POLITECNICO MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET digital innovation

Osservatorio Information Security & Privacy

# Cyber Crime: La minaccia invisibile che cambia il mondo

Febbraio 2017

# Indice

# Introduzione

La trasformazione digitale delle imprese, guidata dai trend emergenti come i big data, il cloud, l'internet of things, il mobile e i social, richiede nuove tecnologie, modelli organizzativi, competenze e regole per garantire insieme l'innovazione e la protezione degli asset informativi aziendali.

In questo scenario si muove l'Osservatorio Information Security & Privacy – promosso dalla School of Management del Politecnico di Milano – in collaborazione con CEFRIEL e DEIB e con il patrocinio di CLUSIT, Associazione Italiana per la Sicurezza Informatica, AUSED ed Europrivacy.

L'Osservatorio intende rispondere al bisogno di conoscere, comprendere e affrontare le principali problematiche dell'information security & privacy e monitorare l'utilizzo di nuove tecniche e tecnologie a supporto di tale area da parte delle aziende end user, creando una community permanente di confronto.
La Ricerca 2016 dell'Osservatorio, al secondo anno di attività, ha previsto una Survey di rilevazione che ha coinvolto 951 CISO, CSO e CIO di imprese italiane. In particolare sono state coinvolte 148 organizzazioni grandi (>249 addetti) e 803 PMI (tra 10 e 249 addetti).

L'Osservatorio ha inoltre attivato un tavolo di confronto permanente, dedicato alle grandi aziende operanti in Italia (prime 1000 organizzazioni per fatturato) con l'obiettivo di indirizzare, monitorare e validare i risultati della Ricerca. Nel corso del 2016 sono stati organizzati, a tal proposito, quattro Workshop che hanno visto la partecipazione di 220 decisori aziendali delle

principali aziende operanti in Italia e dei player dell'offerta. È stato inoltre organizzato un incontro di approfondimento sulle implicazioni del General Data Protection Regulation (GDPR) per le organizzazioni italiane che ha visto la partecipazione di oltre 570 executive.

Gli obiettivi della Ricerca 2016 sono stati i seguenti:

- Quantificare il mercato della sicurezza informatica in Italia;
- Indagare come i nuovi trend dell'innovazione digitali come il Cloud, i Big Data, l'Internet of Things e il Mobile impattano sulla gestione dell'information security e della privacy;
- Identificare le principali tendenze internazionali in ambito Information Security & Privacy;
- Comprendere l'impatto del Regolamento UE sulla privacy;
- Monitorare lo stato di adozione di sistemi di Information Security e privacy nelle organizzazioni italiane;
- Studiare gli impatti sulle grandi imprese e sulle PMI;
- Identificare i casi di successo.

*Comitato Scientifico*

***Umberto Bertelè***
*Chairman degli Osservatori Digital Innovation*

***Alessandro Perego***
*Direttore Scientifico Osservatori Digital Innovation*

***Raffaello Balocco***
*Comitato Scientifico Osservatori Digital Innovation*

***Mariano Corso***
*Comitato Scientifico Osservatori Digital Innovation*

**I risultati completi della Ricerca sono consultabili su www.osservatori.net**

POLITECNICO MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET digital innovation

## Osservatorio Information Security & Privacy

# Cyber Crime: La minaccia invisibile che cambia il mondo

# La Ricerca

Febbraio 2017

# Executive Summary

## L'anno degli attacchi

Il 2016 verrà con buona probabilità ricordato come l'anno dell'Hack. In primis le rivelazioni di Yahoo, che ha prima reso pubblico di aver scoperto solo nel corso dell'anno una violazione risalente al 2014 che ha interessato 500 milioni di account, poi ammesso di aver subito un attacco ancora più grave nell'agosto 2013, che ha coinvolto oltre un miliardo di utenti.

Gli ultimi mesi hanno visto aumentare drasticamente l'attenzione al cybercrime in seguito a quanto emerso durante le elezioni presidenziali americane, dove si ritiene che vi possano essere state azioni di cyberspionaggio in grado di influenzare l'esito delle consultazioni.

Vi è stata inoltre una continua e progressiva crescita dei ransomware – una particolare minaccia che richiede il pagamento di una somma per rientrare in possesso dei propri dati – che si sono diffusi in differenti varianti, in grado di colpire anche dispositivi mobile.

Gli stessi device smart connessi all'internet of things sono diventati veicolo di possibili minacce; è il caso dell'attacco DDoS (Distributed Denial of Service) di ottobre che ha colpito Dyn, uno dei principali DNS provider, causando l'impossibilità di accedere a servizi quali, ad esempio, Netflix e Twitter. In questo caso, infatti, l'attacco è stato causato dalla breccia in decine di migliaia di device di videosorveglianza che, infettati da un malware, sono diventati agenti in grado di mettere fuori uso i server del provider.

Solo un mese dopo, in novembre, un altro attacco DDoS rilevante è stato compiuto in Finlandia, dove i sistemi di automazione di due edifici sono stati messi fuori uso, impendendo di controllare da remoto sistemi quali il riscaldamento e la ventilazione.

Per fornire un ulteriore esempio di violazione è opportuno citare anche l'attacco condotto ai danni di Tesco Bank, che ha comportato la perdita di alcune centinaia di sterline dal proprio conto per 9000 clienti. Questo incidente è particolarmente rilevante perché in questo caso sono concretamente evidenti i danni al consumatore, che solitamente viene tenuto all'oscuro del fatto che i propri dati siano stati trafugati.

## Il mercato delle soluzioni di information security in Italia

Nel rapporto di Ricerca dell'Osservatorio dello scorso anno si evidenziava una crescente consapevolezza da parte delle imprese rispetto alle sfide dell'information security, sebbene solo una parte limitata delle realtà interpellate avesse definito strategia e piani concreti. Il secondo anno di Ricerca approfondisce le scelte delle organizzazioni e analizza le principali aree di investimento, con particolare attenzione ai nuovi trend dell'innovazione digitale e il percorso di adeguamento alle nuove regolamentazioni europee riguardanti la privacy. L'Osservatorio, al suo secondo anno di attività, ha coinvolto nella rilevazione 951 organizzazioni italiane di differenti dimensioni, 148 grandi imprese (sopra i 249 addetti) e 803 PMI (tra 10 e 249 addetti).

L'analisi di un ampio campione di imprese e il coinvolgimento delle principali aziende dell'offerta di security ha inoltre permesso di stimare il mercato delle soluzioni di information security in Italia, che nel 2016 vale 972 milioni di Euro, con tasso di crescita del 5% sul

2015, sostanzialmente allineato a ciò che avviene a livello internazionale[1]. Questo dato tuttavia non rassicura, la crescita esponenziale delle minacce richiede infatti una spinta molto più decisa verso la tutela del patrimonio informativo delle organizzazioni.

[1] Gartner stima per il mercato globale dell'information security nel 2016 un valore di 81,6 miliardi di dollari, con un tasso di crescita del 7,9%.

La spesa è concentrata nelle grandi imprese, che catalizzano il 74% della cifra complessiva. Il mercato preso in considerazione si riferisce alla spesa in information security delle organizzazioni con almeno dieci addetti ed è suddivisibile in tecnologia (28%), servizi di integrazione IT e consulenza (29%), software (28%) e managed services (15%).

## Dalla consapevolezza alla realizzazione di una strategia di gestione della sicurezza e della privacy

La possibilità di mettere in campo piani ed azioni concrete, con uno scope che non si limiti al solo ambito tecnologico, richiede una consapevolezza organizzativa chiara rispetto alla necessità di un approccio di lungo periodo alla gestione dell'information security e privacy. Da questa presa di coscienza discende la necessità di strutturare un'organizzazione con ruoli di governance ed indirizzo che sia in grado di sviluppare una strategia ben delineata per la gestione dell'information security & privacy, e di allinearla alle esigenze del business.

Il piano strategico, definito e concordato con il top management aziendale, esplicita ad alto livello come l'organizzazione intende governare le minacce e come si propone di garantire la sicurezza delle informazioni aziendali sensibili. Una volta stabilite le linee di indirizzo si identifica un framework, sulla base di modelli di riferimento e specificità del settore dell'impresa. Il piano necessita di essere comunicato in modo chiaro all'interno dell'organizzazione

e di essere revisionato continuativamente, per identificare la coerenza con il piano strategico e l'individuazione di aree di intervento. La capacità di circoscrivere processi e procedure di valutazione del rischio, che sappiano localizzare e analizzare le diverse minacce basate sul profilo di rischio dell'organizzazione, diventa fondamentale per mettere in atto misure efficaci in grado di mantenere i rischi all'interno di limiti accettabili.

Il paradigma di gestione della sicurezza sta cambiando nel corso del tempo, passando progressivamente da una gestione perimetrale ad un approccio maggiormente incentrato sul dato. La maggior consapevolezza della complessità intrinseca in un mondo dove il digitale è sempre più pervasivo nei processi aziendali conduce ad una trasformazione: da una visione legata alla mera compliance si passa alla gestione del rischio e della sua mitigazione, tramite il controllo dell'intero ciclo di vita dell'informazione. Cambia l'approccio al fattore umano, alla persona da sensibilizzare ed incoraggiare a comportamenti responsabili. I progetti e le azioni messe in campo possono essere di svariato tipo e possono orientarsi ad anticipare possibili minacce o a mitigarne gli effetti. Oggi, accanto alla capacità di prevenire e contrastare gli attacchi, è sempre più richiesto di saperli predire, monitorare e di saper rispondere in modo tempestivo ed efficace. L'identificazione di metriche di monitoraggio e di misurazione delle performance serve poi a identificare azioni correttive e a mettere in atto miglioramenti nei processi di governo della security e nella revisione del piano nel suo complesso. Infine, l'approvazione della nuova regolamentazione europea sulla privacy (General Data Protection Regulation – GDPR) richiede di analizzare le implicazioni per la sicurezza e di mettere in atto conseguentemente misure tecnologiche, organizzative e di processo.

Con riferimento al campione di analisi di grandi imprese, solo il 18% delle organizzazioni ha messo in campo un piano di investimento con orizzonte pluriennale con inserimento di riferi-

menti espliciti nel piano industriale (nelle aziende quotate con maggiore capitalizzazione si arriva al 58%). Un ulteriore 21% ha sempre un piano pluriennale, senza però nessun richiamo nel piano industriale. Nel 34% dei casi vi è un piano con orizzonte annuale, mentre nel 27% restante il budget viene stanziato solo all'occorrenza. Rispetto allo scorso anno il quadro mostra una maggiore consapevolezza, con un 7% in più di organizzazioni che hanno predisposto un piano pluriennale.

## L'evoluzione del Ruolo del Chief Information Security Officer (CISO)

La bontà di un piano strategico di gestione della security e della privacy passa necessariamente dal disegno di una struttura di governo chiara: al suo interno le responsabilità devono essere definite in modo univoco, così come le competenze necessarie a svolgere uno specifico compito e i meccanismi di misura e monitoraggio della qualità dei processi, delle soluzioni tecnologiche e delle policy messe in atto. Concentrandosi sull'aspetto di information security, appare evidente la necessità di identificare un profilo direzionale, un capo della sicurezza, che viene comunemente chiamato Chief Information Security Officer (CISO).

Tuttavia, nel campione di grandi imprese analizzato, emerge come solo nel 46% dei casi sia presente in modo formalizzata la figura del CISO, nel 12% vi sia una presenza non formalizzata, mentre in un ulteriore 9% ne sia prevista l'introduzione nei prossimi 12 mesi. Nei restanti casi non esiste una figura dedicata ed il presidio dell'information security è demandato direttamente al Chief Information Officer (28%) o a figure esterne all' ICT (5%).

Il "ritardo" della situazione italiana si conferma focalizzandosi sulle organizzazioni dove il CISO è presente: nel 65% dei casi infatti tale figura fa parte della direzione ICT e fa riferi-

mento al CIO. Solo in un 10% dei casi si tratta di una figura che si rapporta direttamente al board aziendale, mentre nelle restanti situazioni vi sono differenti possibilità: in taluni casi (7%) il CISO riporta ad una funzione Security corporate (che si occupa di sicurezza sia fisica sia logica), a Risk Management (4%), Operations (4%), o in casi marginali a Compliance, Finance o altre strutture.

Il ruolo del Chief Information Security Officer (CISO) sta evolvendo verso un profilo completo, che affianca alle competenze tecnologiche e organizzative soft skill relazionali, conoscenze del dominio di business e capacità di sviluppare e governare un team complesso. Oggi aumentare la consapevolezza delle problematiche di cybersecurity richiede sempre più la capacità di comprendere il business, interfacciandosi con i responsabili di prodotto, e di comunicare al top management i rischi derivanti dalle nuove minacce con una visione sistemica. Le conoscenze di industry diventano distintive, a fronte di obblighi di compliance, legislazioni e minacce sempre più focalizzate su settori di mercato ben identificati. Dotarsi di competenze tecnologiche eterogenee richiede una progressiva strutturazione di ruoli e strumenti di governo: diventa fondamentale sviluppare capacità di project management e di gestione e sviluppo del capitale umano.

Identificare il corretto mix delle competenze appena citate non è semplice e non è univocamente valido per tutte le situazioni. Il ruolo ricoperto dal CISO può essere maggiormente strategico, non limitandosi esclusivamente a compiti tecnici, e richiedere maggiore relazione con il management aziendale; in questi casi le competenze relazionali e di business diventano fondamentali. L'attività, inoltre, può essere orientata alla mera gestione e monitoraggio del servizio, e quindi essere incentrata sulla gestione dei processi e delle tecnologie. Infine ci può essere un ruolo di stampo manageriale, con la responsabilità di controllo e supervisione di persone afferenti ad aree di sapere diverse, dalla gestione del rischio alla compliance e privacy.

## I progetti e le policy per gestire il cambiamento

Come evidenziano diversi framework di riferimento[2], esistono diffenti aspetti da prendere in considerazione per una gestione consapevole dell'information security: *identificare*, ovvero la capacità di comprendere come gestire il rischio cyber; *proteggere*, la capacità di sviluppare ed implementare misure di sicurezza in grado di garantire la corretta erogazione dei servizi; *rilevare*, la capacità di svolgere le attività necessarie ad individuare l'accadimento di un evento di cybersecurity; *rispondere*, la capacità di pianificare e mettere in atto azioni in relazione ad un evento identificato; *ripristinare*, la capacità di gestire piani in grado di garantire la resilienza dei sistemi e la facoltà di riattivare i servizi in seguito ad un incidente. Questi aspetti non richiedono necessariamente un'implementazione sequenziale, ma fanno parte di un approccio complessivo orientato alla creazione di una cultura incentrata sulla gestione della cybersecurity. Per rispondere a tali esigenze è necessario mettere in campo progettualità tecnologiche e policy.

[2] Si prendono a riferimento in particolare le "Functions" del "Framework for improving Critical Infrastructure Cybersecurity" del NIST.

In merito alle progettualità messe in atto, con riferimento alle grandi imprese, quelle più diffuse nelle organizzazioni sono penetration test e data security (51%), network security (48%), application security (45%), endpoint security (43%), security information & event management (SIEM) (38%), messaging security (38%), web security (36%), identity governance & administration (IGA) (32%), threat intelligence (20%), transaction security (19%), social media security (16%).

In seguito si approfondiranno in dettaglio alcune progettualità legate ai nuovi trend dell'innovazione digitale e alle nuove esigenze: mobile security, cloud security, cyber intelligence, IoT security e cyber insurance.

Le policy più diffuse all'interno delle aziende riguardano il backup (89%), la gestione degli accessi logici (84%), la regolamentazione delle procedure di sicurezza informatica (80%), la gestione e l'utilizzo dei device aziendali (72%), la gestione del ciclo di vita del dato (58%), l'utilizzo di social media e web (57%), le azioni da mettere in atto in risposta agli incidenti informatici (52%), le policy di classificazione dei dati (52%) e di criptazione degli stessi (39%).

Con riferimento agli aspetti definiti, le progettualità e le policy messe in atto sono orientate principalmente all'*identificazione* e alla *protezione*, mentre risulta ancora in larga parte immaturo il supporto a *rilevazione*, *risposta* e *ripristino*.

## Le nuove esigenze di sicurezza e l'impatto dei nuovi trend dell'innovazione digitale

I trend emergenti dell'innovazione digitale pongono nuove sfide all'information security, in termini di progetti e policy da mettere in campo. Quest'anno l'Osservatorio ha approfondito l'impatto di quattro aspetti in particolare: il mobile, il cloud, l'internet of things e la data intelligence. Infine è stato dedicato un approfondimento agli aspetti legati all'assicurazione del rischio cyber, tendenza emergente nel panorama della gestione della sicurezza. Tutti questi fenomeni pongono ulteriormente in risalto gli aspetti legati alla sensibilizzazione dell'utente, di quello che possiamo chiamare il fattore umano, che deve essere gestito in modo strategico.

## La Mobile Security

I device mobili sono ormai uno strumento essenziale per ogni azienda, indipendentemente dalla sua dimensione o settore d'appartenenza. L'emergere di nuove modalità di lavoro, come ad esempio lo smart working, ha portato all'utilizzo sempre più massivo di dispositivi mobile oltre i normali confini aziendali.

Quasi la totalità delle aziende (97%) mette a disposizione dei propri dipendenti device mobili, siano essi notebook, smartphone, tablet o mobile business app, legate per esempio alla personal productivity (es. mail) e al supporto della forza vendita[3].

[3] Secondo quanto emerge dalla Ricerca 2016 dell'Osservatorio Smart Working del Politecnico di Milano.

Inoltre, sempre più spesso gli utenti utilizzano anche al di fuori dell'ambito lavorativo dispositivi mobili che contengono dati aziendali quali email, liste contatti, password, ecc. Nonostante questi dispositivi rappresentino un elemento fondamentale per favorire la collaborazione e incrementare la produttività, essi costituiscono allo stesso tempo una minaccia per la sicurezza aziendale.

I rischi connessi al mobile non riguardano soltanto il possibile furto o smarrimento dei device, con la conseguente perdita dei dati confidenziali in essi contenuti. La rapida diffusione dell'utilizzo di smartphone e tablet, infatti, ha portato con sé l'aumento degli attacchi cyber mirati a questi dispositivi. Negli ultimi anni il fenomeno del malware mobile è stato in costante crescita, sia tramite attacchi DDoS, ransomware e hacking, sia sotto forma di applicazioni mobile scaricabili dagli app store in cui gli sviluppatori criminali inseriscono volutamente codice malevolo: vere e proprie piattaforme di social engineering sfruttate dagli hacker per bypassare qualsiasi forma di sicurezza.

Dalla Ricerca emerge come il 74% delle grandi organizzazioni intervistate abbia già messo in campo iniziative specifiche volte a mitigare il rischio connesso alla mobile security, accanto ad un 7% che non ha ancora attuato né ha in previsione azioni e a un 19% che si colloca in fase di valutazione.

Le azioni che le aziende stanno implementando riguardano l'introduzione di piattaforme e strumenti tecnologici specifici, quali soluzioni di MDM (mobile device management) per governare/limitare l'utilizzo di device mobili (61%), ma anche la definizione standardizzata di regole a cui gli utilizzatori di dispositivi devono attenersi quando accedono ai sistemi e ai dati business. Il 27% delle organizzazioni ha infatti fissato norme che limitano l'accesso a particolari applicazioni e servizi da reti esterne all'azienda e il 61% ha stabilito specifiche policy per l'utilizzo dei device mobili.

## La Cloud Security

Il cloud computing negli ultimi anni è andato via via affermandosi come un trend sempre più essenziale per le aziende, sia per rendere il proprio sistema informativo più flessibile sia come abilitatore per l'utilizzo di altre tecnologie. Quando si affronta il tema della sicurezza nel cloud, il modello che preoccupa maggiormente le aziende è quello del public cloud, in cui l'infrastruttura è di proprietà di un service provider che eroga servizi ad aziende clienti. Gli investimenti infrastrutturali sono interamente sostenuti dal fornitore, mentre il cliente paga a consumo solamente per i servizi effettivamente fruiti.

Il modello public cloud permette alle aziende utenti di contenere i costi e di sperimentare dei servizi aggiornati e tecnologicamente avanzati direttamente attraverso il mercato;

in questo modo il time-to-market è significativamente ridotto rispetto all'implementazione interna tipica dell'IT tradizionale.

Il mercato del public cloud in Italia è in costante crescita: secondo le stime dell'Osservatorio Cloud & ICT as a Service del Politecnico di Milano, la spesa in public cloud nel 2016 si è attestata sui 587 milioni di Euro, con una crescita del 27% rispetto all'anno precedente. Stiamo quindi riferendoci ad un trend sempre più pervasivo per le imprese, che di conseguenza deve essere trattato con le dovute cautele.

La Ricerca mette in luce come le principali minacce legate alla sicurezza per gli ambienti cloud delle grandi imprese siano in larga parte riconducibili al rapporto col fornitore: il 63% degli intervistati evidenzia infatti la mancanza di controllo sulle operations del service provider, il 46% indica i problemi derivanti dal lock in col fornitore (in particolare riguardo alla migrazione dei dati), il 42% possibili data breach e la scarsa trasparenza rispetto agli obblighi contrattuali. È quindi evidente come non siano solo le minacce tecnologiche a preoccupare le aziende (es. vulnerabilità intrinseche nelle applicazioni cloud o legate a risorse condivise, advanced persistent threat o rischio di attacchi DDoS) ma anche gli aspetti che regolano la relazione cliente – fornitore, come la stesura del contratto e la definizione degli obblighi.

Accanto a soluzioni cloud di classe enterprise, esistono poi servizi di natura consumer, sempre più utilizzati dagli utenti in modo estemporaneo e non governato. Questo approccio mette in pericolo dati sensibili, poiché gli ambienti consumer non sempre sono progettati con standard di sicurezza paragonabili a quelli destinati al mercato enterprise.

Indagando il tema specifico con le grandi aziende emerge come il 57% cerchi di mitigare le minacce connesse agli ambienti cloud consumer limitando l'utilizzo solo ad alcuni servizi

specifici, il 17% tramite una policy comportamentale che ne regola l'uso, il 5% attraverso una piattaforma di gestione o monitoraggio dei suddetti servizi mentre il 30% delle imprese intervistate dichiara di non presidiare la tematica. Questi dati sono molto significativi: il fatto che quasi un'azienda su tre non si preoccupi di questo tema mette in evidenza come la sensibilità rispetto al trend sia ancora scarsamente diffusa.

## La Security e l'Internet of Things (IoT)

Un altro trend recente che sta raccogliendo un grande interesse da parte delle aziende è l'Internet of Things (IoT). Alla base dell'internet of things vi sono gli oggetti intelligenti (smart object), contraddistinti dal possedere una o più delle seguenti funzionalità:

- *self-awareness*, che comprende l'identificazione, ovvero il possesso di un identificativo digitale univoco; la localizzazione, ovvero la capacità di conoscere la propria posizione; e la diagnosi stato, ovvero la capacità di monitorare funzionamento e necessità di assistenza;
- *interazione con l'ambiente circostante*, che comprende l'acquisizione di dati tramite la misura di variabili di stato (sensing) – come la temperatura o la concentrazione di inquinanti – o di variabili di flusso (metering) – come il consumo di energia elettrica, gas, acqua e calore – e l'attuazione, ovvero la capacità di eseguire comandi;
- *elaborazione dati*, che può essere base (ad esempio filtraggio, calcolo di medie) o avanzata (ad esempio analisi statistiche, previsioni);
- *connessione* (wired o wireless) per trasportare l'informazione raccolta a livello locale. L'intelligenza non si ferma agli oggetti, ma si spinge fin dentro alla natura della rete che li interconnette: utilizzo di standard tecnologici aperti, accessibilità al dato e raggiungibilità degli oggetti, multifunzionalità sono proprietà chiave della rete intelligente (smart network).

A testimonianza dell'esplosione del trend è sufficiente considerare i dati del mercato, che nel 2015 è stato stimato intorno ai 2 miliardi di Euro, in aumento del 30% rispetto all'anno precedente secondo i dati dell'Osservatorio Internet of Things del Politecnico di Milano.

Oltre alle opportunità che possono offrire queste tecnologie è importante prestare attenzione alle implicazioni sulla sicurezza, poiché aumentando il numero di dispositivi connessi alla rete aumenta anche il numero di possibili punti di accesso per un eventuale attacco al sistema informativo aziendale.

Aumentando le potenzialità offerte dagli oggetti intelligenti dell'internet of things, infatti, crescono di pari passo anche le vulnerabilità. I protocolli di sicurezza per questi dispositivi, il più delle volte, non sono sviluppati con la stessa attenzione con cui viene creato lo strumento. Questo è un tema rilevante per il mondo del business to business, dove è possibile trovare sensori utilizzati per monitorare la produzione o tracciare il percorso della merce, ma anche per il mercato di largo consumo, poiché la maggior parte dei dispositivi che ogni giorno le persone portano con sé rilevano dati sensibili, come ad esempio le pulsazioni o gli spostamenti effettuati. Tutte queste informazioni possono facilitare la vita di tutti i giorni, ma espongono contestualmente gli individui a una potenziale perdita della propria privacy e le aziende a rischi legati alla perdita di dati o all'esposizione a terzi di informazioni sensibili.

Le rilevazioni dell'Osservatorio evidenziano come il 47% delle organizzazioni non abbia ancora messo in atto nessuna azione per tutelarsi e il 40% stia valutando delle possibili azioni. Il 12%, invece, ha adottato policy di security by design nella progettazione di prodotti, il

10% utilizza soluzioni tecnologiche specifiche, il 9% possiede policy legate alla rilevazione di dati nel perimetro aziendale e il 6% ha policy per la gestione di dati raccolti da oggetti smart.

