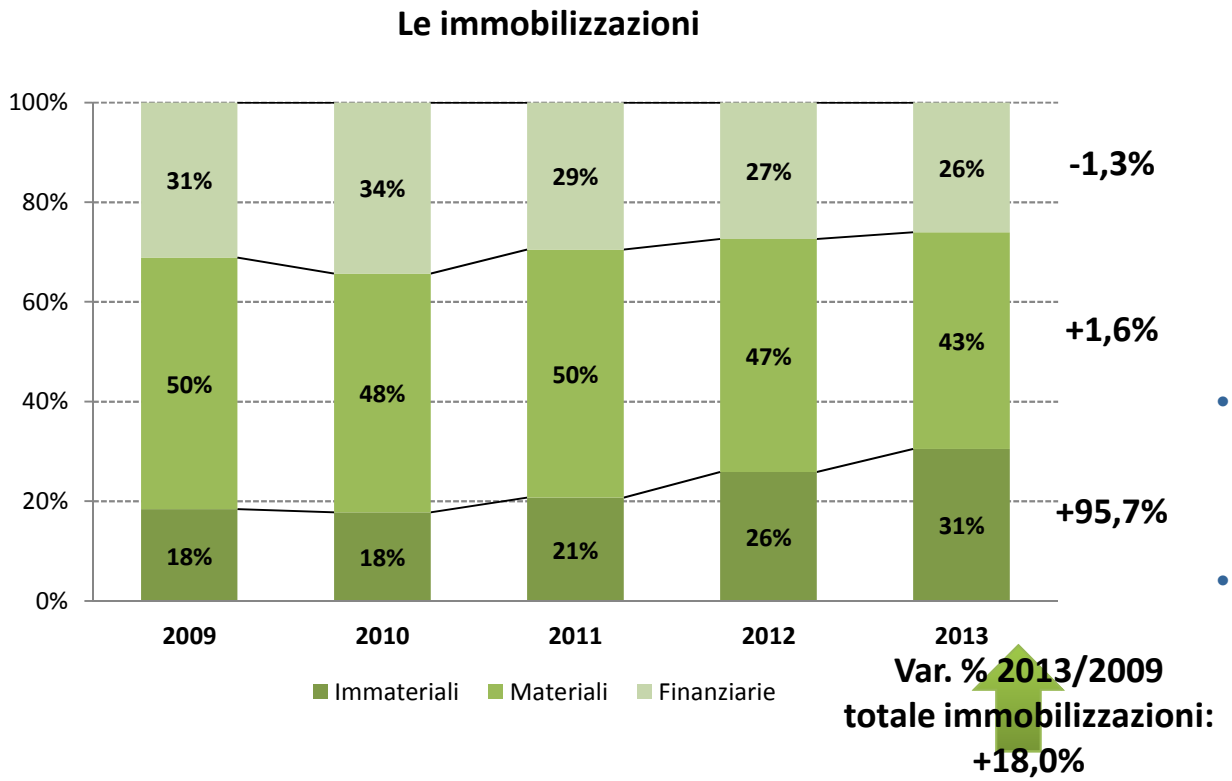


Fonte: elaborazioni Nomisma su dati Aida - Bureau van Dijk

FOCUS SULLE PERFORMANCE DI UN CAMPIONE DI IMPRESE

nomisma.it

Le immobilizzazioni



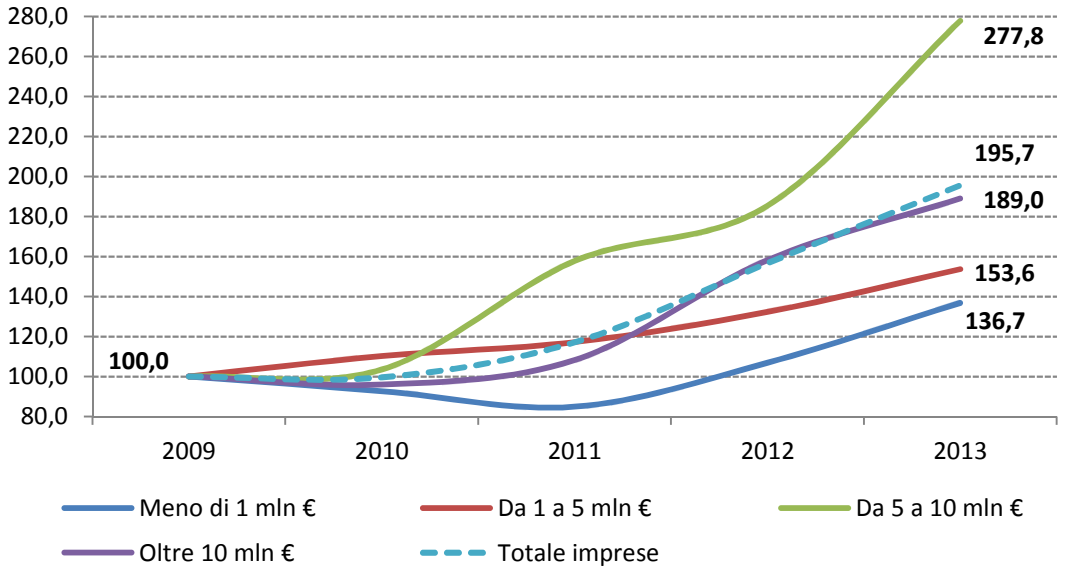
- A fronte di un aumento del totale delle immobilizzazioni pari al +18,0%, le immobilizzazioni immateriali crescono del 95,7%, mentre le immobilizzazioni materiali e quelle finanziarie non evidenziano sostanziali cambiamenti (+1,6% e -1,3%, rispettivamente). La quota delle immobilizzazioni immateriali su quelle totali passa così dal 18% del 2009 al 31% del 2013.
- L'incremento delle immobilizzazioni deve leggersi come una propensione delle imprese agli investimenti in R&S, brevetti, licenze, diritti, ecc;
- Tale propensione dimostra la potenzialità che le imprese hanno nel sedimentare in un innalzamento della qualità industriale del Sistema Paese.

Fonte: elaborazioni Nomisma su dati Aida - Bureau van Dijk

Le immobilizzazioni immateriali

•La dimensione in termini di ricavi delle vendite sembra giocare un ruolo determinante in relazione all'evoluzione della dinamica delle immobilizzazioni di beni non tangibili: sono infatti le imprese che presentano un volume di affari maggiore a evidenziare una crescita più sostenuta nel quadriennio considerato (+177,8% le imprese con ricavi compresi a 5 a 10 milioni di euro e + 89,0% quelle con ricavi superiori ai 10 milioni di euro)

Dinamica delle immobilizzazioni immateriali per classe di ricavi delle vendite – Anno base 2009=100. *Anni 2009-2013*