È evidente la mancanza di linee guida da parte delle imprese anche per quanto riguarda il tema della security by design. Con questa espressione si intende un approccio per lo sviluppo software e hardware che cerca di mettere i sistemi in sicurezza rispetto ad attacchi e vulnerabilità impreviste, attraverso misure come il monitoraggio continuo, l'utilizzo di credenziali e l'aderenza a pratiche di programmazione migliori.

Si tratta di un approccio rivoluzionario, che capovolge completamente il punto di vista con cui si affronta un nuovo progetto: se di solito la sicurezza è un problema che si valuta a lavoro finito, con questa metodologia la questione viene invece presa in considerazione subito, sin dalle fondamenta del progetto. Questo cambio di prospettiva è fondamentale, poiché permette di mettere in campo strategie più efficaci, sviluppate in fase di progettazione, permettendo quindi di identificare le soluzioni migliori, adattando, se necessario, lo sviluppo ai parametri di sicurezza.

Sempre secondo la Ricerca, il 44% delle aziende non ha un presidio di alcun tipo per le tematiche connesse con l'internet of things, il 25% ha un presidio informale, il 17% ha un presidio formale e il 14% ha un presidio ma al di fuori delle attività core dell'information security. I dati confermano ancora una bassa sensibilità verso questo tema, dovuta ad una scarsa comprensione del fenomeno.

## La Cyber Intelligence

Considerato che le minacce informatiche stanno diventando sempre più parte integrante del tessuto digitale aziendale e che non è possibile attuare misure in grado di evitare con certezza una violazione della sicurezza, accanto all'approccio tradizionale basato sulla protezione dei sistemi le aziende stanno cominciando ad adottare una logica di anticipazione delle minacce. Le organizzazioni hanno infatti a disposizione una grande quantità di dati, che possono analizzare per cercare di sviluppare strategie di sicurezza.

A supporto dell'esplorazione di questo volume di dati vi sono metodologie di analytics che possono realizzare, attraverso l'utilizzo di nuovi modelli, analisi sempre più customizzate rispetto alle esigenze e maggiormente rispondenti. Secondo i dati dell'Osservatorio Big Data Analytics & Business Intelligence del Politecnico di Milano, il mercato analytics nel 2016 ha registrato una crescita pari al 15%, per un valore totale di 905 milioni di Euro. In particolare, la componente big data (implementazioni che impiegano dati caratterizzati da volume, velocità e varietà elevate) ha visto un incremento del 44%, raggiungendo i 183 milioni di Euro. Le applicazioni degli analytics trovano ampia diffusione nei settori più svariati: nell'ambito della sicurezza si parla di cyber intelligence. L'integrazione di dati provenienti da varie fonti (es. dati sugli incidenti avvenuti a livello mondiale, indirizzi IP, log, URL sospette provenienti dalle segnalazioni degli utenti, ecc.) permette di sviluppare modelli di monitoraggio delle minacce in grado di intercettare possibili anomalie e gestirle prima che la situazione diventi effettivamente critica. In alcune aziende esistono apposite strutture all'interno dei security operation center, che analizzano e correlano i dati in ottica di cyber intelligence.

Secondo i dati emersi dalla Ricerca, il tema dell'analisi dei dati legati al mondo dell'information security è presidiato dal 57% delle grandi organizzazioni intervistate, tramite l'esistenza di un pre-

sidio formale (28%) o informale (29%). Per l'8% delle aziende esiste un presidio, ma al di fuori delle attività core dell'information security e nel restante 35% dei casi il tema non è presidiato.

Il 32% delle imprese del campione dichiara di non utilizzare i dati per interpretare e/o anticipare criticità. Il restante 68%, invece, ha già implementato azioni in questo ambito. Il 20% delle organizzazioni utilizza i dati e li correla con diverse fonti informative ex ante per sviluppare modelli predittivi di monitoraggio delle minacce (threat intelligence). Il 23% li analizza in tempo reale per risolvere più velocemente una situazione di minaccia, mentre il 39% delle organizzazioni li analizza ex post in seguito ad incidenti per attività prevalentemente legate ad audit aziendali. Per il 31%, i dati relativi ad attacchi passati vengono inoltre analizzati per creare una base di conoscenza delle minacce e degli attacchi e sviluppare strategie di risposta/azione.

## La Cyber Insurance

La crescente complessità nella gestione della sicurezza e della mitigazione del rischio rende di particolare interesse il tema dell'assicurazione del rischio cyber. L'attivazione di una copertura può essere scatenata da diversi fattori:

- una violazione dei dati personali, legata all'accesso o alla trasmissione di dati personali;
- difetti di sicurezza, legati ad un'intrusione o ad una rivelazione di dati dovuta a furto;
- difetti legati a una omissione negligente durante uso o manutenzione del sistema informativo.

Il mercato dell'assicurazione del rischio cyber è ancora immaturo e lo scenario è in continuo cambiamento. La copertura del rischio cyber riguarda i danni causati direttamente al sottoscrittore o a terze parti. Le principali aree di copertura riguardano, a titolo esemplificativo:

- investigazione e gestione degli eventi. Comprende il coinvolgimento di esperti legali ed informatici e ha come obiettivo quello di coprire le spese relative alla comunicazione dell'attacco, all'identificazione delle modalità che hanno portato al difetto di sicurezza o negligenza, alla tutela della reputazione e alla mitigazione del danno;
- gestione istruttorie. Comprende le attività necessarie a produrre una risposta ad un controllo ufficiale da parte di autorità – quale ad esempio il garante privacy – in merito a sospetto utilizzo improprio di dati personali;
- copertura danni in seguito a richieste di terze parti o di danni subiti direttamente. Si parla di danni legati a violazioni di dati personali, a intrusioni oppure omesso/errato trattamento dei dati, oppure a danni derivanti da downtime di rete, interruzione di servizio, perdita di dati. Vi sono incluse coperture anche ad azioni cyber di tipo estorsivo (es. attacchi ransomware).

Dalla Ricerca emerge come le grandi organizzazioni siano ancora immature nell'utilizzo di coperture assicurative del rischio cyber. Solo il 15% delle imprese ha già attive coperture assicurative, sebbene solo nella metà dei casi si tratta di polizze espressamente orientate al rischio cyber, mentre nei restanti casi si tratta di coperture generaliste. Il 29% si dice in valutazione di coperture assicurative, mentre il 35% non ritiene sufficientemente maturo il mercato cyber insurance e il 21% non ritiene il problema rilevante.

## L'importanza del fattore umano e della sua gestione

Quando si parla di information security non si può tralasciare il cosiddetto *fattore X*, l'elemento di incertezza legato al comportamento umano. Molto spesso, infatti, i cybercriminali non utilizzano sistemi tecnologici particolarmente sofisticati, ma sfruttano aspetti del comportamento umano, come la distrazione o la mancanza di consapevolezza, per fare breccia nei sistemi aziendali. Basti pensare al phishing o ai sempre più diffusi attacchi ransomware che inducono l'utente a cliccare su un link malevolo, inserire dati personali oppure scaricare un allegato infetto. Per la stragrande maggioranza delle organizzazioni, il *fattore X* rappresenta una delle vulnerabilità che maggiormente incidono in negativo sulla sicurezza aziendale.

Per mitigare i rischi legati alla sicurezza informatica, le aziende non devono soltanto dotarsi di sistemi tecnologici, ma anche introdurre iniziative volte a educare, sensibilizzare e rendere consapevoli i propri dipendenti rispetto alle possibili minacce.

Secondo quanto emerge dalla Ricerca, il 95% delle grandi organizzazioni intervistate dichiara di aver messo in campo azioni specifiche per sensibilizzare gli utenti aziendali. Le iniziative più diffuse riguardano comunicazioni periodiche inviate ai dipendenti tramite mail (78%) e corsi di formazione (66%), che avvengono attraverso sessioni d'aula o e-learning. Nel 28% dei casi la formazione viene inoltre supportata dalla distribuzione spot di materiale informativo (voucher, booklet, cartellonistica). Per il 28% delle organizzazioni si tratta di veri e propri progetti strutturati di sensibilizzazione, che vengono messi in atto tramite l'utilizzo di diversi strumenti e coprono spesso un orizzonte pluriennale. Vengono inoltre effettuate attività di vulnerability assessment (28%) sui dipendenti aziendali, per esempio tramite l'invio di finte mail di phishing o simulazioni di attacchi informatici, che servono da un

lato a misurare il livello di consapevolezza dei dipendenti, dall'altro a testare l'efficacia delle iniziative già portate avanti.

In molti casi le iniziative si basano su una logica di gaming o puntano a ottenere un forte impatto emozionale sugli utenti, in modo da risultare maggiormente efficaci. Le azioni mirano ad agire sul comportamento dei dipendenti, a tutti i livelli, per aumentarne il livello di awareness, sia in ottica preventiva (es. utilizzo consapevole dei device mobili, gestione delle password, buone pratiche per evitare un incidente di sicurezza) sia di risposta alle minacce (es. riconoscimento di un attacco informatico).

## General Data Protection Regulation: il percorso delle organizzazioni italiane

La Ricerca, condotta tra settembre e novembre 2016, ha inoltre indagato come le imprese si stiano organizzando per adempiere agli obblighi derivanti dall'applicazione del General Data Protection Regulation, il regolamento europeo sulla protezione dei dati personali. Il testo del Regolamento è stato approvato in via definitiva il 14 aprile 2016 e pubblicato il 4 maggio 2016 sulla Gazzetta Ufficiale dell'Unione Europea. Il GDPR è quindi già divenuto realtà a tutti gli effetti per gli Stati membri dell'Unione, ma non si applicherà se non decorsi due anni dalla data dell'entrata in vigore (che decorrono dal ventesimo giorno dalla suddetta pubblicazione in Gazzetta Ufficiale), affinché i soggetti destinatari possano implementare quanto necessario per mettersi in regola. La Ricerca ha indagato quattro aspetti in particolare: l'*awareness*, il *budget dedicato*, i *cambiamenti organizzativi* in atto e le *azioni implementate*.

Dai dati emerge come l'*awareness* sia spesso limitata: il 23% del campione dichiara che le implicazioni del GDPR non sono note in dettaglio all'interno dell'organizzazione ed un ulteriore 22% che le specifiche della normativa sono conosciute nelle funzioni specialistiche, ma non è ancora un tema all'attenzione del vertice. In quasi la metà del campione (46%) è in corso un'analisi dei requisiti richiesti e dei piani di attuazione possibili. Solo nel 9% è già in corso un progetto strutturato di adeguamento alla normativa.

In pochi casi esiste un *budget dedicato* (nel 7% pluriennale, nell'8% annuale), nel 35% dei casi sarà stanziato a breve (entro i successivi 6 mesi), mentre nel restante 50% non è presente e non lo sarà neanche in futuro.

Anche i *cambiamenti organizzativi* sono ancora limitati, nel 12% dei casi si declinano nella definizione di nuovi ruoli oppure nell'identificazione di un team di lavoro trasversale (9%). Nel 34% dei casi attualmente non vi è stato nessun cambiamento ma sarà attuato nei prossimi 6 mesi, mentre nel restante 45% non sono previste modifiche nemmeno in futuro.

Tra le principali *azioni implementate* dalle organizzazioni vi sono assessment rispetto ai rischi privacy (42%), il coinvolgimento di consulenti esterni (39%), la definizione di responsabilità e owner di processo (26%), azioni informative verso Board e Top Management (25%), revisione profonda degli attuali sistemi di IT security (22%), ricerche e corsi di formazione (20%), definizione di nuovi processi decisionali e comportamentali (12%).

I risultati della Ricerca mostrano una fotografia di uno scenario in divenire, in cui le organizzazioni stanno progressivamente prendendo confidenza delle implicazioni della nuova regolamentazione. Il GDPR è ancora percepito perlopiù come una questione di carattere

legale, di cui si conoscono ancora in modo poco chiaro le concrete implicazioni dal punto di vista delle soluzioni di information security.

## La figura del Data Protection Officer (DPO)

Tra le novità di rilievo introdotte dal GDPR vi è la disciplina del ruolo e delle funzioni del responsabile della protezione dei dati, in inglese Data Protection Officer (DPO), la cui introduzione nelle organizzazioni è in alcuni casi obbligatoria. Nello specifico il GDPR prevede che il titolare del trattamento e il responsabile del trattamento debbano designare sistematicamente un responsabile della protezione dei dati ogniqualvolta:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e reati.

Il responsabile della protezione dei dati deve essere incaricato di svolgere diversi compiti anch'essi disciplinati dal GDPR. Tra i principali: informare e fornire consulenza al titolare o al responsabile nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; sorvegliare l'osservanza dei suddetti obblighi nonché delle politiche del titolare del trat-

tamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento; cooperare con l'autorità di controllo; fungere da punto di contatto per l'autorità di controllo rispetto a questioni connesse al trattamento ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Lo scorso 13 dicembre 2016 il Gruppo dei Garanti UE (WP29) ha pubblicato un documento contenente le linee guida sul DPO, specificando innanzitutto come la designazione di tale figura costituisca la base di un buon processo di adeguamento alla normativa e come egli possa al contempo agire da intermediario verso diversi interlocutori, tra cui le Autorità di controllo. Appare dunque evidente come il WP29, ancor prima di soffermarsi sulle ipotesi nelle quali la nomina del DPO assume carattere obbligatorio ai sensi della nuova disciplina, ritenga la designazione di tale figura una buona prassi e incoraggi l'individuazione di un Data Protection Officer anche da parte delle aziende che sarebbero esenti da tale adempimento. Le linee guida specificano inoltre che la funzione del DPO può essere svolta, su basi contrattuali, anche da persone fisiche o organizzazioni esterne al titolare o responsabile.

La Ricerca mostra che nel 18% dei casi la figura del DPO è formalizzata, nel 15% è una presenza di tipo informale. Il 31% del campione dichiara di volerla introdurre nei prossimi 12 mesi, mentre il restante 34% afferma che per il momento non saranno inserite figure di questo tipo. Nel 2% dei casi la responsabilità è delegata ad una figura esterna all'azienda.

## Alcuni suggerimenti per impostare un percorso di adeguamento al Regolamento UE n. 679/2016

Ad ormai otto mesi dall'entrata in vigore del Regolamento UE n. 679/2016 in materia di protezione dei dati personali (di seguito anche "GDPR" o "Regolamento"), molte organizzazioni hanno avviato progetti di adeguamento o stanno pianificando di farlo.

L'Osservatorio Information Security & Privacy del Politecnico di Milano ha avviato nel corso del 2016 un progetto di Ricerca con l'obiettivo di comprendere la portata innovativa del GDPR e fornire alle organizzazioni le prime indicazioni volte all'impostazione di un percorso di adeguamento mirato al raggiungimento della compliance, sfruttando il tempo a disposizione prima della sua piena applicabilità a maggio 2018.

L'attività di Ricerca ha innanzitutto analizzato nel dettaglio i contenuti del GDPR per approfondire, valutare e verificare le singole disposizioni normative e comprendere le innovazioni introdotte rispetto all'attuale normativa in materia di protezione dei dati personali. Questa analisi ha portato ad elaborare sia una vera e propria mappatura dei singoli articoli del Regolamento, in grado di offrire una base di confronto tra la presente e passata regolamentazione in materia di protezione dei dati personali, sia un possibile piano di adeguamento per le imprese, al fine di individuare le singole azioni da intraprendere per conformarsi ai nuovi obblighi introdotti.

Si forniscono di seguito alcune indicazioni utili, emerse nello svolgimento del lavoro, per impostare correttamente un progetto di adeguamento al GDPR.

Innanzitutto, si ritiene necessario un cambiamento di approccio alla normativa, che impone ai princi-

pali attori nei processi di trattamento di dati personali (titolari e responsabili) un onere di dimostrazione delle scelte effettuate e della loro idoneità rispetto ai requisiti del GDPR. Questo requisito definito nel Regolamento come "responsabilizzazione" ("accountability") era già stato preso in considerazione nel Parere 3/2010 del Gruppo di lavoro ex art. 29, nel quale si suggeriva l'attuazione di misure e procedure volte a rendere effettivi i principi di protezione dei dati esistenti, assicurandone l'efficacia e introducendo al contempo l'obbligo di dimostrarne il rispetto qualora le autorità di protezione dei dati ne facciano richiesta. Il primo richiamo è contenuto nell'art. 5 del Regolamento, dove non solo si individua nel titolare del trattamento il soggetto competente a garantire il rispetto dei principi applicabili al trattamento di dati personali (ovvero i principi di "liceità, correttezza e trasparenza", "limitazione della finalità", "minimizzazione dei dati", "esattezza limitazione della conservazione" e "integrità e riservatezza") ma si stabilisce che il medesimo debba essere anche "in grado di comprovarlo". Tale concetto è ulteriormente delineato dall'art. 24 dove si ribadisce che il titolare del trattamento viene gravato dell'obbligo di mettere in atto (nonché di riesaminare e di aggiornare) misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento. Tali misure devono essere attuate dal titolare del trattamento tenendo in considerazione tutta una serie di aspetti quali la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, nonché i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche e, ove ciò risulti proporzionato, le stesse devono includere l'attuazione di politiche adeguate in materia di protezione dei dati.

Alla luce delle precedenti considerazioni, dunque, si ritiene che l'accountability debba costituire lo strumento interpretativo dell'efficacia delle azioni intraprese per l'adeguamento al GDPR, imponendo un cambiamento di prospettiva nella gestione della protezione dei dati da parte delle organizzazioni che è poi ribadito in numerose altre norme. Si tratta, in sintesi, di creare un "sistema di gestione della data protection" che consenta di avere regole chiare e definite per la gestione dei singoli adempimenti, di documentare le scelte effettuate (es. la conservazione delle evidenze di ciò che si è fatto per ottenere un determinato

risultato) e l'effettuazione di verifiche circa la sua applicazione attraverso controlli sia da parte di soggetti interni ("internal audits") che esterni ("external audits"). Il GDPR lascia dunque maggiore discrezionalità ai titolari di decidere, in qualità di soggetti che determinano le finalità e i mezzi del trattamento di dati personali, le modalità attraverso le quali conformarsi alle sue disposizioni. La maggiore libertà è però gravata dall'onere di essere in grado di dimostrare le ragioni che hanno portato a tali decisioni e le motivazioni per cui si ritiene che le medesime abbiano consentito di raggiungere la conformità normativa.

Avendo chiarito il contesto all'interno del quale ci si dovrà muovere per impostare sin dall'inizio un progetto di adeguamento al GDPR, i risultati dalla Ricerca effettuata hanno portato ad ipotizzare un percorso che preveda i seguenti passi:

- *Predisposizione di un piano di intervento*: analisi organizzativa e documentale e predisposizione un piano di intervento per colmare i gap e adeguarsi alle nuove disposizioni del GDPR.
- *Impostazione del registro dei trattamenti*: è il cardine su cui basare l'intero adempimento al GDPR, anche se obbligatorio solo per organizzazioni con più di 250 dipendenti. È opportuno strutturare il registro in modo tale da renderlo sia uno strumento operativo di lavoro mediante il quale censire in maniera ordinata le banche dati e gli altri elementi rilevanti per assicurare un corretto «ciclo di gestione» dei dati personali, sia un documento probatorio mediante il quale il dimostrare di aver adempiuto alle prescrizioni del GDPR, nell'ottica del generale principio di accountability.
- *Stesura modifica documentazione*: individuare la documentazione mancante alla luce dei gap rilevati e aggiornare la documentazione esistente per renderla conforme alle disposizioni del GDPR.
- *Individuazione dei ruoli e delle responsabilità*: tale attività prevede l'individuazione dei responsabili del trattamento, nonché dei referenti per la gestione della data protection, la determinazione del contenuto dei contratti/atti giuridici vincolanti e l'impostazione di un sistema di controllo periodico per il monitoraggio costante della compliance al GDPR.
- *Definizione delle politiche di sicurezza e valutazione dei rischi*: il GDPR contiene continui richiami

al concetto di rischio (es. artt. 25, 32 e 35) e, dunque, alla necessità di definire le azioni da adottare prendendo in considerazione l'origine, la natura, la gravità del rischio stesso, nonché i costi di attuazione. In questa fase si ritiene opportuno analizzare la realtà organizzativa e definire la metodologia più adatta per la valutazione dei rischi nell'ambito della data protection, effettuare tale analisi e/o aggiornare quella eventualmente già esistente e, infine, definire un piano d'intervento per l'adozione delle misure necessarie a colmare i gap emersi.

- *Implementazione di un processo di data breach*: occorre strutturare il processo per la gestione delle violazioni e creare la documentazione di supporto (es. procedure di *incident management*). A tal fine, può risultare opportuno:
  - implementare un sistema di corretta gestione delle informazioni a supporto delle violazioni e delle indagini sottostanti;
  - impostare un registro delle violazioni;
  - creare la modulistica per la comunicazione al Garante per la protezione dei dati personali ed eventualmente agli interessati.
- *Valutazione d'impatto sulla protezione dei dati:* si tratta di un nuovo adempimento introdotto nel GDPR. Si suggerisce di esaminare le operazioni di trattamento effettuate all'interno della singola organizzazione che ricadono sotto la prescrizione normativa (anche alla luce di provvedimenti specifici che saranno approvati in materia) ed eventualmente effettuare le necessarie valutazioni d'impatto individuando la metodologia più appropriata e le misure (organizzative e tecniche) a mitigazione dei rischi.
- *Implementazione dei processi per l'esercizio dei diritti dell'interessato e la portabilità dei dati*: è necessario innanzitutto verificare la portata di tali obblighi in relazione alla specifiche caratteristiche dell'organizzazione e delle attività di trattamento svolte e successivamente valutare e implementare le misure tecniche ed organizzative volte a dare piena attuazione a tali diritti (anche alla luce delle linee guida emanate dal gruppo di lavoro dei Garanti Europei sulla portabilità dei dati).
- *Introduzione della figura del Data Protection Officer*: si tratta di una figura obbligatoria solo in al-

cuni casi espressamente richiamati dal GDPR. In questi casi e negli altri dove si ritiene comunque opportuno dotarsi di questa figura, occorre selezionarla accuratamente e affidargli i compiti previsti dal Regolamento, anche alla luce delle linee guida emanate dal gruppo di lavoro dei Garanti Europei.

## L'analisi delle PMI

La Ricerca ha visto il coinvolgimento di 803 PMI e ha analizzato la diffusione di soluzioni di information security, la spesa e la sua scomposizione, le motivazioni che guidano le scelte delle imprese, la tipologia di soluzioni messe in campo e la tipologia di approccio scelto per difendere l'organizzazione. Le soluzioni di information security sono ampiamente diffuse nelle PMI: il 93% delle imprese infatti dichiara di aver dedicato alla sicurezza un budget nel 2016, sebbene questo non corrisponda necessariamente ad un utilizzo maturo e consapevole.

Le principali motivazioni che guidano le scelte di spesa delle PMI sono l'adeguamento normativo (48%) e gli attacchi subiti in passato (35%). Talvolta, tuttavia, gli investimenti seguono la necessità di rispondere a nuove esigenze tecnologiche che richiedono di mettere in sicurezza i dati aziendali (22%), o a nuove esigenze di business (31%).

Al crescere della dimensione delle imprese, aumenta la necessità di adeguare i propri standard alle nuove esigenze tecnologiche: la percentuale di aziende che dichiara di essere

principalmente guidata da questo driver cresce infatti dal 21% delle piccole imprese (10-49 addetti), al 32% delle imprese di dimensioni maggiori (100-249 addetti).

L'analisi settoriale mostra come l'esigenza di adeguamento normativo sia la principale motivazione di spesa per ogni comparto esaminato. Il settore dei servizi risulta essere, in termini di spesa in information security, quello maggiormente guidato dalle esigenze di business (36%).

La maggior parte delle imprese disponde di soluzioni di sicurezza di base (76%) quali per esempio antivirus ed antispam ed il 62% dichiara di disporre anche di soluzioni sofisticate, come firewall o sistemi di intrusion detection. Un'organizzazione su quattro però (25%), si affida al buon senso dei propri dipendenti, senza seguire un approccio tecnologico definito. Il 46% delle imprese ha per contro policy aziendali ben definite, mentre solo il 10% ha programmi di formazione orientati ad aumentare la consapevolezza.

Le aziende del finance sono quelle caratterizzate da una maggior diffusione di soluzioni sofisticate (79%), mentre le aziende del settore telecomunicazioni sono quelle che hanno sviluppato policy aziendali in modo più diffuso (66%).

Se, da un lato, le grandi imprese sembrano percepire il rischio legato al fattore umano, dalla Ricerca emerge come le PMI sembrino invece sottovalutare la tematica della creazione di consapevolezza tra i propri dipendenti. Solo il 9% delle realtà di piccole dimensioni (tra i 10 e i 49 addetti) dichiara infatti di effettuare specifici programmi di formazione per aumentare la consapevolezza delle risorse rispetti ai rischi informatici (corsi online o in aula, mail periodiche di aggiornamento, distribuzione materiale informativo, ecc.). La rilevanza attribuita alle azioni di sensibilizzazione cresce con l'aumentare della dimensione aziendale, attestandosi al 20% per le aziende

medio-piccole (tra i 50 e i 99 addetti) e al 24% per le imprese più grandi (tra i 100 e i 249 addetti).

L'approccio alla sicurezza nelle PMI è orientato prevalentemente all'*identificazione* (66%) e alla *protezione* (66%), molto meno alla *rilevazione* (12%) e alla *risposta* (15%). L'attenzione alla *rilevazione* cresce all' aumentare della dimensione di impresa, passando dall'11% delle piccole imprese (10-49 addetti) al 20% delle aziende di dimensioni maggiori (100-249 addetti). Il settore delle telco appare quello maggiormente orientato agli aspetti di *risposta* (40%).

## Le priorità per il 2017

La Ricerca ed il coinvolgimento delle organizzazioni nei Workshop di lavoro hanno evidenziato numerose priorità di evoluzione per le imprese italiane.

In primo luogo emerge la necessità di sviluppare modelli di governance più maturi e trasversali all'organizzazione con l'identificazione del corretto mix di competenze necessario per gestire tecnologie sempre più pervasive. Inoltre, l'applicazione del General Data Protection Regulation (GDPR) è nel pieno corso di attuazione ed è necessario comprendere appieno non solo le implicazioni legali, ma anche quelle a livello di progettazione dei sistemi di security, che ad oggi sono risultate essere meno chiare agli occhi delle organizzazioni. In termini di evoluzione dell'architettura di gestione della security la direzione è quella di porre un focus maggiore agli aspetti di *rilevazione*, *risposta* e *ripristino* rispetto all'*identificazione* e alla *prevenzione*.

Si rende inoltre necessaria l'individuazione di un corretto modello di sourcing per la gestione di un Security Operation Center (SOC) orientato alla gestione reattiva e proattiva della sicurez-

za IT e del monitoraggio. La volontà di orientarsi ad un'esternalizzazione verso un modello di managed services è controbilanciata dalla necessità di trovare competenze specialistiche verticali per il business dell'impresa.

Lo scorso anno il report di Ricerca titolava: *Digital Transformation: siamo al sicuro?* A distanza di un anno, non ci sentiamo di poter rispondere con certezza in modo positivo a questa domanda. Come ci mostrano i fatti di cronaca, il cyber crime si configura sempre più come una minaccia invisibile e potente, in grado di poter influenzare, e a volte cambiare, il mondo. Permangono inoltre ancora troppe incognite sulla capacità delle imprese di governare le crescenti minacce derivanti dalla sicurezza informatica. Tuttavia l'ultimo anno ha portato in modo dirompente alla ribalta dei media il problema, rendendo forse più semplice, per il futuro, comprendere le implicazioni di un approccio contingente all'information security.

***Mariano Corso***

***Gabriele Faggioli***

***Alessandro Piva***

**I risultati completi della Ricerca sono consultabili su www.osservatori.net**

# I Rapporti

*I Rapporti con i risultati completi della Ricerca scaricabili da www.osservatori.net*

**La maturità delle imprese e lo scenario di mercato dell'Information Security & Privacy**
Il Report intende fotografare lo scenario del mercato dell'Information Security in Italia, analizzando lo stato di maturità e gli approcci delle aziende in termini di consapevolezza strategica e progettualità messe in campo. Vengono inoltre analizzate le implicazioni dei nuovi trend dell'innovazione digitale sulla sicurezza aziendale (Cloud, Mobile, Big Data, Internet of Things).

*Temi correlati:*
*Information Security, Privacy, CISO, DPO, Governance, Aree di investimento, mercato*

**Il Regolamento UE per la protezione dei dati personali**
Il Report analizza il Regolamento UE per la protezione dei dati personali, di recente pubblicazione, proponendosi di fornire alcune indicazioni alle organizzazioni volte all'impostazione di un percorso di adeguamento mirato al raggiungimento della compliance, sfruttando il tempo a disposizione prima della sua piena applicabilità a maggio 2018.

*Temi correlati:*
*Privacy, Compliance, Normative, Data Protection, GDPR, Regolamento UE*

# La Nota Metodologica

## La Ricerca 2016

La Ricerca 2016 è stata condotta con lo scopo di monitorare lo stato dell'arte di tecnologie e strategie per l'information security e privacy, coinvolgendo le principali organizzazioni end user e fornitrici di servizi e soluzioni di information security del panorama italiano.

Nella Ricerca sono state coinvolte diverse figure professionali che si occupano di security e di privacy, da diversi punti di vista: CISO (Chief Information Security Officer), CSO (Chief Security Officer), CIO (Chief Information Officer), Compliance Manager e DPO (Data Protection Officer) di grandi imprese italiane, con focus maggiore sulle prime 1.000 aziende per fatturato e Pubbliche Amministrazioni operanti in Italia. Sono stati inoltre coinvolti i Responsabili dei Sistemi informativi di piccole e medie imprese italiane.

La rilevazione è avvenuta utilizzando diversi strumenti:

- una Survey online rivolta ai CISO, CSO e CIO di grandi imprese italiane;
- una Survey online e telefonica rivolta ai Responsabili dei Sistemi informativi di piccole e medie imprese italiane;
- alcuni studi di caso svolti mediante approfondimenti de visu, telefonici o da fonti secondarie con alcune aziende utenti e i principali player dell'offerta, con l'obiettivo di analizzare approfonditamente le iniziative più significative.

I risultati ottenuti dalla rilevazione empirica sono stati discussi e validati attraverso quattro incontri a porte chiuse:

- *Advisory Board* (19 Aprile 2016) – Il primo Workshop del piano 2016 dell'Osservatorio Information & Privacy ha coinvolto 48 partecipanti (33 appartenenti ad aziende end user e 15 afferenti al mondo dell'offerta), con lo scopo di indirizzare i temi di Ricerca di maggior interesse per le imprese da sviluppare nel corso dell'anno.
- *Cloud Security: sicurezza in ambienti Cloud* (4 luglio 2016) – Il Workshop, durante il quale sono intervenuti 32 tra CIO, CISO, DPO ed Executive IT di grandi imprese italiane e PA e 17 rappresentanti del mondo dell'offerta, ha analizzato, attraverso dati di scenario e testimonianze, il tema della gestione della sicurezza in ambiti Cloud. All'interno dell'incontro si è dato spazio in particolare ai temi legati al trattamento dei dati, sulla base delle indicazioni del nuovo Regolamento generale sulla Protezione dei Dati personali. Si sono discusse inoltre le principali strategie di gestione della sicurezza in termini di policy e progettualità messe in campo dalle aziende.
- *Scenari privacy per i Big Data Analytics* (16 Settembre 2016) – Il Workshop, attraverso dati di scenario e testimonianze, ha affrontato la tematica dei Big Data Analytics e le relative problematiche di gestione della privacy legata agli aspetti di raccolta e analisi dei dati provenienti da fonti eterogenee. Sono state illustrate le principali novità sul tema legislativo nel contesto italiano ed internazionale, tra le quali in particolare il Regolamento europeo sulla Data Protection e le relative implicazioni per le aziende. Su questi temi sono stati coinvolti 41 rappresentati di aziende end user e 29 aziende del mondo dell'offerta.
- *Security & Privacy Journey* (18 Novembre 2016) – L'ultimo incontro a porte chiuse dell'Osservatorio ha coinvolto 36 aziende end user e 17 rappresentanti del mondo dell'offerta.

Durante il Workshop, svolto in logica interattiva, è stato chiesto ai partecipanti di effettuare una mappatura della propria realtà aziendale su un framework di riferimento, basato su una metodologia di lavoro sviluppata ad hoc per l'occasione, e una successiva discussione all'interno del gruppo di lavoro. Il serious game ha affrontato le tematiche relative alla gestione delle dinamiche di sicurezza e privacy all'interno delle aziende, analizzando i diversi approcci utilizzati dalle aziende, sia in ottica di prevenzione sia in ottica di reazione e risposta, e le principali progettualità implementate.

***La Ricerca 2016 si è focalizzata sui seguenti obiettivi:***

- Quantificare il mercato della sicurezza informatica in Italia;
- Indagare come i nuovi trend dell'innovazione digitale come il Cloud, i Big Data, l'Internet of Things e il Mobile impattano sulla gestione dell'information security e della privacy;
- Identificare le principali tendenze internazionali in ambito information security & privacy;
- Comprendere l'impatto del Regolamento UE sulla privacy;
- Monitorare lo stato di adozione di sistemi di Information Security e privacy nelle organizzazioni italiane;
- Studiare gli impatti sulle grandi imprese e sulle PMI;
- Identificare i casi di successo.

## La Survey

A partire da un modello comune di indagine, sviluppato in funzione degli obiettivi della Ricerca, è stato definito il questionario che è stato sottoposto ai CISO, CSO e CIO di orga-

nizzazioni di piccole, medie e grandi dimensioni e Pubbliche Amministrazioni presenti in Italia e appartenenti a diversi settori.

La rilevazione ha coinvolto 148 organizzazioni italiane di grandi dimensioni, aventi un numero di addetti superiore a 249, e 803 piccole e medie imprese operanti in Italia, con un numero di addetti compreso tra 10 e 249, per un totale di 951 organizzazioni indagate.

Il campione considerato nelle analisi comprende tutti i settori aziendali. Il panel della rilevazione sulle grandi imprese ha la seguente composizione settoriale:

- Manufacturing: 34%
- Servizi: 15%
- Retail e GDO: 14%
- Finance: 14%
- PA e Sanità: 12%
- Utility: 6%
- Media e Telco: 5%

Per le PMI la composizione per area industriale è invece la seguente:

- Manufacturing: 54%
- Servizi: 15%
- Retail e GDO: 15%
- Utility: 10%
- PA e Sanità: 2%
- Finance: 2%
- Media e Telco: 2%

Le analisi statistiche svolte sul campione delle 803 piccole e medie imprese hanno considerato la reale distribuzione delle stesse secondo i dati ISTAT, ed il contributo delle osservazioni è stato pesato per classe dimensionale, settore e area geografica, in modo da rappresentare un dato statisticamente rappresentativo.

## Gli studi di caso

Sono stati effettuati 53 approfondimenti dettagliati attraverso la conduzione di interviste telefoniche o de visu ai Security Manager di alcune grandi aziende ritenute particolarmente rilevanti. Gli studi di caso hanno indagato in particolare gli ambiti seguenti:

- Posizionamento e organizzazione della funzione information security all'interno dell'azienda;
- Strategia e committment del Board aziendale;
- Impatto dei nuovi trend tecnologici (Cloud, Mobile, Big Data, Internet of Things) sulla sicurezza aziendale e relativa gestione;
- Iniziative di awareness sviluppate;
- Impatto e percorsi di adeguamento al Regolamento Europeo sulla protezione dei dati.

# Il Gruppo di Lavoro

**Mariano Corso**
Responsabile Scientifico

**Gabriele Faggioli**
Responsabile Scientifico

**Alessandro Piva**
Direttore

**Giorgia Dragoni**
Ricercatore

**Luca Dozio**
Ricercatore

**Martina Broggi**
Program Management office

**I risultati completi della Ricerca sono consultabili su www.osservatori.net**

*Si ringraziano inoltre*

**Andrea Reghelin**
Senior Advisor

**Guglielmo Troiano**
Senior Advisor

**Attilio Guadalascara**
Ricercatore

*Per qualsiasi commento e richiesta di informazioni:* alessandro.piva@polimi.it

# La Community dell'Osservatorio Information Security & Privacy

Valentino Angeletti,
Global ICT – Cyber Security PM,
Enel

Luca Attias,
Dirigente Generale Sistemi Informativi Automatizzati,
Corte dei Conti

Gennaro Auriemma,
H3G ICT – Security,
H3G

Moreno Baldini,
IT Information Systems Manager,
Butali

Alberto Borgonovo,
Chief Information Security Officer,
Mediobanca Innovation Services – Gruppo Mediobanca

Raoul Brenna,
Responsabile della Practice Information Security & Infrastructures,
Co-direttore Corso Information Security Management,
CEFRIEL

Claudio Brisa,
Responsabile Servizio Sicurezza Logica,
Gruppo Bancario Credito Valtellinese

Marco Caleri,
Responsabile u.o. Sicurezza Sistemi,
Autostrade per l'Italia

Michele Carminati,
DEIB,
Politecnico di Milano

**Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net**

Alessandro Castelli,
Internal Audit Manager,
Direct Line (MAPFRE Group)

Daniele Cavagnero,
Senior Manager,
Johnson Electric Asti

Daniela Cecagallina,
Compliance ICT,
ICBPI (Istituto Centrale delle Banche Popolari)

Massimiliano Chiardoni,
Responsabile Cyber Security,
SO.G.I.N. – Società Gestione Impianti Nucleari

Sonja Codnich,
Banking Services Lines Management Division – Advocacy Manager,
UniCredit Business Integrated Solutions

Corradino Corradi,
Head of ICT Security, Privacy & Fraud Management,
Vodafone Italia

Matteo Emilio Corsi,
CISO,
Aruba

Alessandro Cosenza,
Chief Information Security Officer,
Bticino

Massimo Cottafavi,
Information Security & Business Continuity Manager,
Snam

Luca Dozio,
I.T. Security Team Leader,
BPM

Antonio Durante,
Compliance & Governance IT,
Snam

**I risultati completi della Ricerca sono consultabili su www.osservatori.net**

Michele Fabbri,
Cyber Security Operations Manager,
Eni

Franco Fantozzi,
Associate Director,
Corporate Security,
Bristol-Myers Squibb Italy

Francesco Gatta,
ICT Coordinator,
APS

Tarek Ghaddar,
Responsabile IT Strategy,
Veneto Banca

Stefano Gorla,
Specialista Privacy, Sicurezza dei dati e Qualità,
Seen Solution

Paolo Grigoletto,
Sicurezza delle Informazioni e Privacy,
Infocamere

Gianfranco Labonia,
IT Manager (Planning and Supply Chain Area),
LaRinascente

Mara Maffei,
ICT Manager,
Heineken Italia

Domenico Nilo Mazza,
Direttore Servizio Informatico,
Fondazione I.R.C.C.S. Istituto Neurologico "Carlo Besta"

Michele Mellone,
Strategie Digitali, Architetture IT e Sicurezza,
INAIL

Massimo Moimare,
ICT Manager,
IVAR

Massimo Montanile,
DPO – Data Protection Officer,
Elettronica

Stefano Pastori,
Information Security & Data Privacy Specialist / Governance & Risk Management,
IKEA Italia Retail

Alessio Pennasilico,
Membro del Comitato Direttivo e del Comitato Tecnico Scientifico, Clusit

Laura Quaroni,
Responsabile Privacy & Security Management,
Banca IFIS

Enrico Riccardi,
Group Information Security Manager,
Chiesi Farmaceutici

Riccardo Roncon,
Responsabile Sicurezza IT,
Gruppo ITAS Assicurazioni

Enrico Maria Rossi,
Responsabile della Divisione Sicurezza,
Gruppo Bancario Credito Valtellinese

Massimo Rosso,
Direttore ICT,
RAI

Giovanni Saglia,
Group Digital & Business Technology,
Barilla G. E R. Fratelli

Matteo Sala,
Responsabile Sistemi Informativi,
Alcantara

**I risultati completi della Ricerca sono consultabili su www.osservatori.net**

Antonio Salis,
Quality and Security Manager,
Tiscali Italia

Corrado Salvemini,
Responsabile della Sicurezza delle Informazioni,
Carrefour Italia

Gianluigi Sangermani,
IT Manager/CIO,
Silvano Chiapparoli Logistica

Gaetano Scebba,
CIO,
Gruppo API

Giovanni Seresini,
Information Risk Manager,
Barclays Bank

Lucia Toia,
IT Processes, Organization & Compliance,
Gewiss

Enrico Toso,
IT Regulatory Risk & Control Specialist,
Deutsche Bank

Ileana Vanzini,
Information Security Expert,
Bayer

Stefano Vercesi,
Information Security Officer,
Allianz Bank Financial Advisors

Maria Gaia Vinciguerra Frezza,
Data Protection, Security & Compliance Manager,
Europcar

Andrea Volponi,
Information Technology – Security Operation and Monitoring,
Alitalia

**Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net**

POLITECNICO MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET digital innovation

## Osservatorio Information Security & Privacy

# Cyber Crime: La minaccia invisibile che cambia il mondo

# Il Convegno

Febbraio 2017

# L'Agenda del Convegno

2 Febbraio 2017

**9.00** **Welcome Coffee**

**9.30** **Benvenuto e introduzione**

Mariano Corso
*Responsabile Scientifico Oss. Information Security & Privacy*

**9.40** **La maturità delle imprese e lo scenario di mercato**

Alessandro Piva
*Direttore Oss. Information Security & Privacy*

**10.00** **L'evoluzione del quadro normativo: le implicazioni del GDPR**

Gabriele Faggioli
*Responsabile Scientifico Oss. Information Security & Privacy*

**10.20** **GDPR: i prossimi passi**

***Entro maggio 2018 le imprese dovranno adeguarsi al General Data Protection Regulation (GDPR), la normativa europea che richiede nuovi modelli di gestione dei dati personali. Quali passi per essere pronti al cambiamento?***

*Ne discutono:*

Vittorio Bitteleri
*Head of Sales & Channel for Enterprise Security, Symantec Italia*

Gianluca Giaccardi
*Business Line Executive, TESISQUARE®*

Sergio Mattioli
*Information Security and Data privacy Director, Gruppo Bosch Italia*

Andrea Mercurio
*Responsabile Security Operations and Products Cybersecurity Practice, Almaviva*

Davide Maria Rossi
*Partner & CEO, Spike Reply*

Maria Gaia Vinciguerra Frezza
*Data Protection, Security & Compliance Manager, Europcar*

**11.15** **L'information security tra "tradizione" e innovazione**

Raoul Brenna
*Responsabile della Practice Information Security, CEFRIEL, Co-direttore Corso Information Security Management*

**11.30** **Disruption tecnologica: quali implicazioni?**

***I nuovi trend della trasformazione digitale, quali l'Internet of Things, i Big Data, il Cloud ed il Mobile richiedono un nuovo approccio alla gestione della sicurezza. Quali risposte per un mondo sempre più interconnesso?***

*Ne discutono:*

Gastone Nencini
*Country Manager, Trend Micro Italia*

**Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net**

Rosario Sorrentino
*Head of BT Security Business Italy*

Giampaolo Tacchini
*CISO ed ICT service Manager, Edison*

**12.00 BankSealer: A decision support system for online banking fraud analysis and investigation**

Michele Carminati
*DEIB, Politecnico di Milano*

**12.15 Il fattore umano: sensibilizzare per mitigare i rischi**

***La principale vulnerabilità sono le persone. Spesso azioni inconsapevoli, dettate da una scarsa conoscenza delle policy aziendali, così come comportamenti ingenui, espongono le organizzazioni a potenziali attacchi. Come sviluppare consapevolezza?***

***Ne discutono:***

Sonja Codnich
*Banking Service Lines Management Division – Advocacy Manager, UniCredit Business Integrated Solutions*

Corrado Salvemini
*Responsabile della Sicurezza delle Informazioni, Carrefour Italia*

Nicola Sotira
*Responsabile Tutela delle Informazioni, Poste Italiane S.p.A. e Direttore Generale Fondazione Global Cyber Security Center*

Gianfranco Vinucci
*Head of Pre-Sales, Kaspersky Lab Italia*

**13.00 Gestire il Cyber Risk: perché e come farlo!**

Alessio L.R. Pennasilico
*Membro del Comitato Direttivo e del Comitato Tecnico Scientifico, Clusit*

**13.15 Chiusura lavori**

Sul sito **www.osservatori.net** è possibile rivedere le riprese integrali del Convegno **"Cyber Crime: La minaccia invisibile che cambia il mondo"**

Visita **www.osservatori.net** e seguici sui nostri **social network**

**I risultati completi della Ricerca sono consultabili su www.osservatori.net**

# I Relatori

Da aprile 2015 guida il team vendite e canale di Symantec Italia. Prima di occupare l'attuale posizione – quando Symantec e Veritas erano un'unica realtà societaria – ha ricoperto il ruolo di Sales Director Enterprise Italy e prima ancora di Finance District Manager. Precedentemente ha maturato un'esperienza di oltre 20 anni in importanti multinazionali del settore IT, quali: Computer Associates, Sterling Software e Peregrine System, gestendo progetti anche complessi sia per una clientela acquisita che per nuovi clienti, perfezionando così un'ampia competenza delle principali problematiche legate al mondo delle tecnologie oltreché una solida conoscenza del mercato italiano.

**Vittorio Bitteleri**
Head of Sales & Channel for Enterprise Security,
Symantec Italia

In CEFRIEL, Centro di Eccellenza del Politecnico di Milano per la Digital Innovation, si occupa di sicurezza informatica da oltre 10 anni, affrontando la tematica sia da un punto di vista "tradizionale" (tecnologico e di processo), sia esplorando ambiti innovativi (sicurezza del fattore umano, nuovi assessment efficaci, IoT/ICS security). Su questi temi collabora attivamente, oltre che con MIP, anche con AIEA, CLUSIT e altre associazioni di settore.

**Raoul Brenna**
Responsabile della Practice Information Security & Infrastructures, Co-direttore Corso Information Security Management,
CEFRIEL

Michele Carminati was born in 1988. He received his B.Sc. in Computer Engineering (2010) and his M.Sc. in Computer Engineering (2013, cum laude) both from Politecnico di Milano. Since November 2013 he is a PhD student in Computer Engineering at Politecnico di Milano supervised by prof. Stefano Zanero. His research interests are mainly focused on computer security and in particular on financial malware analysis and Internet banking fraud detection.

**Michele Carminati**
DEIB,
Politecnico di Milano

**Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net**

**Gianluca Giaccardi**
Business Line Executive,
TESISQUARE®

Gianluca Giaccardi inizia la propria esperienza professionale nell'ambito della consulenza informatica. Nel 1995 è tra i soci fondatori di Tesi e da allora è direttamente coinvolto nella direzione aziendale. Da oltre 15 anni segue clienti di medio-grandi dimensioni, proponendo software orientati al miglioramento dell'efficienza dei processi HR e di quelli legati a normative e policy interne. È Responsabile della Line of Business Human Resources Management and Governance Risk and Compliance.

**Andrea Mercurio**
Responsabile Security Operations and Products – Cybersecurity Practice,
Almaviva

Laureato in Fisica, opera da 27 anni nel settore ICT e da oltre 15 anni nell'aera della sicurezza informatica. Attualmente è responsabile dell'area Operations and Products della Cybersecurity Practice di Almaviva. Ha collaborato con istituti universitari quali La Sapienza e LUISS di Roma e UNICAL di Cosenza come docente e relatore di tesi di master in sicurezza. Certificato CISA, CISM, CRISC, ISO27001 auditor, è membro di diversi gruppi di lavoro tecnici ed istituzionali di settore e socio ISACA.

**Gastone Nencini**
Country Manager,
Trend Micro Italia

Gastone Nencini vanta una carriera nel settore IT di oltre 25 anni. Nel 1998 approda in Trend Micro Italia dove viene nominato Senior Sales Engineer per il Centro e Sud Italia, per passare successivamente a un ruolo di maggiore responsabilità e prestigio, diventando prima Technical Manager Developing BU (Italia, Benelux e Paesi Scandinavi) per poi focalizzarsi sul mercato Italiano con l'incarico di Senior Technical Manager Italy. Nel 2012 Gastone diventa Technical Director Southern Europe e a Gennaio 2015 è ufficialmente nominato anche Country Manager Italia.

**Alessio Pennasilico**
Membro del Comitato Direttivo e del Comitato Tecnico Scientifico,
Clusit

Noto nell'hacker underground come -=mayhem=-, è internazionalmente riconosciuto come esperto di information security. All'interno di Obiectivo, per importanti Clienti operanti nei più diversi settori di attività, sviluppa progetti per la riduzione dell'impatto del rischio informatico/cyber sul business aziendale. È membro del Comitato Direttivo e del Comitato Tecnico Scientifico di Clusit, Vice Presidente di Associazione informatici Professionisti, membro del Comitato di Schema UNI 11506 – Informatico Professionista dell'ente di certificazione Kiwa Cermet e Vice Presidente del Comitato di Salvaguardia per l'Imparzialità di LRQA, l'ente di certificazione dei LLoyd's.

**Davide Maria Rossi**
Partner & CEO,
Spike Reply

Partner & CEO di Spike Reply, Società di consulenza del Gruppo Reply specializzata negli ambiti CyberSecurity, Risk Management&Compliance e System Integration; nel 2003, dopo alcune esperienze multidisciplinari nel mondo IT, unisce la passione delle tecnologie a quella della sicurezza informatica, contribuendo allo sviluppo di alcune delle più importanti realtà di consulenza italiane. Nel 2007 approda in Spike Reply e nel 2017 diventa il leader della Practice Cyber Security di Reply.

**Rosario Sorrentino**
Head of BT Security Business Italy,
BT

Rosario ha oltre 15 anni di esperienza in tema di cyber security, maturata in BT occupandosi con responsabilità crescenti delle tematiche di gestione dei rischi, continuità operativa, salvaguardia dell'organizzazione e sviluppo di modelli di governance, information security management system e architetture di sicurezza di coumicazioni e IT. Ha inoltre gestito per conto di BT la relazione con gli enti esterni e le istituzioni per quanto riguarda la sicurezza.

**Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net**

**Nicola Sotira**
Responsabile Tutela delle Informazioni,
Poste Italiane
Direttore Generale,
Fondazione Global Cyber Security Center

Responsabile di Tutela delle Informazioni in Poste Italiane, lavora da oltre 20 anni nel settore della sicurezza informatica con esperienze in diverse aziende a livello internazionale. Docente al Master di Sicurezza e Gestione delle Reti dell'Università La Sapienza, è Membro della Association for Computing Machinery. Da sempre promotore dell'innovazione tecnologica, ha collaborato con diverse startup in Italia e all'estero.