Fonte: elaborazioni Nomisma su dati Aida - Bureau van Dijk

5. PROTEZIONE O PROTEZIONISMO?

La minaccia protezionistica

- Come documentato da BSA – Business Software Alliance - nel 2012 in "*Lockout How a New Wave of Trade Protectionism Is Spreading through the World's Fastest-Growing IT Markets — and What to Do about It*" una nuova ondata di protezionismo digitale sta prendendo piede in molti paesi del mondo.

- Il fenomeno non riguarda solo l'imposizione di barriere commerciali evidenti, ma anche restrizioni al flusso di dati commerciali attraverso le frontiere, certificazioni tecnologiche nazionalistiche, politiche per gli standard tecnici che distorcono la concorrenza internazionale, favoritismi nei confronti di prodotti IT locali negli appalti pubblici, diffusa violazione della proprietà intellettuale.

- Queste e altre nuove forme di protezionismo IT focalizzata minacciano di inibire il commercio digitale, soffocare l'innovazione e rallentare la crescita economica a scapito di imprese e clienti in tutto il mondo.

- Le proposte di BSA per la liberalizzazione del commercio volte a rafforzare l'IT a livello globale:
  - (1) **Modernizzare le regole del commercio per promuovere il commercio digitale**. Gli accordi commerciali devono garantire che i dati possano superare i confini con poche restrizioni.
  - (2) **Promuovere l'innovazione tecnologica**. Gli accordi commerciali devono fornire robuste protezioni della proprietà intellettuale.
  - (3) **Definire parità di condizioni.** Gli accordi commerciali devono aprire gli appalti pubblici.

PROTEZIONE O PROTEZIONISMO?