**Giampaolo Tacchini**
CISO ed ICT service Manager,
Edison

In Edison spa dal 2001, ha 5 anni di esperienza nel campo della sicurezza ICT, con responsabilità di esercizio e sviluppo sia della sicurezza che di tutte le infrastrutture informatiche del gruppo. Ha curato l'impostazione strategica e la realizzazione del piano ISMS, il coordinamento dei team che hanno realizzato sistemi e servizi per la gestione della sicurezza (integrazione fra servizi ICT e OT), l'avvio di un servizio SOC dedicato e l'introduzione di un sistema di gestione e controllo basata sugli standard ISO27002/27005. Da un anno chairman all'interno del security working group del gruppo EDF, di cui Edison fa parte.

**Maria Gaia Vinciguerra Frezza**
Data Protection, Security & Compliance Manager,
Europcar

Laureata in Economia, approfondisce le conoscenze informatiche conseguendo una serie di certificazioni tra le quali CCNA, CISM, ISO 27001 L.A, ISO 20000 L.A., ITIL, DPO. Impegnata in diversi progetti nazionali ed internazionali, attualmente guida il processo di adeguamento al nuovo GDPR per la Europcar. Grazie all'approccio multidisciplinare, è inoltre impegnata nell'elaborazione di un modello "realistico" di analisi quantitativa del rischio.

**I risultati completi della Ricerca sono consultabili su www.osservatori.net**

È responsabile del team italiano che gestisce le operazioni di prevendita e le attività di training per partner e clienti. In Kaspersky Lab da ottobre del 2008, ha ricoperto il ruolo di Head of Support & Services Manager come responsabile delle attività di supporto tecnico di prevendita e postvendita per i clienti del mercato Online, Retail e Corporate Italiano e Israele.

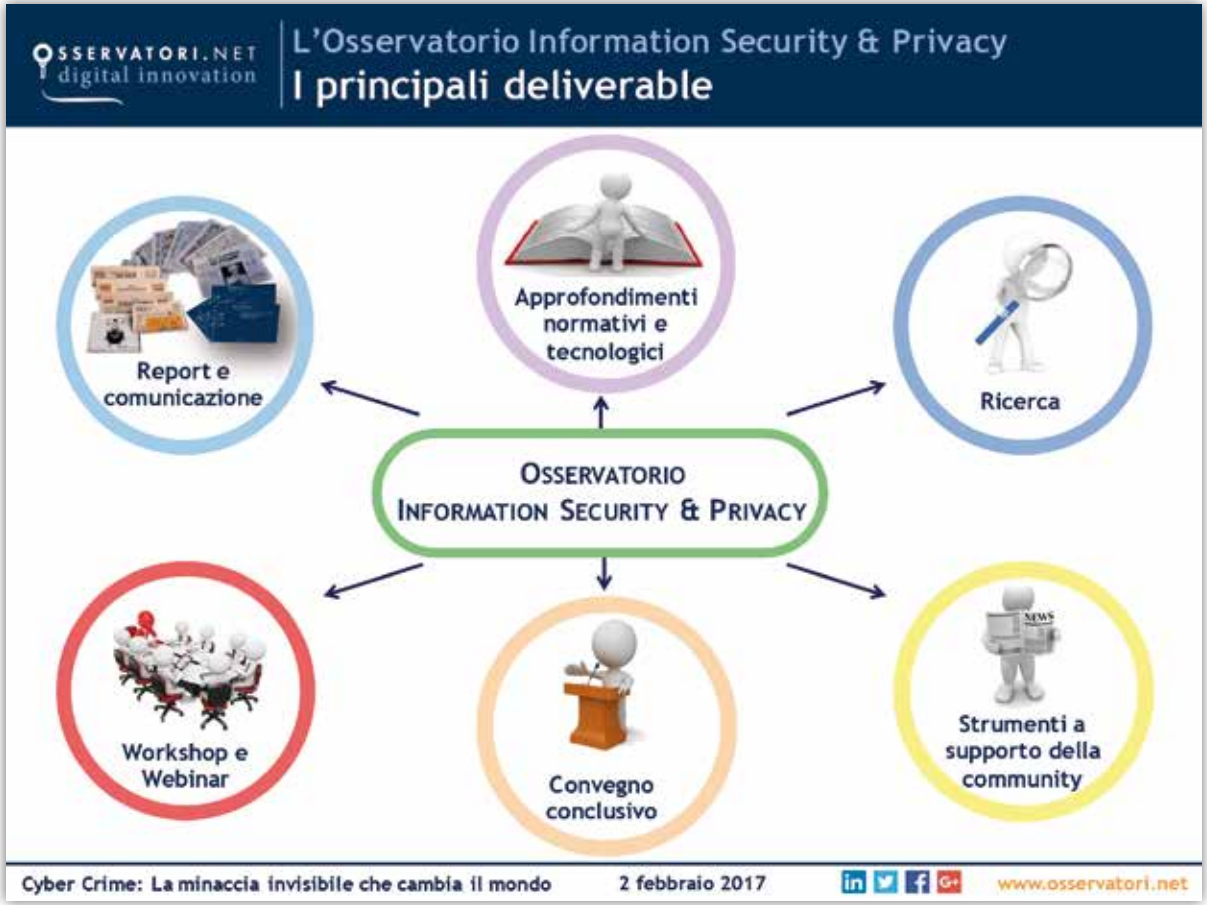
**Gianfranco Vinucci**
Head of Pre-Sales,
Kaspersky Lab Italia


Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

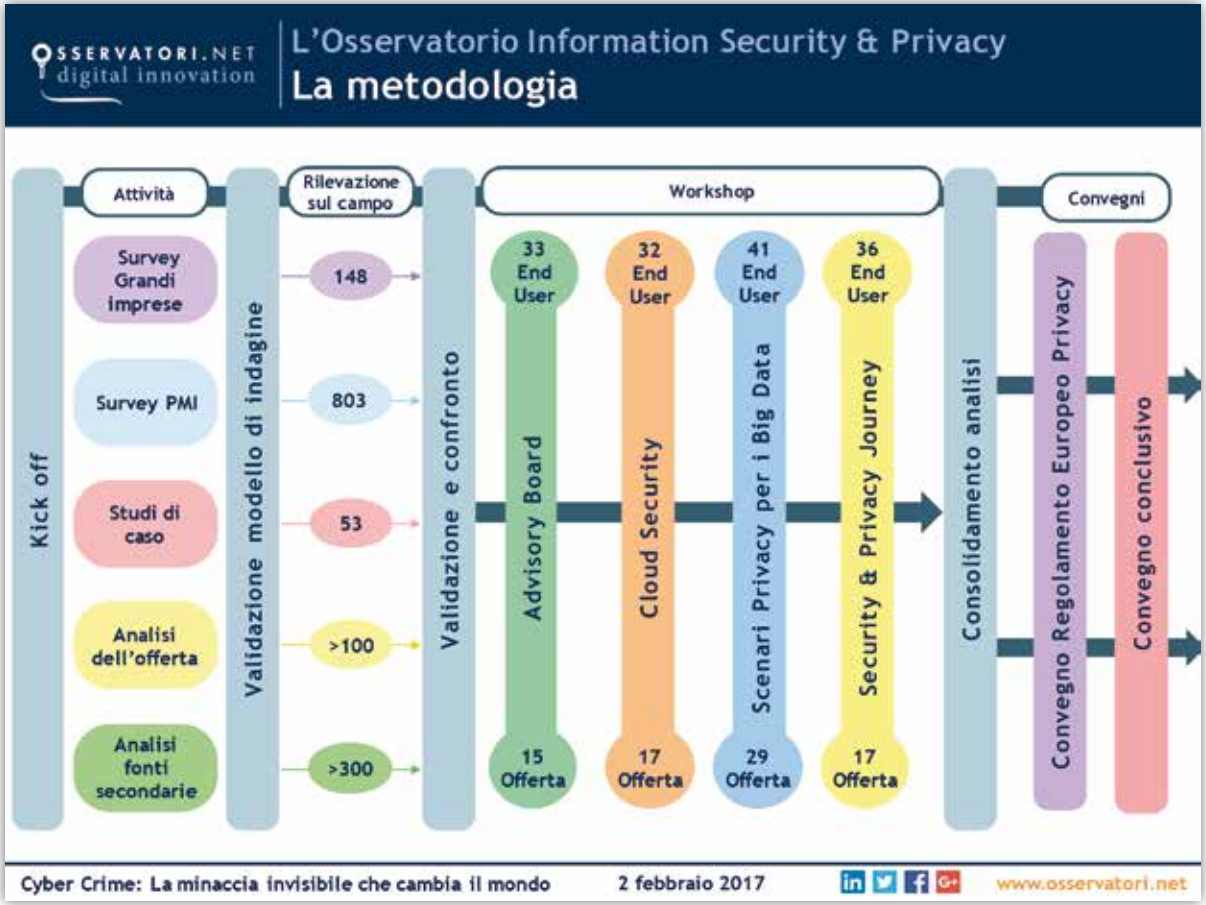

I risultati completi della Ricerca sono consultabili su www.osservatori.net


**Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net**


I risultati completi della Ricerca sono consultabili su www.osservatori.net



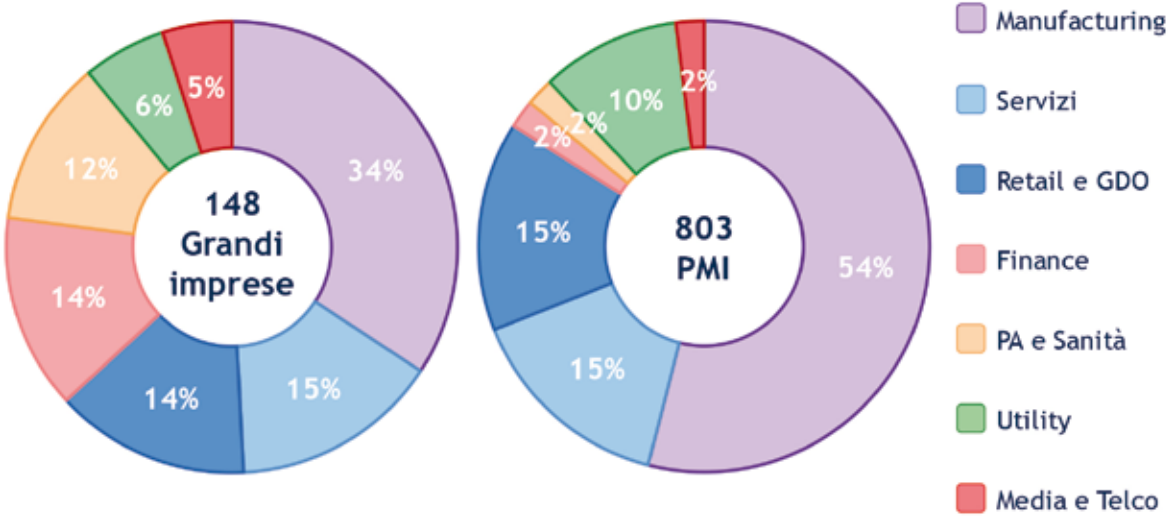

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net




I risultati completi della Ricerca sono consultabili su www.osservatori.net

OSSERVATORI.NET digital innovation

## L'Osservatorio Information Security & Privacy
## Le aziende del panel - Grandi imprese

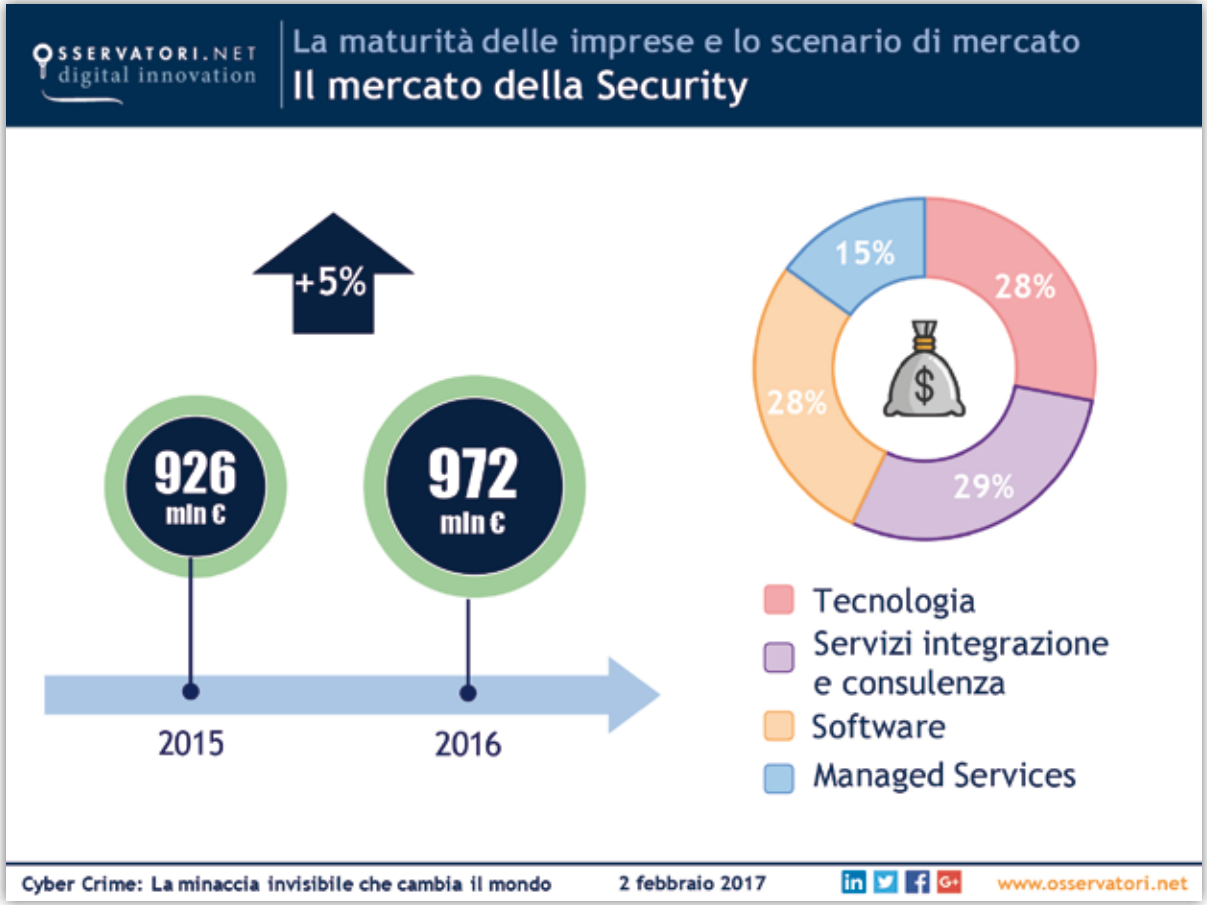



*Campione : 148 grandi imprese (>249 addetti) e 803 PMI (tra i 10 e i 249 addetti)*

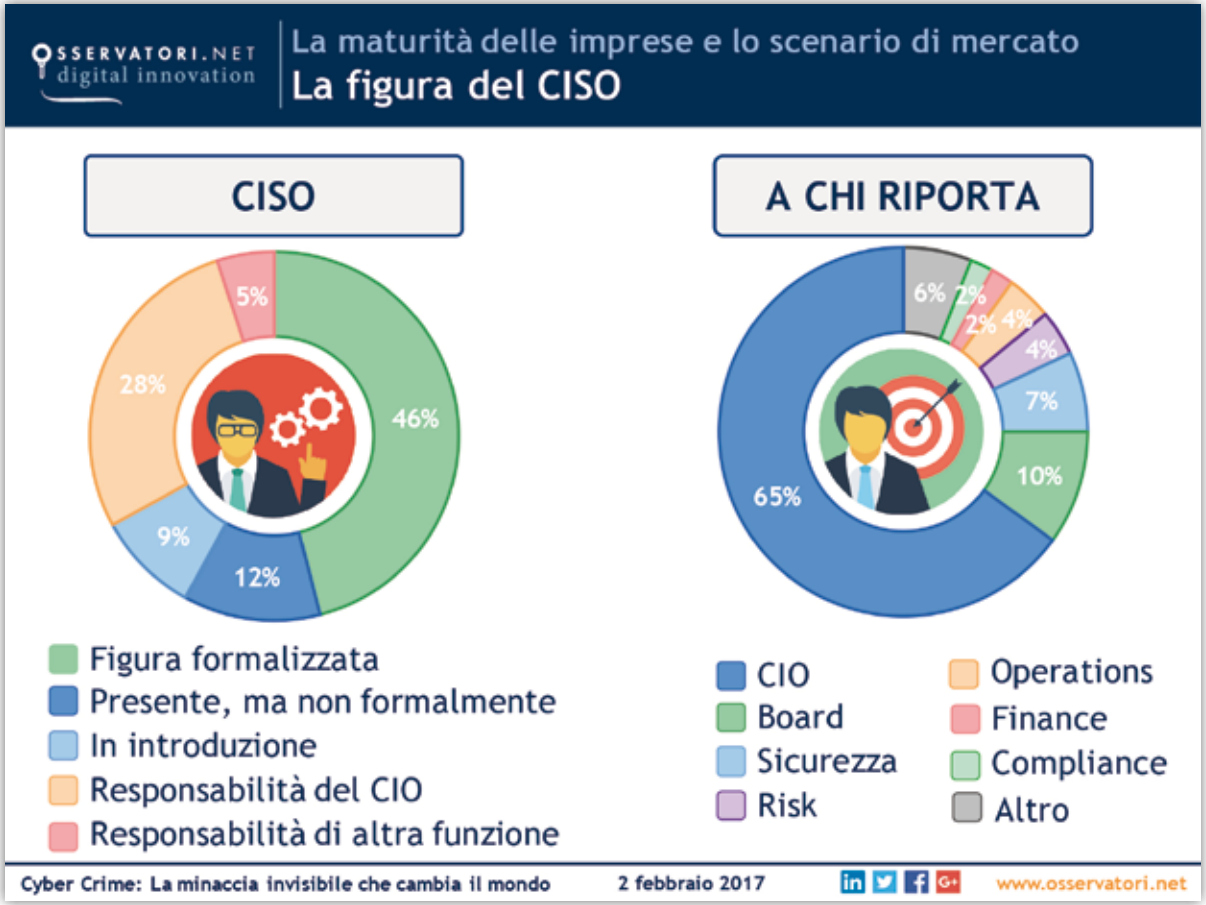
Cyber Crime: La minaccia invisibile che cambia il mondo 2 febbraio 2017 www.osservatori.net