Non solo PVS

- Anche Brookings ha dedicato molto attenzione al tema del protezionismo degli Stati in campo IT (Allan A. Friedman "*Cybersecurity and Trade: National Policies, Global and Local Consequences*" Brookings Institution, 2013)

- Il Canada ha recentemente emesso un bando per consolidare le molteplici piattaforme di posta elettronica non interoperabili in un unico sistema. Il Paese ha introdotto diverse misure che potrebbero essere viste come discriminatorie, tra cui la limitazione delle offerte a imprese canadesi, o consociate canadesi, richiedendo che il personale sia composto da cittadini canadesi. Il Paese ha spiegato che la priorità nazionale è " creare una infrastruttura di comunicazione centralizzata sicura" e ha quindi invocato l' Eccezione per la Sicurezza Nazionale agli scambi commerciali.

- Il Congresso degli Stati Uniti ha dichiarato che le quattro agenzie governative, tra cui i Dipartimenti del Commercio e della Giustizia, non possono comprare "sistemi informatici prodotti, fabbricati o assemblati" da entità "di proprietà, diretta o sovvenzionati dalla Repubblica popolare cinese" a meno che il capo dell'agenzia di acquisto, dopo una consultazione con l'FBI, determini che l'acquisto è "nell'interesse nazionale degli Stati Uniti".

- Le questioni in materia di sicurezza informatica recenti mostrano che, mentre alcuni membri dell'OMC hanno una visione alta della sicurezza nazionale quando essa riguarda l'attività all'interno dei loro Paesi, gli stessi sono contrari al medesimo grado di flessibilità quando esercitato da altri Paesi.

I 5 dilemmi della NATO

- La NATO (Klimberg, Alexander (ed). "*National Cyber Security Framework Manual*" NATO CCD COE Publications. December 2012). evidenzia come la sicurezza nazionale informatica sia uno strumento per raggiungere uno stato desiderato di cose, non un fine in sé.

- La maggior parte delle nazioni definisce un obiettivo strategico per un ambiente sicuro e protetto entro il quale si possa raggiungere il pieno potenziale economico e proteggere i cittadini dalle vari rischi cyber e non, sia interni che esteri.

- Per raggiungere questo obiettivo, la National Cyber Security deve fare i conti con il proprio set di "dilemmi nazionali di sicurezza informatica":

  - Stimolare l'economia vs. migliorare la sicurezza nazionale
  - Modernizzazione delle infrastrutture vs. protezione delle infrastrutture critiche
  - Settore privato vs. Settore Pubblico
  - Protezione dei dati vs. condivisione delle informazioni
  - Libertà di espressione vs. stabilità politica

- Mentre le nazioni e le organizzazioni intergovernative impostano lo sviluppo e l'attuazione delle misure nell'ambito di strategie di National Cyber Security, essi devono bilanciare l'importanza economica e sociale del libero flusso di informazioni con le esigenze di sicurezza del governo, dell'industria e dei cittadini.

6. POLITICA INDUSTRIALE PER IL SETTORE IT SECURITY

Indicazioni dall'OECD

- Il Rapporto dell'OECD "*Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*" del 2012 raccomanda lo sviluppo di iniziative di politica industriale per la sicurezza informatica come accade in Francia, Regno Unito, Stati Uniti, Spagna. Parecchie strategie includono gli appalti pubblici come strumento per aiutare le PMI della cyber security.

- La Francia mira a sostenere le PMI innovative nel settore della sicurezza. La cyber security è uno dei 34 settori prioritari per lo sviluppo del Paese.

- Gli Stati Uniti con DoD intendono "promuovere opportunità per le PMI e il lavoro con gli imprenditori della Silicon Valley e altri poli di innovazione tecnologica degli Stati Uniti [...] ".

- La strategia del 2011 del Regno Unito ha esplorato le modalità per rendere l'esperienza di GCHQ (Government Communications Headquarters) fruibile per la crescita economica del Paese e per sostenere lo sviluppo del settore della sicurezza informatica senza compromettere la sua missione.

- La Spagna sottolinea la necessità di sostenere lo sviluppo di aziende private nazionali in questo settore strategico "dove la dipendenza da imprese estere potrebbe essere pericolosa".

- La Germania ha identificato la ricerca su approcci innovativi per la sicurezza IT tra gli obiettivi prioritari. Questo programma di finanziamento della ricerca scientifica e tecnologica a lungo termine si concentra sul rafforzamento della posizione della Germania come sede di impianti industriali e la protezione dei dati e la privacy dei suoi cittadini.

Politica industriale in Italia: il CINI

- Il CINI (Consorzio Interuniversitario Nazionale per l'Informatica) costituisce in Italia il principale punto di riferimento della ricerca accademica nazionale nei settori dell'Informatica e dell'Information Technology.