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

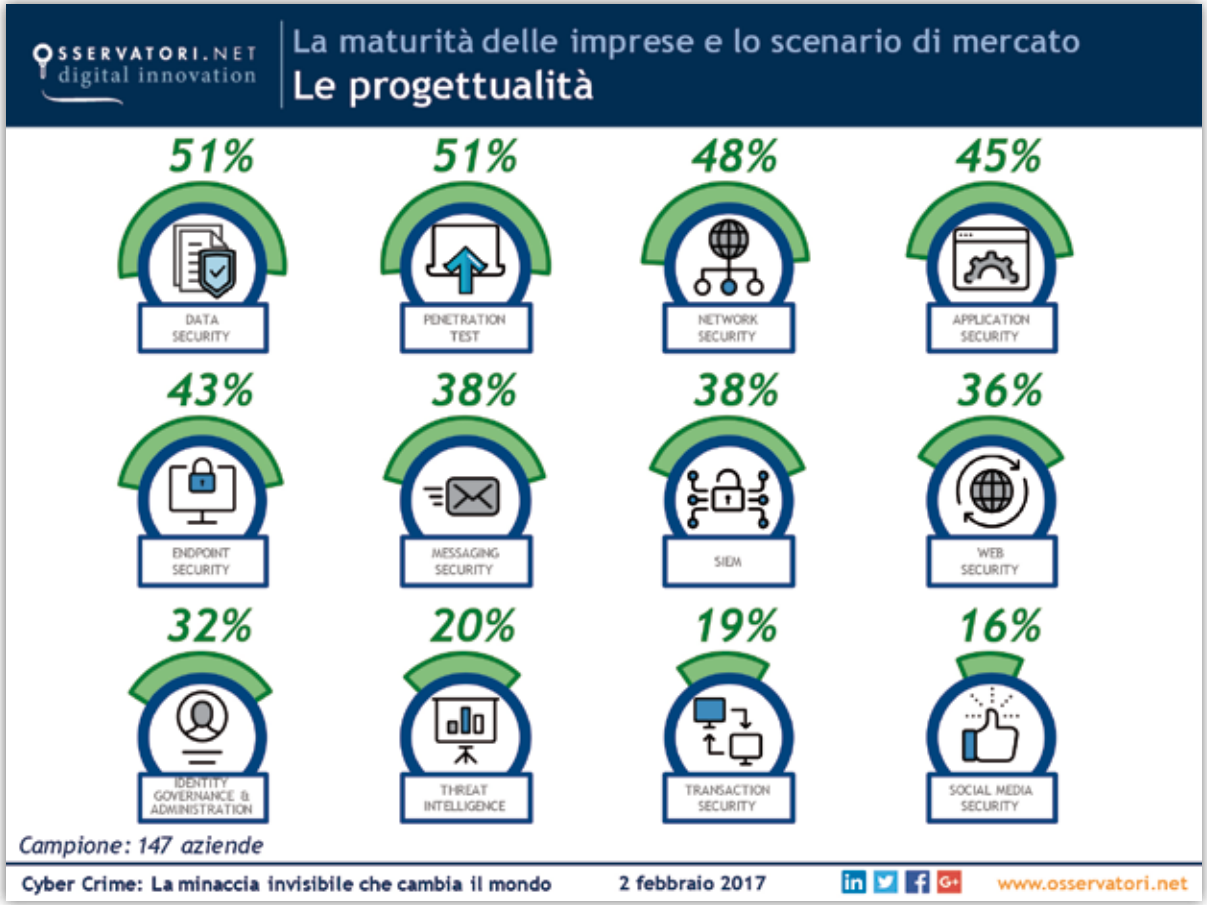

I risultati completi della Ricerca sono consultabili su www.osservatori.net



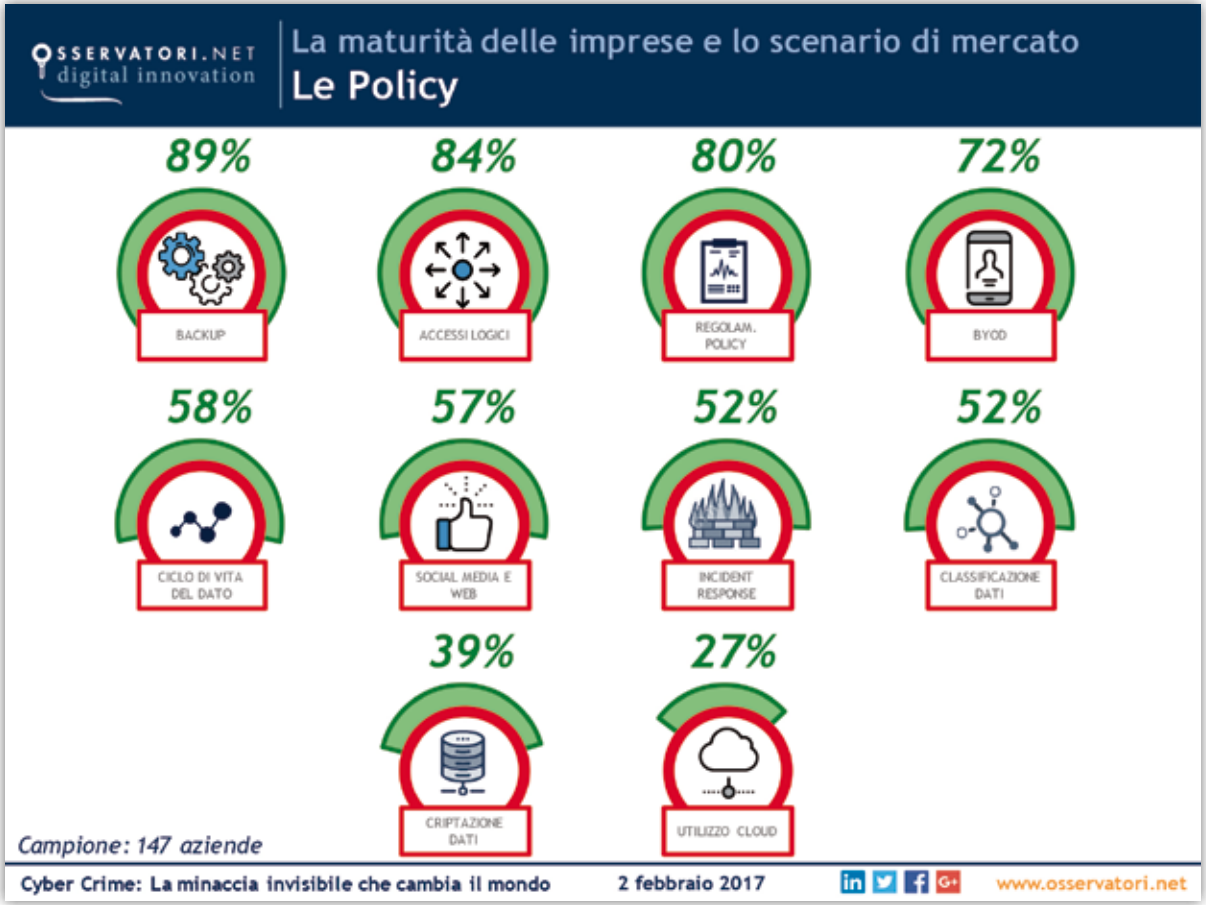

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net




I risultati completi della Ricerca sono consultabili su www.osservatori.net




Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net




I risultati completi della Ricerca sono consultabili su www.osservatori.net

OSSERVATORI.NET digital innovation

## La maturità delle imprese e lo scenario di mercato
## Le iniziative di sensibilizzazione

78% Comunicazioni tramite mail periodiche

66% Corsi di formazione

28% Distribuzione materiale informativo

28% Progetti strutturati di sensibilizzazione

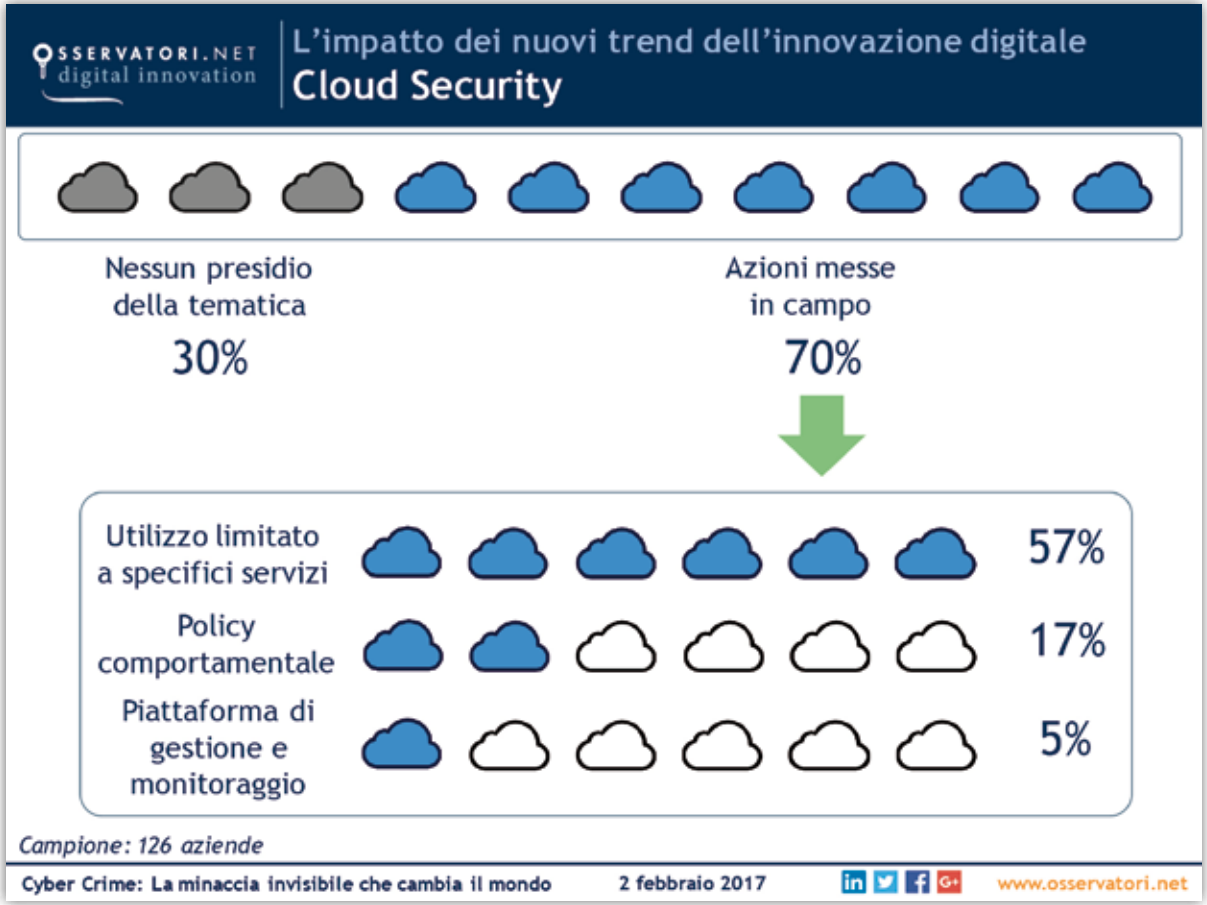
28% Vulnerability assessment sui dipendenti

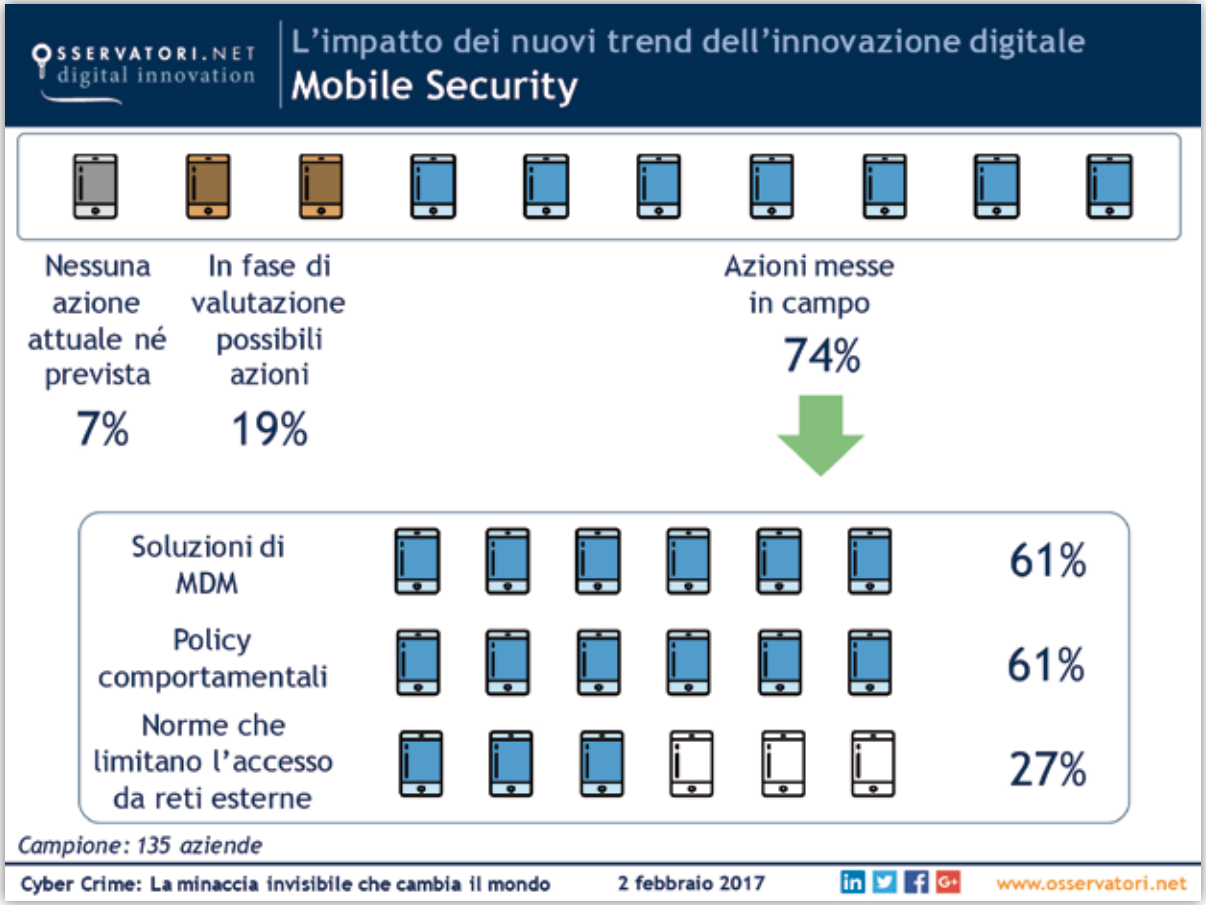
*Campione: 145 aziende*

Cyber Crime: La minaccia invisibile che cambia il mondo 2 febbraio 2017 www.osservatori.net

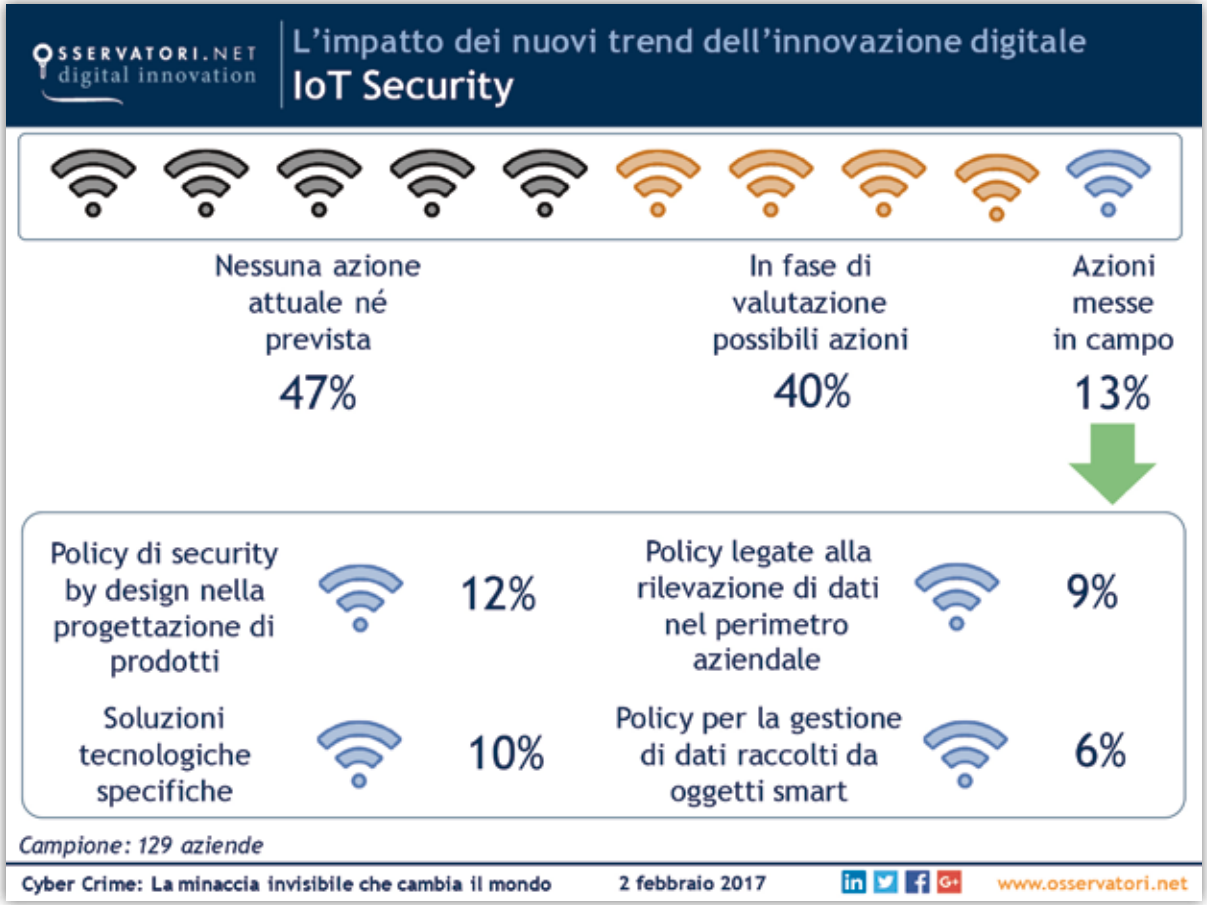
Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net


**I risultati completi della Ricerca sono consultabili su www.osservatori.net**

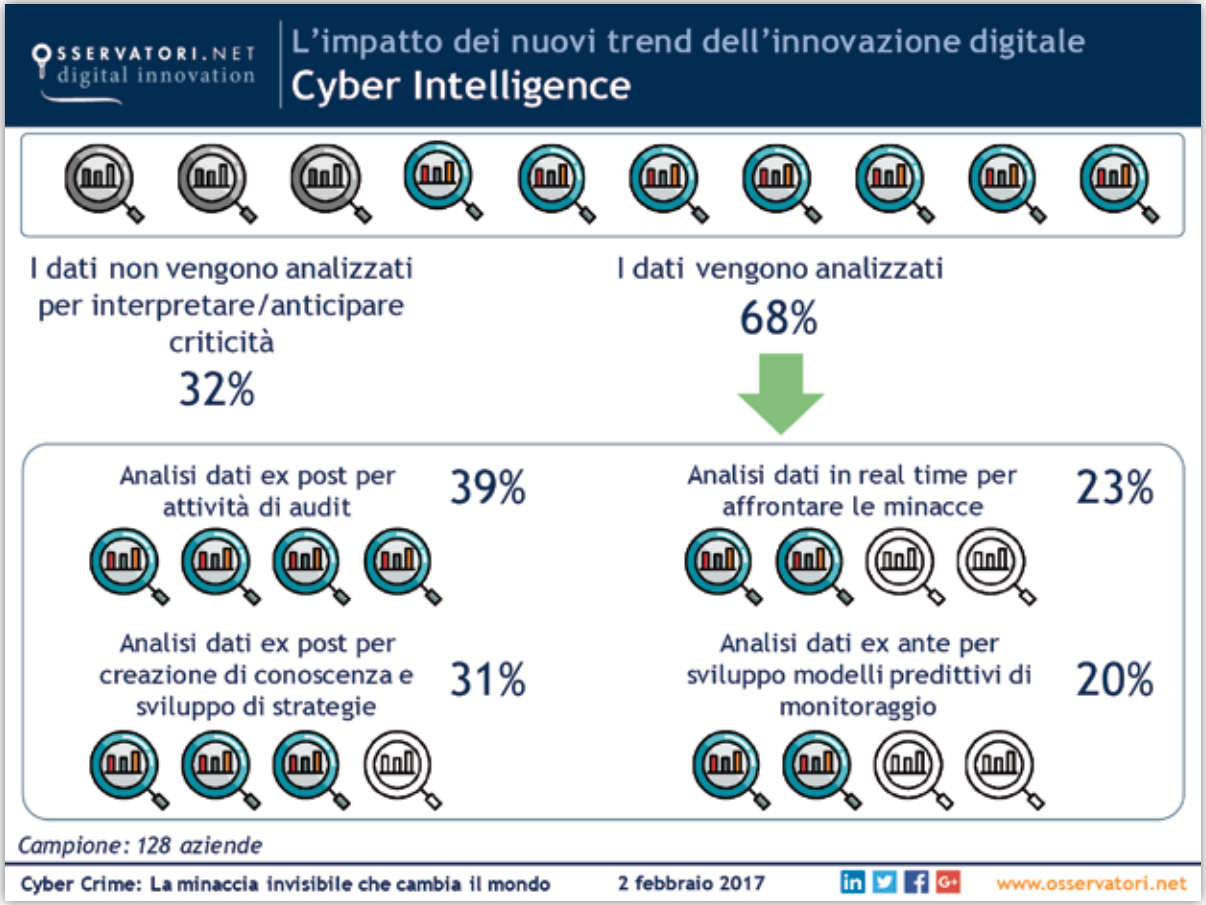




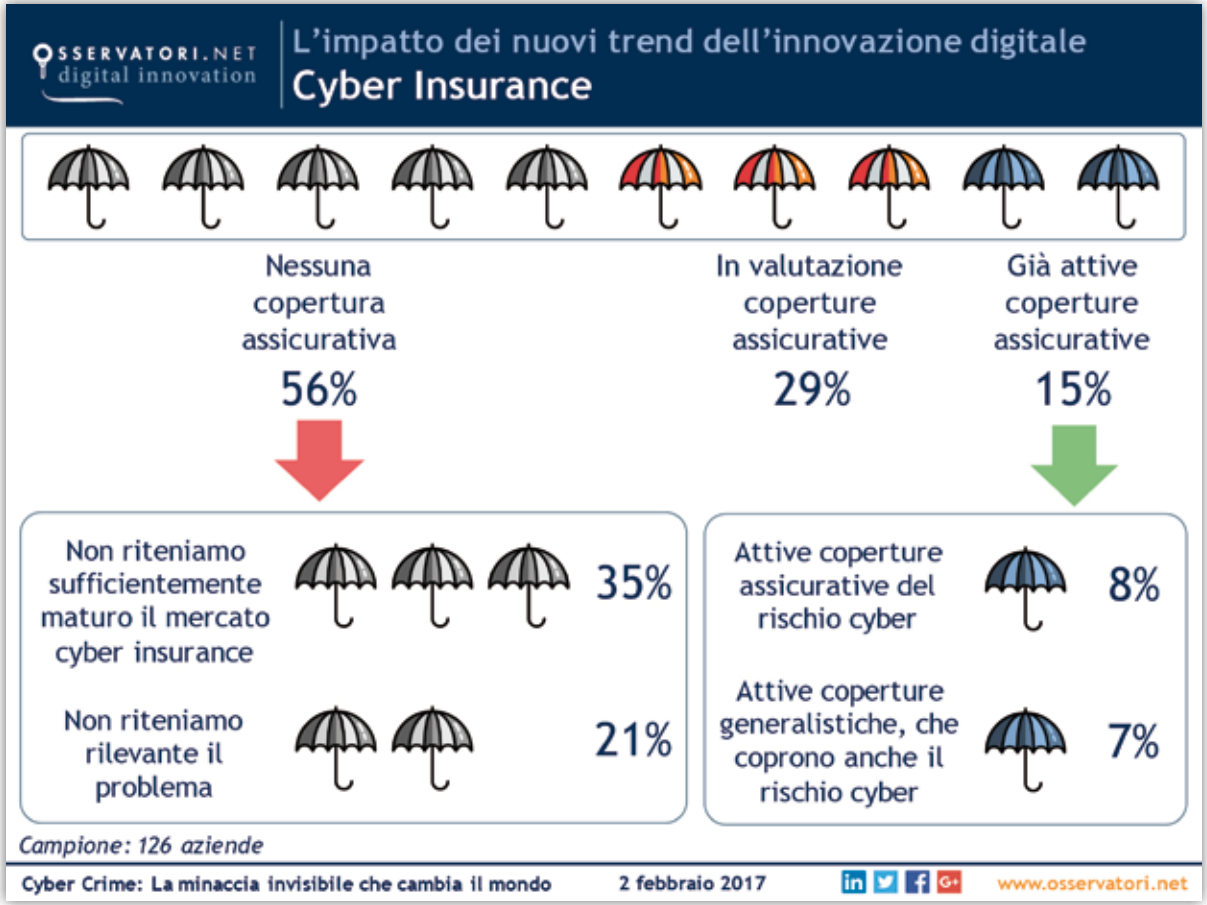

I risultati completi della Ricerca sono consultabili su www.osservatori.net




Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net



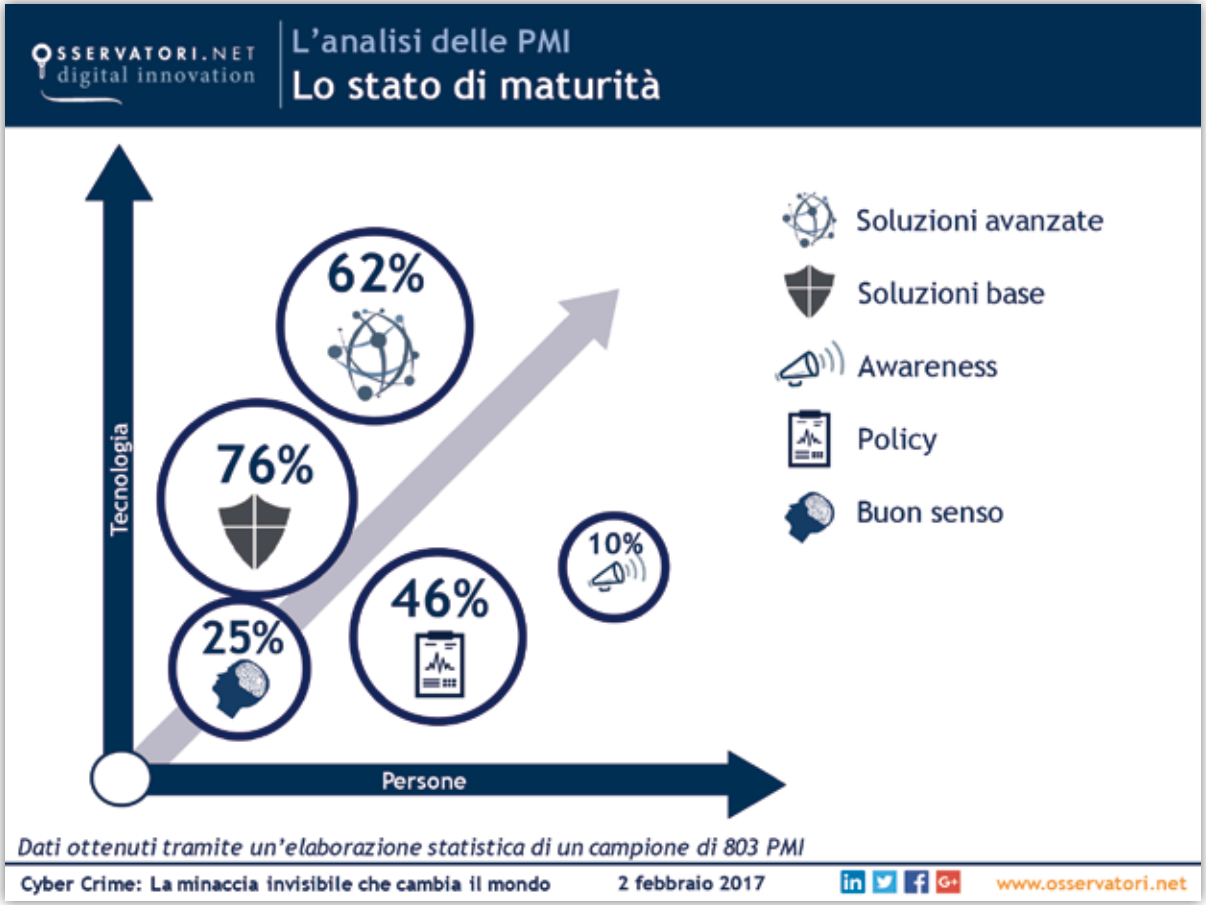

I risultati completi della Ricerca sono consultabili su www.osservatori.net




Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net


**I risultati completi della Ricerca sono consultabili su www.osservatori.net**


Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

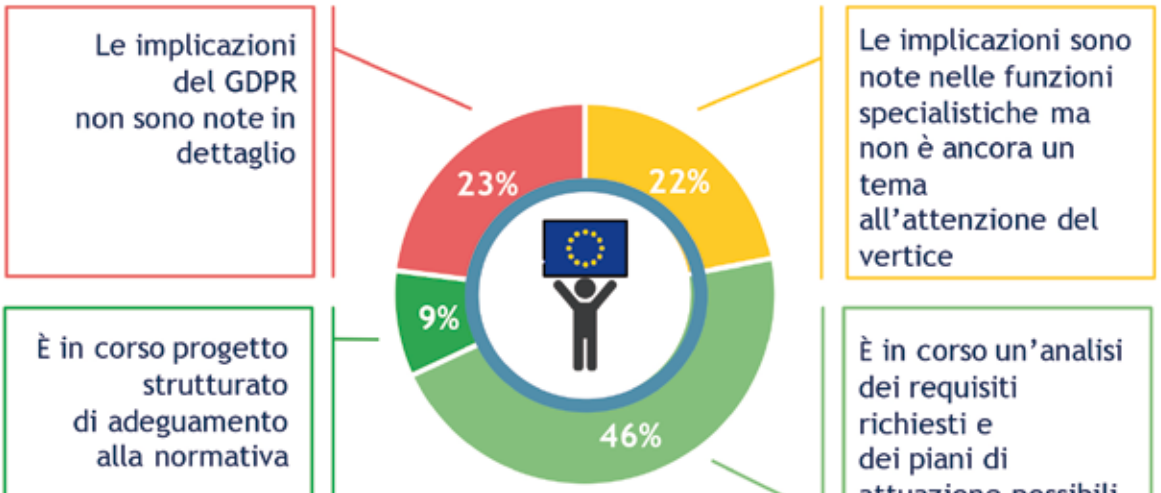



**I risultati completi della Ricerca sono consultabili su www.osservatori.net**


**Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net**

OSSERVATORI.NET digital innovation

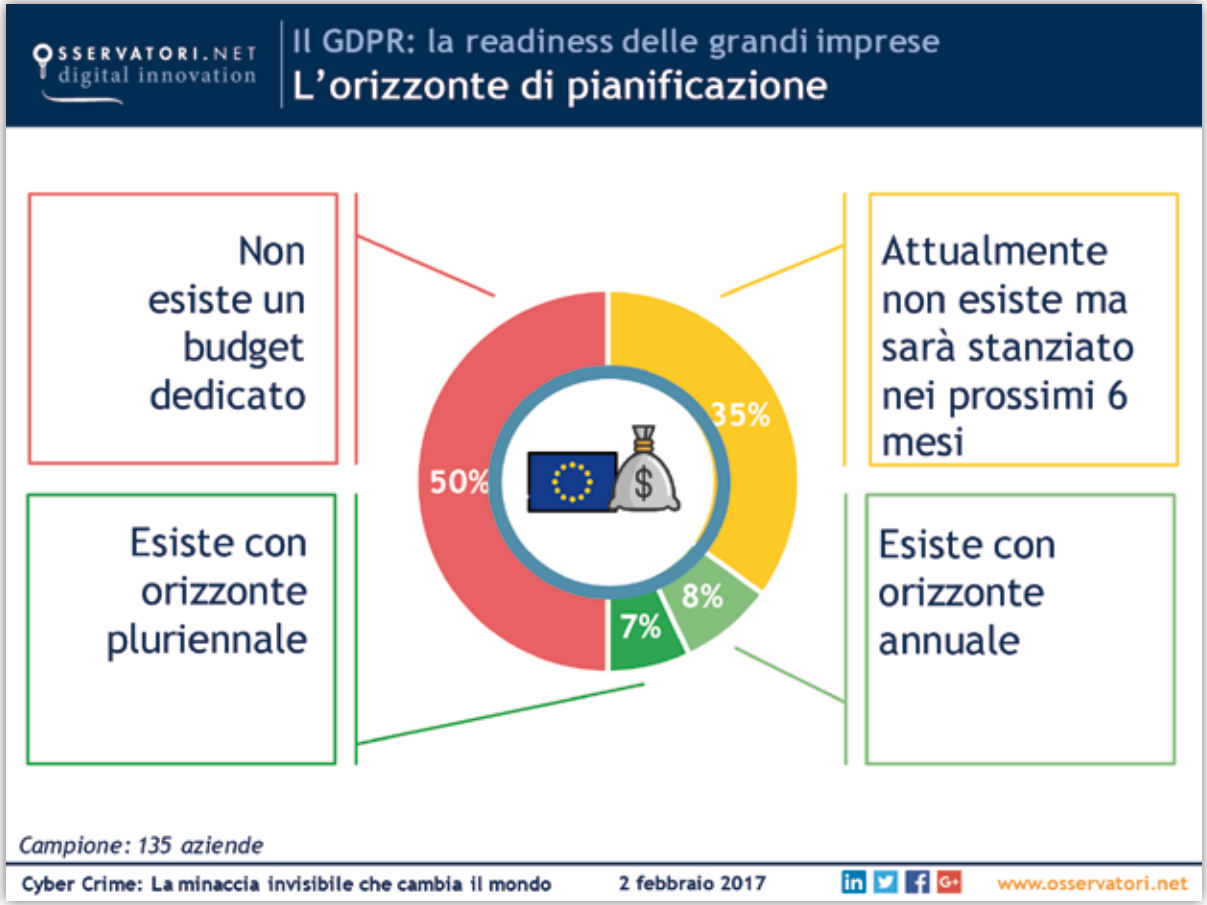
## Il GDPR: la readiness delle grandi imprese
## Le misure di adeguamento




*Campione: 136 aziende*

Cyber Crime: La minaccia invisibile che cambia il mondo 2 febbraio 2017 www.osservatori.net

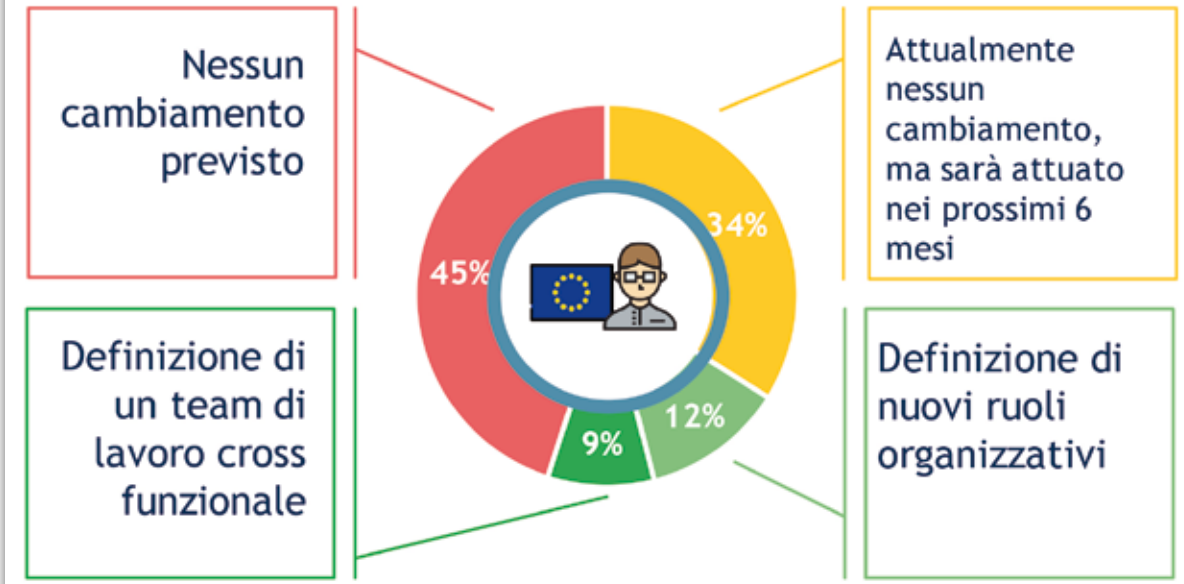
**I risultati completi della Ricerca sono consultabili su www.osservatori.net**




Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

OSSERVATORI.NET digital innovation

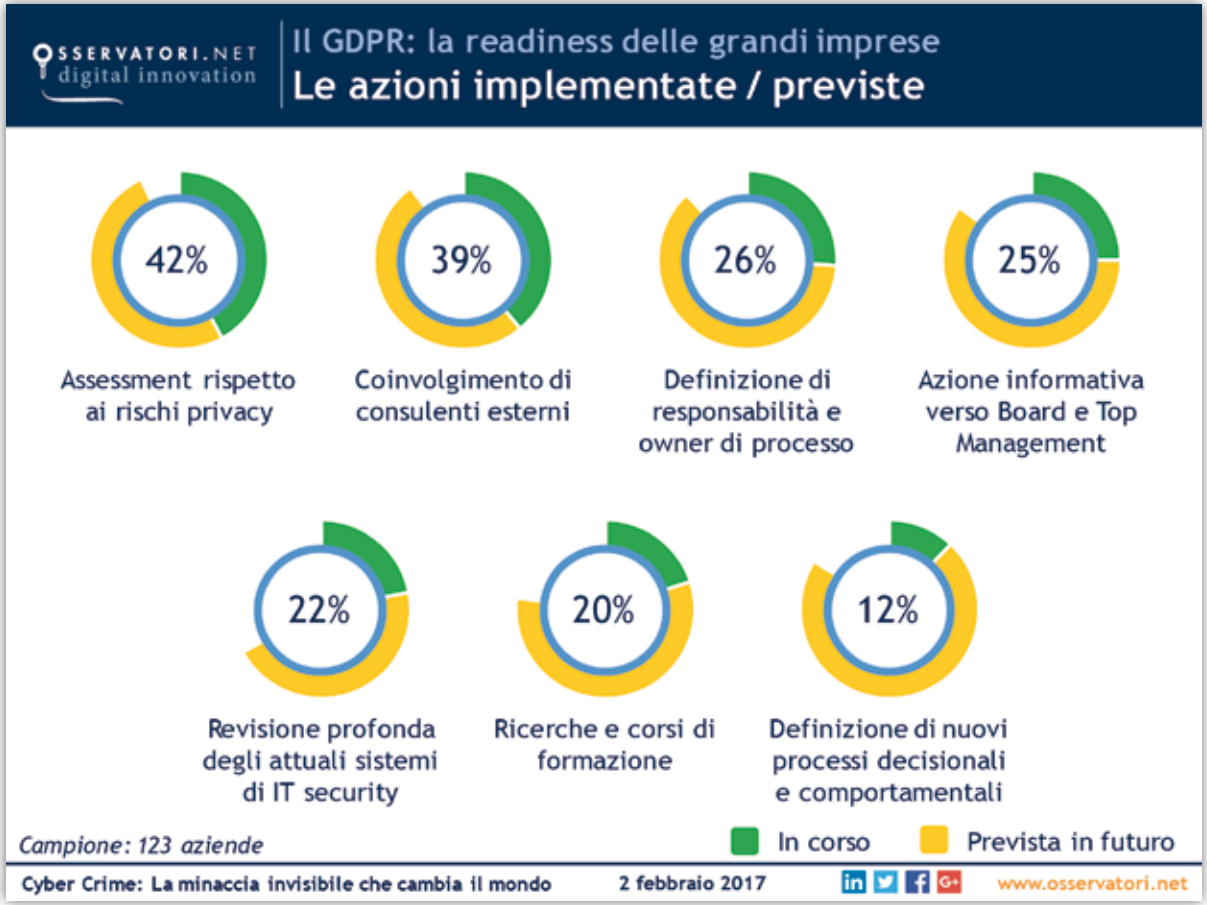
## Il GDPR: la readiness delle grandi imprese
## I cambiamenti organizzativi




*Campione: 128 aziende*

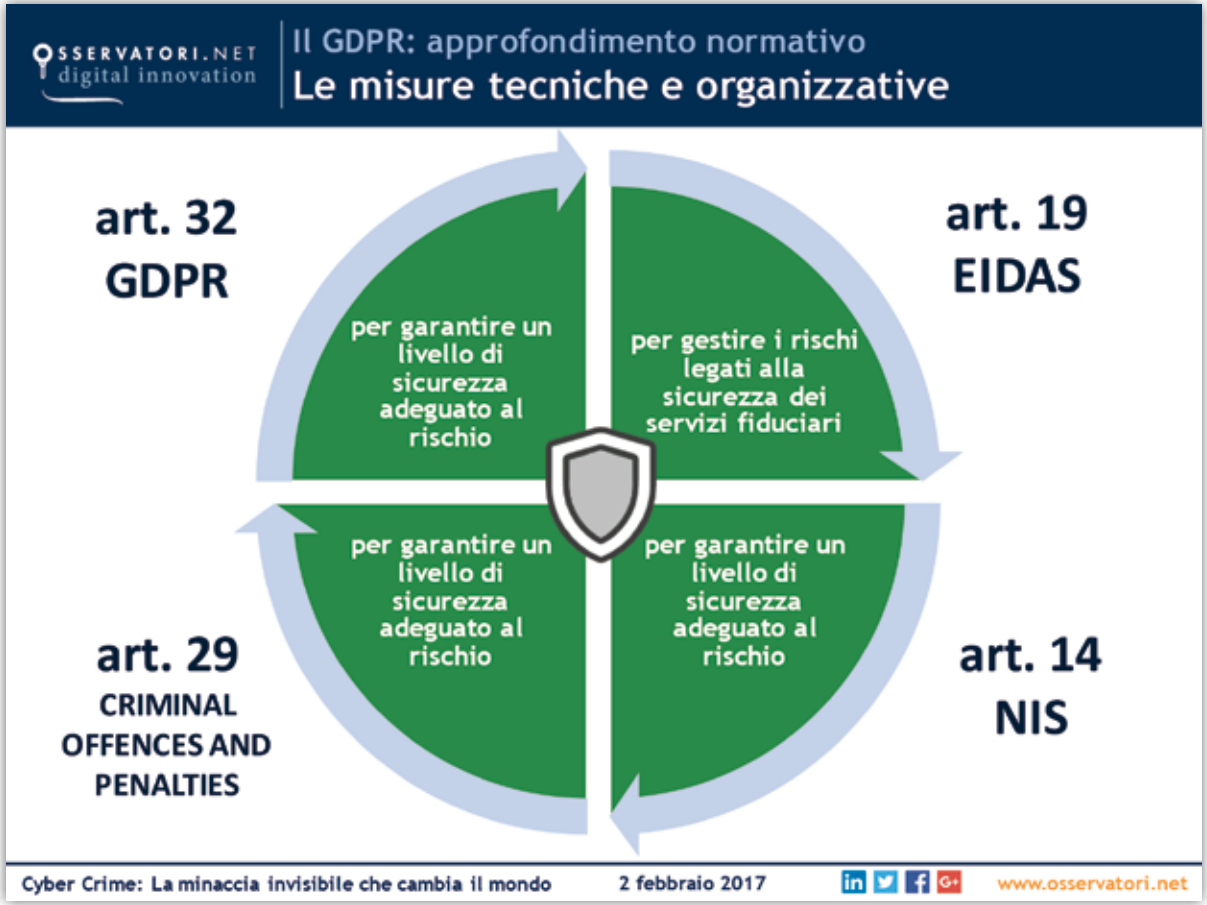
Cyber Crime: La minaccia invisibile che cambia il mondo 2 febbraio 2017 www.osservatori.net

I risultati completi della Ricerca sono consultabili su www.osservatori.net

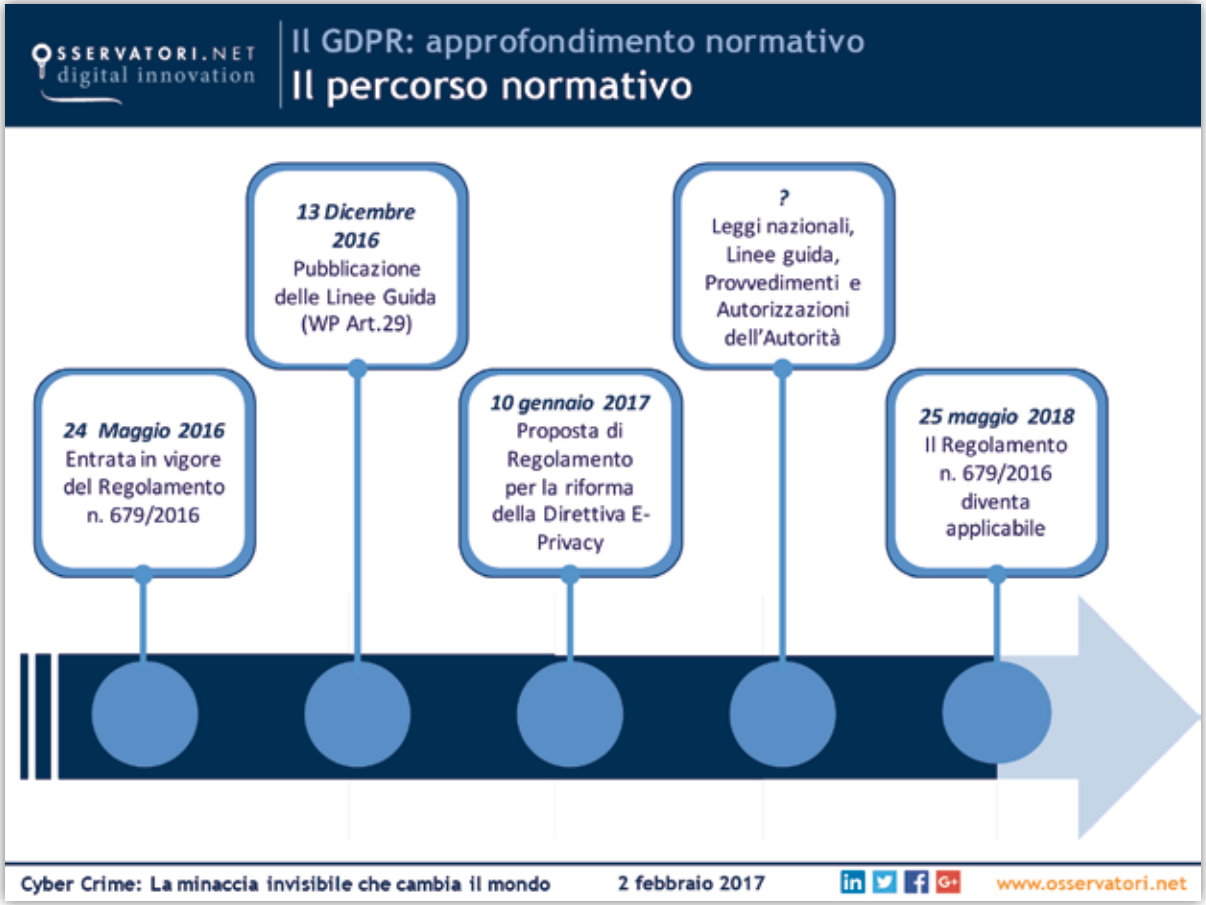



Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net


I risultati completi della Ricerca sono consultabili su www.osservatori.net

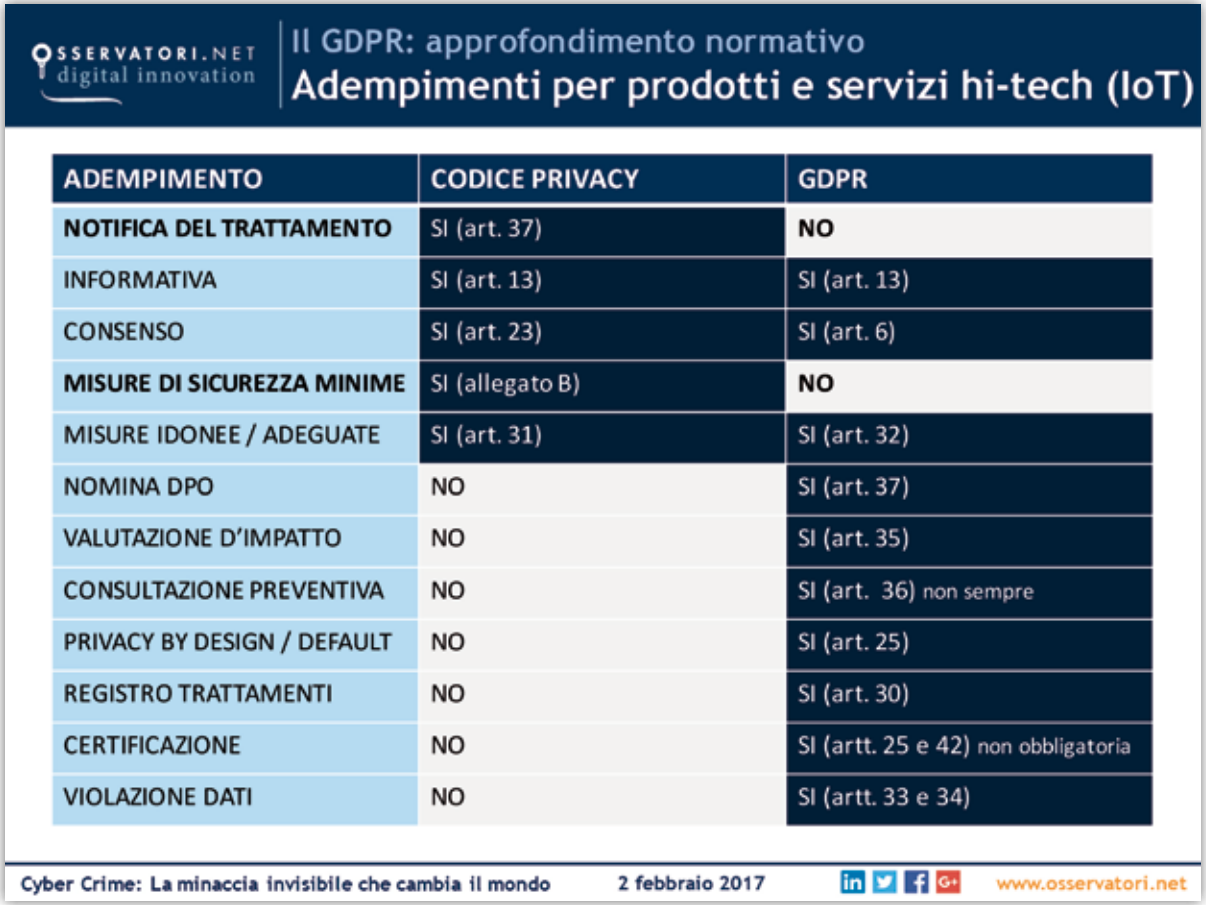



Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net




I risultati completi della Ricerca sono consultabili su www.osservatori.net


Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net



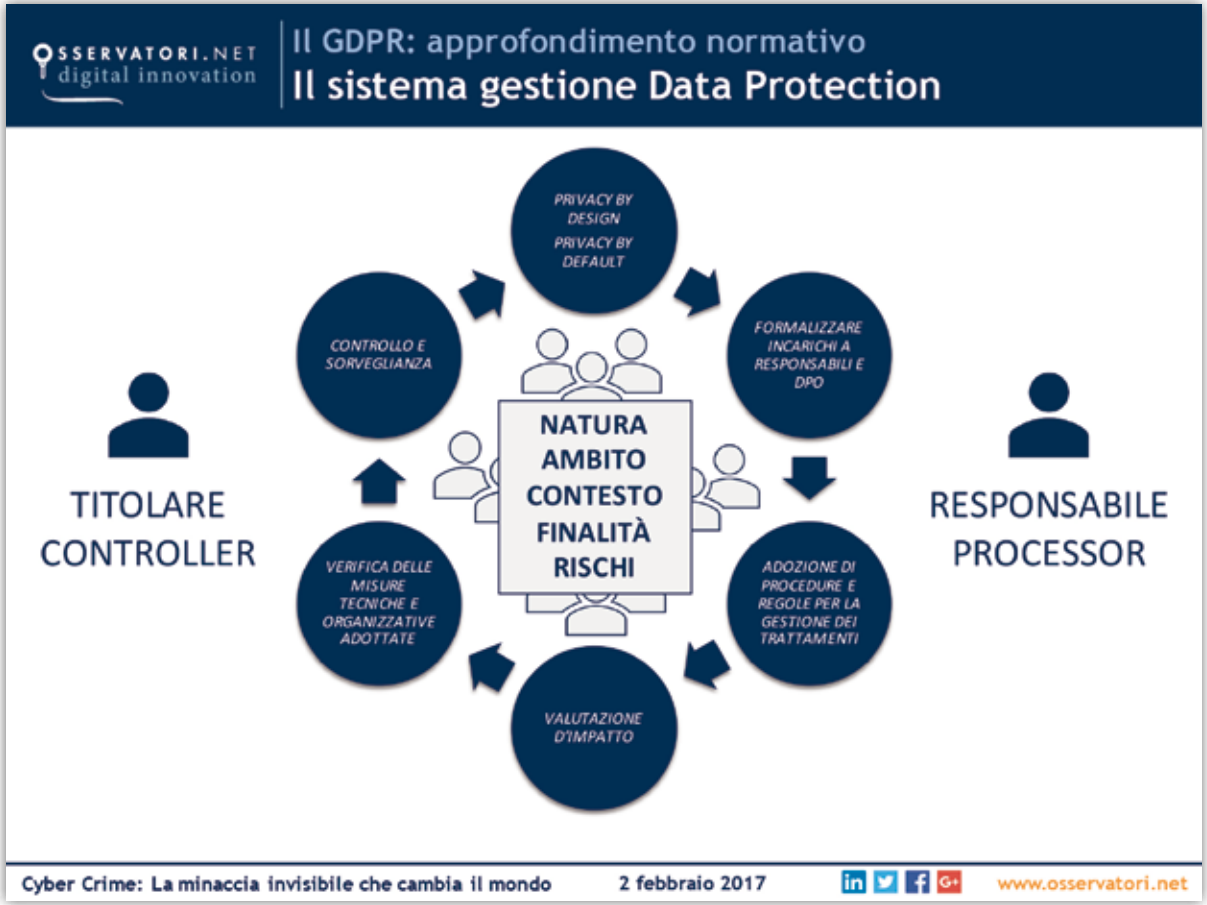
OSSERVATORI.NET digital innovation

## Il GDPR: approfondimento normativo
## Adempimenti per prodotti e servizi hi-tech (IoT)

| ADEMPIMENTO | CODICE PRIVACY | GDPR |
|---|---|---|
| **NOTIFICA DEL TRATTAMENTO** | SI (art. 37) | **NO** |
| INFORMATIVA | SI (art. 13) | SI (art. 13) |
| CONSENSO | SI (art. 23) | SI (art. 6) |
| **MISURE DI SICUREZZA MINIME** | SI (allegato B) | **NO** |
| MISURE IDONEE / ADEGUATE | SI (art. 31) | SI (art. 32) |
| NOMINA DPO | NO | SI (art. 37) |
| VALUTAZIONE D'IMPATTO | NO | SI (art. 35) |
| CONSULTAZIONE PREVENTIVA | NO | SI (art. 36) non sempre |
| PRIVACY BY DESIGN / DEFAULT | NO | SI (art. 25) |
| REGISTRO TRATTAMENTI | NO | SI (art. 30) |
| CERTIFICAZIONE | NO | SI (artt. 25 e 42) non obbligatoria |
| VIOLAZIONE DATI | NO | SI (artt. 33 e 34) |

Cyber Crime: La minaccia invisibile che cambia il mondo 2 febbraio 2017 www.osservatori.net

**I risultati completi della Ricerca sono consultabili su www.osservatori.net**




Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net


I risultati completi della Ricerca sono consultabili su www.osservatori.net


**Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net**


**I risultati completi della Ricerca sono consultabili su www.osservatori.net**


Nel corso del 2016 lo "slancio" verso aree progettuali innovative sembra aver subito un freno.

Le iniziative su cui si è rivolta l'attenzione si possono ricondurre alle tematiche maggiormente "tradizionali" della sicurezza informatica.

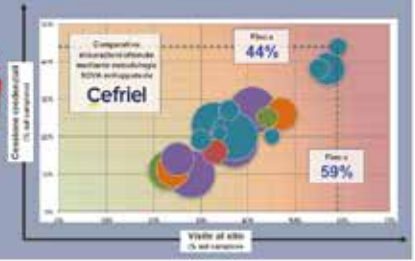
Ciò, in un panorama mondiale in cui attacchi anche a bassa complessità hanno sempre maggior risonanza e ottengono risultati.