- Costituito nel 1989, il CINI è posto sotto la vigilanza del Ministero competente per l'Università e la Ricerca. Il Consorzio è costituito da 39 Università pubbliche con oltre 1.300 Docenti coinvolti, afferenti ai Settori Scientifico Disciplinari INF/01 e ING-INF/05.

- Il Consorzio promuove e coordina attività scientifiche, di ricerca e di trasferimento, sia di base sia applicative, nel campo dell'informatica, di concerto con le comunità scientifiche nazionali di riferimento.

- Il CINI è attualmente dotato di 7 Laboratori nazionali, di cui uno dedicato alla Cyber Security . L'eccellenza Nazionale in ambito sicurezza oggi è ben verificabile a livello scientifico e industriale e vanta una presenza significativa distribuita su vari territori Regionali. Questa eccellenza, se ben coordinata e supportata da una efficace rete Nazionale, potrà avere importanti riflessi e ricadute specifiche. Questo rende l'Italia un terreno fertile per le iniziative di sicurezza informatica, che potrebbero essere una fonte di occupazione per le generazioni attuali e prossime.

- Il Laboratorio Nazionale CINI di Cyber Security si propone di coordinare questa rete e di proporre azioni a livello Nazionale e Internazionale, aiutare il sistema Paese nel territorio ad essere più resiliente alla minaccia cibernetica, migliorando la continuità di servizio dei sistemi critici, aumentando la consapevolezza nella società, migliorando le misure di protezione da attacchi cibernetici della pubblica amministrazione e delle imprese e supportando processi di definizione di standard e framework metodologici a livello Nazionale. Il tutto armonizzato con le istituzione Europee ed il programma Horizon 2020.

Collaborazione Accademia Dipartimento Informazioni per al Sicurezza

- L'Ambasciatore Giampiero Massolo, Direttore Generale del Dipartimento delle Informazioni per la Sicurezza (Presidenza del Consiglio dei Ministri), e il Presidente del CINI Professor Paolo Prinetto hanno firmato un accordo di collaborazione triennale sul tema della Cyber Security incentrato su iniziative progettuali, scientifiche e di formazione. L'accordo sarà centrato sul Laboratorio Nazionale di cyber security.

7. CONCLUSIONI PER UN PERCORSO

CONCLUSIONI

Il percorso

- Ciò che emerge dalle analisi effettuate è un quadro in cui vi sono punti di forza e potenzialità molto rilevanti.

- I punti di forza comprendono un sistema industriale dedicato alla sicurezza cibernetica che – pur avendo sofferto durante la crisi - ha le capacità e le risorse per riorganizzarsi e continuare a crescere. Comprende anche un produttore di conoscenza (l'accademia) che ha compreso da tempo la rilevanza del tema e su questo ha investito. Comprende, infine, un settore pubblico sensibile al tema e sul punto di avviare una nuova stagione di investimenti importanti con i Fondi europei 2014-2020 .

- Le potenzialità sono purtroppo legate alla rapida evoluzione degli eventi negativi in ambito cyber e quindi alla necessità di dare risposte rapide ed efficaci al problema.

- Non mancano però gli aspetti critici.
  - In primo luogo una domanda scarsamente consapevole, soprattutto se espressa da imprese ed enti di piccole dimensioni, molto contenuta rispetto al rischio effettivo, come emerge con evidenza dalla ricerca realizzata da Nomisma per il Dipartimento delle Informazioni per la Sicurezza lo scorso anno ("Percezione della minaccia cibernetica nelle imprese italiane").
  - In secondo luogo una declinazione ancora poco chiara circa il ruolo le imprese della sicurezza cyber possono giocare all'interno della partnership pubblico-privato più volte auspicata nei documenti strategici del Governo.
  - In terzo luogo i vincoli stringenti (patto di stabilità, spending review) che limitano la capacità di spesa della PA (locale, in particolare).

- Un percorso virtuoso è possibile. C'è ancora ampio spazio di azione e sperimentazione su un fronte molto delicato volto a coniugare la tutela della concorrenza con la sicurezza del dato. L'Agenda Digitale italiana, anche con il supporto delle risorse comunitarie della nuova programmazione, può rappresentare il contesto ideale attraverso cui avviare una efficace collaborazione pubblico-privato in tale direzione.