## PIU' SENSIBILIZZAZIONE MA…

Corsi di Formazione
(sessioni d'aula o e-learning) **66%**

Attività di vulnerability assessment sui dipendenti
(es. simulazione di campagne di phishing) **28%**

Update: 01/2017






I moderni attacchi si realizzano mediante un connubio sempre più inscindibile tra tecnologia e ingegneria sociale.

La componente tecnologica degli exploit è sempre più raffinata… ogni minima vulnerabilità può essere un accesso.

Tuttavia le modalità di ingaggio delle persone, usate come vettore inconsapevole, sono spesso "basilari", e fanno leva su inconsapevolezza, scarsa conoscenza ICT, distrazione. Le persone devono essere coinvolte in modi efficaci!

**I risultati completi della Ricerca sono consultabili su www.osservatori.net**

## IL CISO PUO' ESSERE EFFICACE?

Orizzonte di budget limitato ("spot" o 1 anno) > 60%

+

Collocazione organizzativa sotto ICT/OPs ~ 70%

=

La collocazione organizzativa del CISO (o figura equivalente) non è facilmente determinabile e dipende fortemente dalla specifica realtà.

Modalità diffuse di approccio rispetto a due leve fondamentali (risorse e potere di intervento) rischiano però di depotenziarne l'operato.

Le iniziative di sicurezza informatica efficaci, oggi, richiedono una vista strategica pluriennale, e spesso rischiano di essere percepite come un ostacolo all'execution della business strategy.

## NUOVI TEMI… VECCHIO APPROCCIO?

### MOBILE SECURITY

Approcci maturi e diffusamente adottati (con inevitabili "deroghe"), lato device management.

E la mobile App strategy?

### CLOUD SECURITY

Molti problemi percepiti… soprattutto quelli relativi ad azioni e comportamenti "del Cloud".

La contromisura? Un uso limitato

### IoT SECURITY

Al di là di quanto se ne parli, poche azioni in campo e scarso presidio.

E se si allarga a SCADA, ICS e apparati SOHO…

### CYBER INSURANCE

Scarsamente diffusa sia in termini di adozione che di offerta.

Quale legame tra "premio" e azioni di mitigazione intraprese? E le PMI?



Il presidio alle tematiche di sicurezza informatica nell'ICT "evoluto" non è certamente assente.

Soprattutto per i paradigmi oramai consolidati, vi è consapevolezza sul rischio e adozione di contromisure.

L'approccio è spesso "conservativo", e rischia di essere limitante anche rispetto alle potenzialità delle tecnologie.

Sui temi ancora relativamente nuovi… la definizione stessa del "perimetro" è incerta.

**I risultati completi della Ricerca sono consultabili su www.osservatori.net**

## QUALI PROSPETTIVE?

- **Una sicurezza "tradizionale" sempre necessaria… non più sufficiente**
  - Quantomeno in termini di necessità pratica. L'attuale panorama degli attacchi non consente in alcun modo di abbassare la guardia su temi considerati "consolidati", tuttavia in un contesto in continuo mutamento in cui il perimetro da presidiare è in costante espansione
- **Il fattore umano come elemento sempre più centrale**
  - Non solo degli attacchi, ma anche (e conseguentemente) delle strategie di protezione. Che tuttavia spesso si dimostrano non all'altezza nella gestione delle peculiarità del tema
- **La possibilità di trasferire il rischio**
  - Mediante approcci assicurativi, che tuttavia, oltre a essere ancora poco diffusi in Italia, ancora stentano a legare misurabilmente il rischio (e la mitigazione "dimostrabilmente" effettuata) con le condizioni offerte, oltre che a trovare applicabilità nel contesto PMI
- **Il GDPR…**
  - Da intendersi (sperabilmente) come ulteriore impulso all'avvio di una strategia di gestione delle minacce di sicurezza informatica che non miri solo alla compliance, ma integri un approccio proattivo con un coinvolgimento realmente diffuso

POLITECNICO MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET digital innovation

Osservatorio Information Security & Privacy

# Cyber Crime: La minaccia invisibile che cambia il mondo

## Gli Attori

Febbraio 2017

## La School of Management del Politecnico di Milano

La **School of Management del Politecnico di Milano**, costituita nel 2003, accoglie le molteplici attività di ricerca, formazione e alta consulenza, nel campo dell'economia, del management e dell'industrial engineering, che il Politecnico porta avanti attraverso le sue diverse strutture interne e consortili.

La Scuola ha ricevuto, nel 2007, il prestigioso accreditamento **EQUIS**. Dal 2009 è nella classifica del **Financial Times delle migliori Business School d'Europa**. Nel Marzo 2013 ha ottenuto il prestigioso accreditamento internazionale da **AMBA** (*Association of MBAs*) per i programmi **MBA** e **Executive MBA**. La Scuola può contare su un corpo docente di più di duecento tra professori, ricercatori, tutor e staff e ogni anno vede oltre seicento matricole entrare nel programma undergraduate. Dal 2014, la Scuola è membro di **UniCON** (*International University Consortium for Executive Education*), **PRME** (*Principles for Responsible Management Education*) e **Cladea** (*Consejo Latinoamericano de Escuela de Administración*).

Fanno parte della Scuola: il **Dipartimento di Ingegneria Gestionale** e **MIP Graduate School of Business** che, in particolare, si focalizza sulla formazione executive e sui programmi Master.

Le attività della School of Management legate all'Innovazione Digitale si articolano in:

- Osservatori *Digital Innovation*, che fanno capo per le attività di ricerca al Dipartimento di Ingegneria Gestionale;
- Formazione executive e programmi Master, erogati dal MIP.

## Gli Osservatori Digital Innovation

Gli Osservatori *Digital Innovation* della School of Management del Politecnico di Milano nascono nel 1999 con l'obiettivo di fare cultura in tutti i principali ambiti di Innovazione Digitale per favorire lo sviluppo del Paese.

***La Vision che guida gli Osservatori è che l'Innovazione Digitale sia un fattore essenziale per lo sviluppo del Paese.***

La **Mission** degli Osservatori è produrre e diffondere conoscenza sulle opportunità e gli impatti che le tecnologie digitali hanno su imprese, pubbliche amministrazioni e cittadini, tramite modelli interpretativi basati su solide evidenze empiriche e spazi di confronto indipendenti, pre-competitivi e duraturi nel tempo, che aggregano la domanda e l'offerta di innovazione digitale in Italia.

Gli Osservatori sono oggi un punto di riferimento qualificato sull'innovazione digitale in Italia che integra attività di Ricerca, Comunicazione, Formazione e una Community sempre più ampia di professionisti.

### *I fattori distintivi*

Le attività degli Osservatori Digital Innovation sono caratterizzate da 3 fattori distintivi.

1. La **Ricerca** sui temi chiave dell'innovazione digitale, basata su solide metodologie (studi di caso, survey, censimenti, quantificazioni di mercato, analisi bibliografiche, ...).

2. La **Community**, composta da decisori e C-Level della domanda, dell'offerta e delle Istituzioni, che collabora e sviluppa relazioni concrete nelle numerose occasioni di interazione.

3. La **Comunicazione**, finalizzata a raggiungere, attraverso Convegni, Media e Pubblicazioni, il più ampio numero di persone, per diffondere buone pratiche, esperienze e cultura legata all'innovazione digitale.

4. La **Formazione**, che attraverso pubblicazioni, webinar e workshop premium del sito Osservatori.net, rappresenta un canale unico per l'aggiornamento professionale sui temi chiave dell'innovazione digitale.

### *Gli Osservatori Digital Innovation (2016-2017)*

Gli Osservatori Digital Innovation sono classificabili in 3 macro categorie:

1. Digital Trasformation, che include gli Osservatori che analizzano in modo trasversale i processi di innovazione digitale che stanno profondamente trasformando il nostro Paese.

2. Digital Solutions, che raggruppa gli Osservatori che studiano in modo approfondito specifici ambiti applicativi e infrastrutturali relativi alle nuove tecnologie digitali.

3. Verticals, che comprende gli Osservatori che analizzano l'innovazione digitale in specifici settori o processi.

**Digital Transformation:**
• Agenda Digitale • Digital Transformation Academy • Startup Hi-tech • Startup Intelligence

**Digital Solutions:**
• Big Data Analytics & Business Intelligence • Cloud & ICT as a Service • eCommerce B2c
• Enterprise Application Governance • Fatturazione Elettronica e Dematerializzazione
• Gestione Progettazione e PLM (GeCo) • Hubility/Multicanalità
• Information Security & Privacy • Internet of Things • Mobile B2c Strategy
• Mobile Payment & Commerce • Smart Working

**Verticals:**
• Cloud nella PA • Contract Logistics • Digital Finance • Digital Insurance
• eGovernment • Export • Gioco Online • HR Innovation Practice • Industria 4.0
• Innovazione Digitale in Sanità • Innovazione Digitale nei Beni e Attività Culturali
• Innovazione Digitale nel Retail • Innovazione Digitale nel Turismo • Internet Media
• Mobile Banking • Professionisti e Innovazione Digitale • Smart AgriFood
• Supply Chain Finance

Riportiamo di seguito alcuni Osservatori in parte correlati all'Osservatorio Information Security & Privacy:

- **Big Data Analytics & Business Intelligence**
- **Cloud & ICT as a Service**
- **Digital Innovation Academy**
- **Enterprise Application Governance**
- **Industria 4.0**
- **Internet of Things**
- **Smart Working**

**I risultati completi della Ricerca sono consultabili su www.osservatori.net**

### *I numeri chiave del 2016*

- **Formazione:** 200 pubblicazioni con i risultati delle ricerche; 200 workshop e webinar; archivio di 800 Pubblicazioni e 300 Eventi on demand.
- **Ricerca:** 34 Osservatori; 5.000 casi; 80 Professori/Ricercatori/Analisti.
- **Network:** 300 partner e sponsor; 150.000 contatti; 8.500 contatti C-Level; 15.000 partecipanti agli Eventi.
- **Comunicazione:** 200 Eventi; 5.000 Uscite stampa; 20.000 Report cartacei distribuiti; 25 Pubblicazioni scientifiche su riviste internazionali.

Per maggiori informazioni si veda il sito **www.osservatori.net**

Seguici anche su:

### *Startup Boosting*

Gli Osservatori, con il progetto *Startup Boosting*, intendono giocare un ruolo sempre più attivo nello *stimolare la nascita e lo sviluppo di nuove avventure imprenditoriali* in ambito digitale in Italia basate sull'innovazione nella convinzione che ciò rappresenti un ingrediente fondamentale per il rilancio della nostra economia.

*Startup Boosting* si pone l'obiettivo, nei diversi settori digitali, di identificare *le idee di business e i progetti imprenditoriali più innovativi*, che saranno supportati e seguiti nel loro sviluppo dalla School of Management del Politecnico di Milano.

Ogni mese vengono valutate le proposte pervenute.

## MIP Politecnico di Milano Graduate School of Business

Gli Osservatori *Digital Innovation* sono fortemente integrati con le attività formative della Scuola: nel senso che rappresentano un'importante sorgente per la produzione di materiale di insegnamento e di discussione per i corsi e traggono anche spesso linfa vitale dalle esperienze di coloro che partecipano ai corsi (in particolare a quelli post-universitari erogati dal MIP) o vi hanno partecipato nel passato.

In sinergia con gli Osservatori, il MIP Politecnico di Milano Graduate School of Business ha lanciato diverse iniziative nell'ambito Digital Innovation:

- Master Executive MBA con possibilità di scegliere corsi elective focalizzati sui temi della Digital Business Transformation;
- Percorso Executive in Gestione Strategica dell'Innovazione Digitale;
- Corsi brevi Digital Innovation.

Per maggiori informazioni si veda il sito **www.mip.polimi.it**

### *Startup Program*

Lo Startup Program è una delle iniziative dell'*Entrepreneurship Academy*, il programma culturale del MIP Politecnico di Milano Graduate School of Business, volto a supportare startupper, imprenditori ed executive nello sviluppo di progetti imprenditoriali.

Il Corso si rivolge ad imprenditori di aziende appena nate (startup) e aspiranti imprenditori (startupper) ed è indicato anche per sviluppatori fortemente motivati all'attività imprenditoriale.

Il programma ha l'obiettivo di supportare i partecipanti nella messa a punto del proprio progetto imprenditoriale, attraverso un alternarsi di lezioni in presenza, assignement da svolgere a distanza, analisi di casi reali e testimonianze; contribuire allo sviluppo e al potenziamento delle "soft skill" rilevanti nel percorso imprenditoriale (innovazione, leadership, negoziazione e gestione dei conflitti, capacità di comunicazione e motivazione, empowerment, ecc.) attraverso specifiche attività di coaching; fornire un insieme di strumenti e metodologie che possano aiutare lo startupper o l'imprenditore nell'analisi e nella gestione del proprio progetto imprenditoriale.

Per maggiori informazioni si veda il sito **www.mip.polimi.it**

POLITECNICO
MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET
digital innovation

# Il punto di riferimento
## per l'Aggiornamento Executive sull'Innovazione Digitale

visita **www.osservatori.net** e scopri come accedere a tutti i servizi

**L'innovazione digitale a portata di Click!**

In un contesto in cui l'innovazione digitale ha sempre più rilevanza per la competitività delle imprese e il cambiamento incessante caratterizza le nuove tecnologie, aggiornarsi è fondamentale per tutti i professionisti a vari livelli aziendali. Dedicare tempo e risorse all'aggiornamento di skill e competenze in questo ambito è fondamentale e va fatto in modo permanente lungo tutta la vita professionale, attraverso nuovi strumenti compatibili con il lavoro quotidiano.

**Osservatori.net**

Gli Osservatori Digital Innovation rappresentano una fonte unica di conoscenza sull'Innovazione Digitale sviluppata da un team di oltre 80 Ricercatori e Professori del Politecnico di Milano, che da anni punta a fornire a professionisti, manager e imprenditori una visione strategica e manageriale dell'innovazione digitale, consapevole che questa rappresenta una leva indispensabile per la competitività delle imprese e il rilancio economico e sociale del nostro Paese.

**Fattori Distintivi**

- Piattaforma multimediale e interattiva per un aggiornamento continuo a distanza;

- Ricerca indipendente, caratterizzata da rigore scientifico, modelli originali e basata sull'analisi dell'eccellenza;

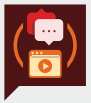
- Analisti e esperti con un know-how unico e distintivo al servizio di manager e professionisti.

**Rapporti**

Osservatori.net offre la più completa raccolta di analisi e dati sull'Innovazione Digitale in Italia. I Rapporti sono caratterizzati da formati innovativi che consentono una rapida ricerca delle informazioni di proprio interesse

**Workshop e Webinar Premium**

Eventi Premium della durata di circa 4 ore (Workshop) e 1 ora (Webinar), durante i quali i partecipanti possono confrontarsi con gli Analisti e Esperti che approfondiscono i temi chiave dell'innovazione digitale



**Percorsi**

Workshop e Webinar sono organizzati in *Percorsi* focalizzati su un particolare tema:

- AGENDA DIGITALE
- BIG DATA & ANALYTICS STRATEGY
- CLOUD COMPUTING STRATEGY & BUSINESS MODEL
- CUSTOMER RELATIONSHIP MANAGEMENT
- DIGITAL TRAVEL INNOVATION
- ECOMMERCE & CUSTOMER EXPERIENCE STRATEGY
- FATTURAZIONE ELETTRONICA E DEMATERIALIZZAZIONE
- HR INNOVATION & SMART WORKING PRACTICE
- INFORMATION SECURITY & PRIVACY
- INTERNET MEDIA STRATEGY
- INTERNET OF THINGS APPLICATION
- MOBILE APP DEVELOPMENT
- MOBILE B2C STRATEGY
- MOBILE PAYMENT
- SOCIAL MEDIA STRATEGY
- STARTUP & INNOVATION

**Percorso – Big Data & Analytics Strategy**
Per comprendere il valore strategico e sfruttare il potenziale innovativo dei Big Data Analytics e della Business Intelligence.

| | |
|---|---|
| **Webinar** | I Big Data e le attività di profilazione: gli aspetti legali da considerare nella configurazione dei sistemi informatici |
| **Workshop** | Big Data e problematiche di gestione della privacy |
| **Webinar** | Big Data Strategy: scenari, opportunità e organizzazione |
| **Webinar** | Business Analytics & Big Data Analytics: metodologie e applicazioni |
| **Webinar** | Big Data & Social Intelligence: come gestire in modo efficace i dati provenienti dai Social Network e dal web |
| **Webinar** | Le nuove professionalità e competenze per la gestione dei Big Data |
| **Webinar** | Big Data: l'ecosistema delle startup |
| **Webinar** | Big Data & IoT: come gestire in modo efficace i dati raccolti dai sensori |

**Percorso – Customer Relationship Management**
Approfondimenti sui sistemi di CRM per comprendere come trattare dati e informazioni, definire i processi e avere un quadro sulle principali tecnologie.

| | |
|---|---|
| **Webinar** | Come trattare i dati raccolti dai social media nell'ambito dei sistemi CRM |
| **Workshop** | Marketing e trattamento dei dati personali: impostare un sistema CRM nel rispetto delle normative vigenti |
| **Webinar** | Calcolare e gestire il customer lifetime value |
| **Webinar** | Data-driven marketing e CRM: come mettersi in moto? |
| **Webinar** | Sistemi CRM: tra normativa attuale e regolamento europeo in materia di protezione dei dati |

**Percorso – Information Security & Privacy**
Per conoscere i temi chiave della sicurezza informatica, realizzato in collaborazione col CLUSIT (Associazione Italiana per la Sicurezza Informatica).

| | |
|---|---|
| **Webinar** | I rischi nascosti nelle soluzioni di continuità operativa e disaster recovery |
| **Webinar** | Regolamento Generale sulla Protezione dei Dati: cosa fare ora? |
| **Webinar** | Utilizzo della SPID per i servizi aziendali |
| **Webinar** | Da quali rischi tutelare il Top Management, per proteggere l'azienda? |
| **Webinar** | Novità su DPO e certificazioni in materia di data protection |
| **Webinar** | Pianificare la conformità al nuovo Regolamento Europeo Privacy |
| **Webinar** | Privacy: come costruire il registro dei trattamenti previsto dal RGDP |
| **Webinar** | La DPIA (Data Protection Impact Assessment) nel Regolamento EU 679/2016 |
| **Webinar** | Analisi del Rischio Informatico: uno strumento indispensabile per la protezione del patrimonio aziendale e per la conformità alle nuove normative |
| **Webinar** | Operational Technology, Industria 4.0, IoT e Cloud: il nuovo perimetro della Cyber Security Industriale |


Per maggiori informazioni sui percorsi

**matteo.castiglioni**@osservatori.net

tel. **+39 02 2399 9590**

cell. **+39 392 3821952**

Per maggiori informazioni sugli abbonamenti

**damiano.degaspari**@osservatori.net

tel. **+39 02 2399 9597**

cell. **+39 349 2818600**

Per maggiori informazioni sugli abbonamenti aziendali

**andrea.vanazzi**@osservatori.net

tel. **+39 02 2399 4813**

cell. **+39 342 9212906**

# Information Security Management

## Percorso Executive e Corsi brevi
Marzo – Luglio 2017

12^ Edizione

www.securman.it

Cefriel
POLITECNICO DI MILANO

MIP
POLITECNICO DI MILANO
GRADUATE SCHOOL OF BUSINESS

in collaborazione con

AIEA

INFO
Maria Teresa Bloise
Digital Knwoledge & Education
+39 0223954343
MariaTeresa.Bloise@cefriel.com

**www.cefriel.com**
Cefriel - Politecnico di Milano
Via Renato Fucini, 2
20133 Milano -IT

## OBIETTIVI E TARGET

Cefriel e MIP Politecnico di Milano presentano la 12ˆ edizione del Percorso Executive in Information Security Management, che si propone di formare esperti a 360° nella progettazione e gestione del sistema preposto alla tutela della sicurezza del patrimonio informatico ed informativo di un'azienda.

UN ESPERTO CHE SIA IN GRADO DI:

- Comprendere e valutare la complessità delle problematiche di sicurezza che impattano sull'ICT aziendale, anticipandole con un approccio proattivo.
- Stimare i costi e i benefici delle diverse soluzioni, valutare il ritorno degli investimenti in sicurezza e comprendere i risvolti organizzativi dell'information security.
- Più in generale, progettare, valutare, implementare e gestire un Information Security Management System, integrato con il core business aziendale, in accordo ai principali standard di riferimento, favorendo quindi una efficace gestione dei rischi noti o prevedibili ed anticipando l'insorgenza dei nuovi.

Il corso è rivolto a responsabili dei sistemi informativi, di reti e di organizzazione di piccole, medie e grandi imprese industriali, di servizi e della Pubblica Amministrazione, nonché a tutti gli specialisti che operano nel campo della consulenza e della gestione in outsourcing di reti e di sistemi informativi.
Si rivolge in particolare a chi ricopre o ricoprirà ruoli di responsabilità nella propria organizzazione con riferimento alla gestione e alla tutela del patrimonio informativo e tecnologico.
E' il percorso ideale per chi è tendenzialmente destinato ad assumere il ruolo di Information Security Manager o Chief Information Security Officer, e a tutti i consulenti che desiderino rafforzare il proprio bagaglio di competenze in quest'area.

## LA STRUTTURA DEL CORSO

Il percorso si compone di tre macro-aree tematiche fortemente integrate tra loro: technology, management e legal, con approfondimenti su "temi caldi" nel mondo dell'ICT security.

UNDERLYING TECHNOLOGY & HOT TOPICS
Per cogliere la dinamicità del panorama dell'Information Security, il corso mira a costruire una solida base di fondamenti sul tema, con un approfondimento sui "temi caldi" del momento. La vista complessiva parte dagli aspetti maggiormente legati alla infrastrutture fisiche, tocca la sicurezza delle applicazioni, la disponibilità dei servizi, le verifiche di conformità, fino alla governance.
L'obiettivo è quello di fornire gli strumenti metodologici per attuare un'efficace protezione del patrimonio informativo aziendale, raccogliendo le sfide e le tendenze di un ambito in continua e rapida evoluzione.

ORGANIZATION AND MANAGEMENT
È dedicata all'esame di tutti gli aspetti organizzativi ed economico-gestionali legati all'Information Security. Si tratterà di governance, certificazioni, contromisure di natura organizzativo-procedurale, metodologie di valutazione ex- ante delle alternative di intervento, gestione della fase di implementazione dei progetti di info-security e misurazione delle prestazioni ottenute.

LEGAL
Affronta tutte le problematiche di carattere giuridico-legale connesse alla creazione, alla conservazione e alla circolazione dei dati e delle informazioni, in particolare riservate, in Internet e nelle aziende. Le tematiche legali sono affrontate dal duplice punto di vista della compliance e della protezione dagli illeciti interni ed esterni.

## DIDATTICA

L'architettura del percorso è ispirata dall'adozione di metodologie didattiche basate su partecipazione attiva e momenti di elaborazione personale che facilitano l'apprendimento e stimolano la capacità innovativa e applicativa. Tali metodologie rappresentano lo schema unificante dell'intero percorso e verranno declinate con modalità diverse nei moduli.

In particolare sarà dato ampio spazio a:
- Discussioni in aula
- Esercitazioni e sviluppo di casi
- Testimonianze aziendali e di professionisti con ampia esperienza sul campo
- Dimostrazioni mediante utilizzo di tools (commerciali e open source)

PROJECT WORK
Elemento fondamentale dell'esperienza formativa è il Project Work, che si propone di sviluppare un progetto di innovazione maturando competenze ed attitudini specifiche. Ogni Project Work sarà realizzato in piccoli gruppi, ciascuno seguito da un tutor Cefriel. Prevedono lo sviluppo di lavori proposti dagli stessi allievi (in potenziale sinergia con iniziative in essere presso le loro aziende di provenienza) con il supporto del tutor per indirizzare i lavori e fornire spunti metodologici.

LA COMMUNITY
La community del corso annovera professionisti qualificati del settore della sicurezza informatica ed è un costante punto di contatto e confronto per un aggiornamento continuo sui temi dell'ICT Security.

# CEFRIEL

CEFRIEL è un Digital Innovation and Design Shop che opera dal 1988 nell'ambito dell'innovazione, della ricerca e della formazione per aziende e Pubbliche Amministrazioni. Suo obiettivo primario è rafforzare i legami tra università e imprese attraverso un approccio multidisciplinare che, partendo dalle esigenze dell'impresa, integra i risultati della ricerca, le migliori tecnologie presenti sul mercato, gli standard emergenti e la realtà dei processi industriali, per innovare o realizzare nuovi prodotti e servizi che uniscono ICT e Design.

Il capitale umano è costituito da circa 130 professionisti, ai quali si affiancano docenti e ricercatori universitari, esperti del mondo delle imprese, visiting researcher, studenti. I docenti universitari rivestono un ruolo proattivo. In particolare, essi sono i mentor scientifici per lo sviluppo delle competenze all'interno del centro e la guida scientifica nelle iniziative di ricerca. I professionisti di Cefriel sono ingegneri e laureati in discipline scientifiche con titoli accademici plurimi (master post-laurea, PhD, MBA, etc.), i più senior con oltre 10-15 anni di esperienza.

Unica azienda italiana a essere inserita da Gartner tra i "Cool Vendors in IoT Solutions 2016", Cefriel è organizzato in centri di competenza specialistici che coprono tutte le aree dell'Information and Communication Technology, dalla microelettronica alle interfacce utente più evolute, in particolare nell'ambito di API Economy and Distributed Architectures, Business and Analytics, Design, Information Security and Infrastructures, Internet of Things, Project Management, Smart Cities, Cross-channel Web, Mobile and Wearable.

Sfruttando le proprie competenze multidisciplinari distintive, CEFRIEL è in grado di sviluppare soluzioni all'avanguardia, dall'ideazione fino all'esecuzione di progetti complessi, integrando hardware, software e le più recenti tecnologie di comunicazione multimediale.

CEFRIEL è oggi una società consortile a responsabilità limitata senza scopo di lucro i cui soci sono il Politecnico di Milano, l'Università degli Studi di Milano, l'Università degli Studi di Milano-Bicocca, l'Università degli Studi dell'Insubria, la Regione Lombardia e aziende multinazionali operanti nei settori ICT, dei media e dell'energia. Inoltre, con la presenza negli USA e in Europa (in particolare UK), CEFRIEL rafforza ulteriormente il supporto alle crescenti esigenze d'innovazione delle imprese anche a livello internazionale. Dal 2014 CEFRIEL è anche affiliate partner di EIT ICT Labs, la rete di centri di ricerca leader in Europa nel campo dell'innovazione ICT, e ospita il nodo satellite di Milano.

# Il Dipartimento di Elettronica, Informazione e Bioingegneria

POLITECNICO MILANO 1863
DIPARTIMENTO DI ELETTRONICA, INFORMAZIONE E BIOINGEGNERIA

Il Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB) è uno dei più grandi dipartimenti di ICT in Europa. Con circa 840 collaboratori, tra personale di ricerca strutturato, collaboratori esterni, studenti di dottorato e personale tecnico e amministrativo, il Dipartimento costituisce una realtà vitale in grado di sostenere la formazione, la ricerca di base, la ricerca applicata e l'attività di trasferimento tecnologico alle imprese.

La qualità della ricerca scientifica è l'obiettivo principale del DEIB, perseguito secondo i più elevati standard internazionali di qualità. All'interno del dipartimento sono presenti competenze eccellenti e consolidate, sia a livello nazionale che internazionale, nei settori dell'automazione, dell'informatica, dell'elettronica, della bioingegneria, dell'ingegneria elettrica e delle telecomunicazioni.

La qualità del lavoro di ricerca è testimoniata dalla vasta rete di collaborazioni con le migliori istituzioni internazionali, che fa del Dipartimento uno dei principali attori dello scenario mondiale dell'innovazione scientifica e tecnologica.

L'ambiente di ricerca del DEIB comprende anche la società consortile CEFRIEL e dodici spin-off.

Per maggiori informazioni si veda il sito **www.deib.polimi.it**

# AUSED

È una Associazione tra Utenti di Sistemi e Tecnologie dell'Informazione indipendente e senza scopi di lucro, nata nel 1976; raccoglie circa duecento aziende operanti nei settori industriale, manifatturiero, dei servizi, nonché alcuni enti pubblici. Dal 1996 accetta tra i propri Associati anche persone fisiche che, per formazione o per esperienza aziendale, siano interessate agli scopi ed alle attività dell'Associazione. Dal 2000 l'AUSED ha tra i propri Associati anche aziende che operano nel settore dell'I.C.T., qualificandole dal 2005 come Soci Sostenitori. L'AUSED non ha condizionamenti di tipo politico, non ha sponsorizzazioni di fornitori e "vive" della sola quota associativa.

*AUSED ambisce ad essere il "VERO" punto di riferimento per la "community ICT" in Italia ed in Europa.*

La nuova strategia di sviluppo dell'associazione si inquadra in un contesto più ampio e coerente con gli obiettivi associativi che mirano a consolidare il ruolo di leadership per l'associazione riconosciuto anche dalle istituzioni.

- *Responsabilità verso il Paese* – che per AUSED siginfica responsabilità delle Aziende – e verso le Aziende associate, ovvero "saper rappresentare e creare valore per le Aziende": questo è un ruolo che compete ad AUSED come associazione.
- *Sguardo al futuro e valorizzazione dei giovani*, non esclusivamente in senso anagrafico, ma come categoria logica che comprende tutti coloro che provano a fare qualcosa e si mettono in gioco, in un mondo sempre più dominato dalle chiacchiere; quindi saper "*valorizzare le esperienze ed al tempo stesso creare anche un percorso professionale per i Junior e le nuove leve*".
- *Innovazione e ricerca della produttività come motori dello Sviluppo Economico*, dove

AUSED può essere un driver notevole in Italia nella misura in cui saprà capitalizzare tutte le competenze e le capacità che riesce ad aggregare, orientandole nella giusta direzione.

L'attività dell'AUSED si concretizza con l'organizzazione di incontri, seminari, corsi, gruppi di studio, indagini ecc., che sono caratterizzati, oltre che da elevata professionalità, da estrema concretezza, in quanto costantemente tesi alla risoluzione dei problemi di scelta, sviluppo, gestione ed adozione delle Tecnologie dell'Informazione nelle aziende. Tali attività sono rese possibili grazie all'impegno professionale e personale dei Consiglieri e degli altri Organi direttivi che svolgono la loro opera a titolo gratuito.

Per maggiori informazioni si veda il sito **www.aused.org**

# Clusit

Il Clusit, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più autorevole associazione italiana nel campo della sicurezza delle informazioni.

Collabora con diversi Ministeri ed Agenzie Governative, con le Forze dell'Ordine, con il Garante per la Privacy, con Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Banca d'Italia, Confindustria e Confcommercio.

Tra le attività ed i progetti per il 2017, ci sono: la produzione di documenti tecnico-scientifici; la formazione specialistica, fruibile anche da remoto; il Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria, arrivato alla 12a edizione; i Security Summit, conferenze specialistiche a Milano in marzo, Roma in giugno e Verona in ottobre; il Rapporto Clusit, rapporto annuale sul Cyber-crime e sullo stato della sicurezza delle informazioni e delle reti in Italia; il Mese Europeo della Sicurezza Informatica, campagna di sensibilizzazione della Commissione Europea e dell'ENISA che si svolge ogni anno in ottobre, coordinata in Italia da Clusit.

Clusit è su **www.clusit.it**

# Europrivacy

Europrivacy.info è un blog collettivo, che nasce nel 2015 da un'iniziativa di Aused, di Clusit e di Oracle Community for Security, di professionisti esperti in Sicurezza e Compliance che vogliono contribuire allo sviluppo della consapevolezza delle organizzazioni in merito al nuovo Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679) e alle norme europee collegate.

Il punto di vista che si propone di esprimere è multidisciplinare e si realizza grazie al lavoro di contributori provenienti sia dal mondo Legal sia da quello dell'Information Technology. Il blog ha l'obiettivo di diventare un punto di riferimento nel percorso di adeguamento alla nuova normativa e di contribuire al dibattito internazionale, di conseguenza i post sono sempre tradotti in inglese.

Europrivacy.info è un sito aperto e dinamico in cui puoi trovare le ultime notizie, registrare i tuoi commenti su ciò che sta accadendo, porre domande per approfondire e contribuire con il tuo punto di vista. Il nuovo Regolamento UE affronta una gamma molto ampia di temi e tocca aspetti che interessano molte altre leggi e regolamenti nazionali o internazionali. Per questo abbiamo deciso di limitare il nostro lavoro solo in due aree:

- Capire l'impatto sulle aziende e come meglio gestirlo.
- Concentrarsi sui collegamenti e le sovrapposizioni tra Compliance e IT Security.

La pubblicazione dei contenuti è libera nel rispetto delle regole del blog che è dedicato a questi argomenti.

Questa iniziativa mette in relazione chi ha bisogno di risposte con chi può darle. Una vasta comunità di esperti ha accettato di contribuire con articoli e riportando notizie, pro bono e con il sostegno delle rispettive aziende. Alcune importanti aziende nel campo della compliance e della sicurezza hanno deciso di sponsorizzare questa iniziativa; i loro nomi sono nella pagina degli sponsor, e sono oltre 50 i professionisti che contribuiscono ad arricchire il contenuto del blog. Tra di loro si trova un gruppo di persone, composto da 6 coordinatori e da un sistemista, un social media manager, un traduttore, un'assistente per il reporting e un "interlocutore dei contributori", che si occupa del corretto funzionamento del blog.

Europrivacy non è tuttavia solo un blog: sono numerose le iniziative, gli eventi, gli articoli apparsi sulla stampa che i coordinatori hanno organizzato in questi mesi e che hanno coinvolto i contributori del blog in veste di relatori e/o autori e rappresentano ulteriori occasioni di confronto e di visibilità per i partecipanti. Contribuisci anche tu a rendere questa iniziativa un successo: costruirai così anche il tuo successo! Sul sito ci sono le istruzioni per contribuire (a livello personale) e sponsorizzare (a livello aziendale).

Per maggiori informazioni si veda il sito **europrivacy.info/it**

# I Sostenitori della Ricerca

## Partner

- AlmavivA
- BT Italia
- Kaspersky Lab
- Poste Italiane
- Spike Reply
- Symantec
- TESISQUARE®
- Trend Micro

## Sponsor

- Hitachi Systems CBT
- Sinergy

## Supporter

- Horizon Security

**AlmavivA**
www.almaviva.it

**AlmavivA** è sinonimo di innovazione tecnologica. Esperienze consolidate, competenze uniche, ricerca continua e una puntuale conoscenza dei diversi settori di mercato, pubblico e privato, ne fanno *il Gruppo leader italiano nell'Information & Communication Technology.*

Con *45.000 persone, 12.000 in Italia e 33.000 all'estero*, AlmavivA è il 6° Gruppo privato italiano per numero di occupati al mondo, il 3° a guida imprenditoriale, con un fatturato nel 2015 pari a 709 milioni di euro.

AlmavivA *opera a livello globale*, attraverso 38 sedi in Italia e 21 all'estero, con un'importante presenza in Brasile, oltre che negli Stati Uniti, Cina, Colombia, Tunisia, Romania e a Bruxelles, centro nevralgico della UE.

Il Gruppo AlmavivA raccoglie la sfida che le organizzazioni di qualsiasi dimensione e settore dovranno affrontare nei prossimi anni per rimanere competitive, innovando il proprio modello di business, la propria organizzazione, la cultura aziendale e l'ICT.
*L'offerta del Gruppo AlmavivA* si articola in quattro macro-aree:

- *Digital Change* – servizi ICT e soluzioni tecnologiche d'eccellenza per far evolvere sistemi e processi di Aziende e Pubbliche Amministrazioni, anche in termini di continuità operativa, privacy e sicurezza dei dati, valorizzando a pieno tutte le opportunità della trasformazione digitale in atto.
- *Knowledge of Everything* – sistemi dedicati alle Imprese 4.0, alla Pubblica Amministrazione e alle Smart Community per trarre il massimo valore dall'Internet delle Cose e delle Persone, creando nuova conoscenza da informazioni e dati provenienti da oggetti, processi e comunicazioni personali, analizzati e interpretati rispetto al contesto culturale, sociale, di business.
- *CRM BPO & CX Services* – consulenza su modelli integrati di Business Process Outsourcing e una gamma estesa di servizi ad alto valore aggiunto per supportare il Customer Journey su tutti i canali di contatto e sviluppare una strategia di Customer Experience di successo.
- *People-centered technologies* – soluzioni basate su Natural language understanding, Big data advanced analytics, Adaptive interfaces e Voice recognition, per la valorizzazione strategica delle informazioni, la semplificazione dei processi operativi, l'efficienza nella Customer Interaction multicanale e nel Knowledge Management.

**BT Italia**
www.bt.com/italia

*Security: un approccio globale alla sicurezza*

La trasformazione digitale a cui stiamo andando incontro ed il progressivo passaggio al cloud rendono più complesso definire il perimetro delle organizzazioni. Con una esposizione agli attacchi sempre crescente, ed un panorama delle minacce in continua evoluzione, proteggere in maniera efficace e completa i dati e l'operatività delle aziende diventa sempre più oneroso.

**BT** da tempo supporta le organizzazioni private e pubbliche nel ripensare il rischio cyber e nel migliorare la capacità di rispondere alle minacce in modo proattivo ed immediato, partendo innanzitutto dalla intelligence globale delle minacce e dall'assessment della situazione corrente, per mettere a punto una strategia vincente.

Per mitigare il rischio occorre adottare le giuste soluzioni, e BT è in grado di selezionare e gestire le tecnologie più adatte, per una strategia di contrasto basata sulla valutazione del rischio, che ponga al centro la rete e che sia indipendente dal vendor di tecnologia. Collaboriamo con i principali vendor di sicurezza ed abbiamo esperti accreditati per installare e gestire le tecnologie più sofisticate, che testiamo sistematicamente nei nostri laboratori di cyber assessment per valutarne l'efficacia sfruttando al meglio i Big Data.

Se dotarsi di soluzioni tecnologiche a protezione delle infrastrutture è il primo passo, un altro elemento critico è la necessità di elevare gli skill a disposizione delle organizzazioni, per ridurre il numero di incidenti imputabili ad errori dei dipendenti.

BT è un player globale -attivo in 180 Paesi e con 14 SOC 'follow the sun' – con una significativa presenza in Italia e con le sue infrastrutture ha un osservatorio privilegiato sugli attacchi alla sicurezza delle reti, malware e violazioni ai danni delle organizzazioni in tutto il mondo.

Le soluzioni di BT oltre a garantire la compliance alle misure per la sicurezza ICT indicate dalle norme e dalla agenzie ed autorità nazionali, hanno anche l'obiettivo di mitigare il rischio rappresentato dalle nuove minacce informatiche e sono realizzate grazie all'esperienza maturata da BT Security nel proteggere sia la rete di BT sia quella dei propri clienti in Italia come in 180 paesi al mondo.

Il portfolio BT Security comprende una gamma di soluzioni puntuali e di servizi di sicurezza gestita end-to-end network-centrici, ma anche di servizi di consulenza e cyber intelligence, così da consentire una miglior comprensione dei rischi di sicurezza a cui far seguire l'implementazione delle giuste misure con cui affrontarli.

BT Security consta di oltre 2.500 specialisti ed è uno dei membri fondatori del Cybersecurity Information Sharing Partnership (CiSP) in Gran Bretagna, è membro dell'IoT Security Foundation e di numerosi progetti internazionali sul tema.

**Kaspersky Lab**
www.kaspersky.com/it

**Kaspersky Lab** è una delle più grandi aziende private di sicurezza informatica al mondo. Opera in 200 Paesi e territori e ha 37 sedi in 32 Paesi. Quasi 3.600 specialisti altamente qualificati lavorano per Kaspersky Lab.

È una multinazionale, con una visione globale e con un focus sui mercati internazionali.

Essere indipendenti ci permette di essere più flessibili, di pensare in modo differente e di agire più velocemente. Siamo costantemente impegnati ad innovare, offrendo una protezione efficace, fruibile e accessibile. Siamo orgogliosi di essere in grado di sviluppare tecnologie di sicurezza all'avanguardia a livello mondiale che permettono a noi – e a ciascuno dei nostri 400 milioni di utenti e 270.000 clienti corporate – di essere sempre un passo avanti rispetto alle potenziali minacce.

Il nostro impegno nei confronti delle persone e la nostra tecnologia avanzata ci assicurano inoltre un vantaggio sulla concorrenza. La nostra società è stata nominata come "Leader" nella protezione degli endpoint dalle agenzie di analisi Gartner e Forrester . Saldamente posizionati tra i quattro maggiori vendor di soluzioni di sicurezza endpoint, continuiamo a migliorare la nostra posizione di mercato.

La sicurezza degli endpoint è sempre stata un core business per noi, specialmente per il settore delle PMI. Tuttavia, ci aspettiamo che il mercato enterprise nei prossimi anni rappresenterà uno dei nostri principali fattori di crescita, specialmente nel campo della sicurezza non-endpoint. Le necessità dei nostri clienti cambiano in linea con l'evoluzione del panorama delle minacce. Di conseguenza, il nostro portfolio enterprise è in continua espansione, con servizi e soluzioni di sicurezza rafforzati dall'intelligence globale di sicurezza informatica di Kaspersky Lab.

Il nostro Global Research and Analysis Team (GReAT) è un gruppo d'élite, composto da oltre 40 tra i maggiori esperti di sicurezza che operano in tutto il mondo e forniscono servizi di intelligence e ricerca all'avanguardia mirati a contrastare le minacce.

Il team è noto per la scoperta e l'analisi delle più sofisticate minacce a livello mondiale, incluse, tra le altre, le minacce di cyberspionaggio e cybersabotaggio come Flame e miniFlame, Gauss, RedOctober, NetTraveler, Icefog, Careto/The Mask, Darkhotel, Regin, Cloud Atlas, Epic Turla Equation, Duqu 2.0, Metel, Adwind, ProjectSauron, Sofacy (Fancy Bear), CozyDuke (Cozy Bear), Black Energy (Sand Worm) e così via.

**Poste Italiane**
www.posteitaliane.it

**Poste Italiane** è la più grande infrastruttura di servizi in Italia. Grazie alla presenza capillare su tutto il territorio nazionale, ai forti investimenti in ambito tecnologico e al patrimonio di conoscenze rappresentato dai suoi *143mila dipendenti*, Poste Italiane ha assunto un ruolo centrale nel processo di crescita e modernizzazione del Paese.

Oggi fornisce servizi logistico-postali, di risparmio e pagamento, assicurativi e di comunicazione digitale a oltre *32 milioni* di clienti.

Gli importanti investimenti in *ricerca e sviluppo* e nella *formazione* dei propri dipendenti hanno inoltre consentito a Poste Italiane di creare servizi avanzati basati sulle esigenze dei clienti e capaci di cogliere le trasformazioni sociali del nostro Paese.

Da sempre attenta al *rispetto dell'ambiente* e ai temi dello *sviluppo sostenibile*, l'Azienda è impegnata nella riduzione delle emissioni e nell'abbattimento dell'inquinamento attraverso un sempre maggiore utilizzo di energia da fonti rinnovabili e la scelta di veicoli a basso impatto ambientale.

L'attenzione all'innovazione e alle persone e la vicinanza territoriale sono alla base dei *risultati di eccellenza* raggiunti da Poste Italiane in particolare nel settore finanziario e ancor più in quello assicurativo, dove Poste Vita ha fatto registrare una crescita straordinaria che l'ha proiettata al secondo posto tra le compagnie di assicurazione attive in Italia.

**Spike Reply**
www.reply.eu

**Spike Reply** è la società del Gruppo Reply specializzata nei servizi di consulenza e soluzioni integrate di Cyber Security.

L'avvento del mondo digitale, e la crescente interconnessione di persone, dispositivi e organizzazioni, sono fonte di maggiori vulnerabilità e di nuovi rischi.

La rapida evoluzione delle esigenze di business e la continua introduzione di nuove tecnologie quali Mobilità, Consumerizzazione, Cloud, automazione industriale, Internet of Things (automotive, smart homes/cities, wearable devices, …) aumentano la possibilità di esposizione al cybercrime e all'utilizzo illecito delle risorse.

Spike Reply supporta le aziende creando e mantenendo un Programma di Cyber Security per governare, analizzare, proteggere, rilevare e rispondere al panorama delle minacce, sviluppando e implementando le protezioni adeguate.

**Symantec**
www.symantec.com

**Symantec** (NASDAQ: SYMC) è uno dei leader nella cybersecurity.

Disponendo di una delle reti di cyber intelligence più estese al mondo, abbiamo visibilità su un ampio panorama di minacce e proteggiamo i nostri clienti da attacchi avanzati.

Aiutiamo aziende, governi e persone a mettere al sicuro i propri dati più importanti, ovunque risiedano.

Dai dati di analisti di mercato Symantec emerge come leader di mercato nell'endpoint security, email security, data loss prevention e certificati SSL.

I clienti che si affidano a Symantec:
- proteggono la propria organizzazione da attacchi avanzanti;
- controllano e salvaguardano gli accessi ai dati critici;
- si affidano ai nostri esperti per monitorare la sicurezza aziendale;
- mettono in sicurezza i propri siti web.

L'offerta è stata recentemente arrichita con l'acquisizione di Blue Coat, offrendo un portafoglio di tecnologie integrate che servono una piattaforma per l'offerta di una cloud generation security a livello mondiale.

**TESISQUARE®**
www.tesisquare.com

**TESISQUARE®** – where IT happens è la piazza delle soluzioni software di tipo collaborativo, protagonista da 20 anni nel mondo dell'Information Technology, con oltre 250 persone impiegate ed un sistema d'offerta che copre le aree più critiche della gestione di diversi settori aziendali: dalle soluzioni per la supply chain ed il transportation ai servizi EDI e le soluzioni per la fatturazione e conservazione elettronica; dai prodotti per la gestione dei processi HR ai servizi di Application Management; dalla piattaforma cloud "molti a molti", per la condivisione in tempo reale di informazioni e documenti all'offerta verticale dedicata al mondo della distribuzione (TESISQUARE® Retail).

All'interno del proprio portafoglio prodotti, TESISQUARE® propone soluzioni per gestire il controllo di tutti i rischi aziendali ed il governo degli adempimenti correlati alle diverse normative, tra le quali il nuovo Regolamento europeo in materia di protezione dei dati personali, l'Attestazione di bilancio (L. 262/05), la Sicurezza sul lavoro (D.Lgs 81/08), la Disciplina della responsabilità amministrativa delle persone giuridiche (D.Lgs 231/01), il D.Lgs. 219/06 ed il Codice Deontologico di Farmindustria e Transparency Code EFPIA.

La soluzione è inoltre aperta alla gestione di ulteriori normative: ad esempio, l'azienda sta avviando progetti in ambito ISO14001. L'esperienza di TESISQUARE® in tema di Governance Risk & Compliance è ormai pluriennale e consolidata e deriva dall'applicazione delle competenze informatiche dell'azienda alle esigenze specifiche dei clienti.

La sede storica dell'azienda è a Bra (CN), con altre unità operative a Milano, Roma, Torino e Padova. Attraverso l'apertura delle sedi di Amsterdam, Parigi, Barcellona e Istanbul, TESISQUARE® ha inoltre concretizzato il processo di espansione a livello internazionale.

**Trend Micro**
www.trendmicro.it

*Sicurezza semplice, efficace e su misura per le diverse esigenze*

Come leader globale nelle soluzioni di sicurezza informatica, sviluppiamo soluzioni innovative che rendono il mondo sicuro affinché aziende e privati possano scambiarsi informazioni digitali. Con oltre 28 anni di esperienza, siamo riconosciuti come leader nel mercato della sicurezza dei server, in-the-cloud e della protezione dei contenuti per le piccole imprese.

Nel 2016 infatti, per il sesto anno consecutivo siamo stati riconosciuti da IDC come leader nel mercato della sicurezza server, mentre è dal 2002 che Gartner ci considera leader nelle soluzioni di sicurezza enterprise.

La sicurezza **Trend Micro** si adatta alle esigenze dei clienti e partner. Le nostre soluzioni proteggono gli utenti finali su qualsiasi dispositivo, ottimizzano la sicurezza per il moderno datacenter e proteggono le reti dalle violazioni degli attacchi mirati. Offriamo una sicurezza di punta per client, server e cloud che blocca più rapidamente le nuove minacce, rileva meglio le violazioni e protegge i dati in ambienti fisici, virtuali e in-the-cloud.

La nostra sicurezza si fonda sulle informazioni globali sulle minacce raccolte dalla nostra tecnologia Trend Micro Smart Protection Network ed è supportata da oltre 1.200 esperti di sicurezza in tutto il mondo.

I nostri laboratori studiano da sempre l'evoluzione degli scenari delle minacce informatiche, per avere prodotti pronti per rispondere a quelle che sono le nuove tipologie di rischi. Oggi diamo sempre maggiore importanza agli scenari dell'Internet of Things e alle insidie che provengo dal Deep Web, ma non ci limitiamo a proporre le nostre soluzioni, la nostra filosofia è quella di condividere le nostre ricerche, il nostro know how e le competenze sia con i clienti che le istituzioni, per avere una strategia comune di difesa sia a livello aziendale che di sistema Paese.

*Cittadinanza globale*

L'impegno di Trend Micro per essere un'azienda-cittadino socialmente responsabile ha plasmato il modo in cui gestiamo la nostra società sin dalla sua fondazione nel 1988.
Sono disponibili ulteriori informazioni sui nostri programmi e su come traduciamo il nostro impegno in azioni in tutto il mondo.

**Hitachi Systems CBT**
www.hitachi-systems-cbt.com

**Sinergy**
www.sinergy.it

**Hitachi Systems CBT S.p.A.** è il System Integrator attivo nell'ambito dei servizi IT e si rivolge alle Medie e Grandi Imprese, private e pubbliche, che hanno la necessità di implementare le proprie infrastrutture informatiche.

ll Cloud Computing, l'outsourcing tecnologico, l'Enterprise Information Management, le soluzioni in ambito Security, l'approccio multivendor e la capacità progettuale rappresentano il focus di Hitachi Systems CBT, esattamente come nella vocazione di Hitachi Systems Ltd., con l'obiettivo di crescere a livello internazionale.

Nelle sedi di Roma, Milano, Venezia, e Bologna, Hitachi Systems CBT si avvale di un team di oltre 300 addetti, al quale si aggiunge il canale di operatori del Network di Partner a copertura del territorio.

Altro grande valore sono le oltre 1.200 certificazioni, sinonimo di competenze e costante aggiornamento sulle tecnologie multivendor a beneficio delle esigenze dei clienti.

Fondata nel 1994 **Sinergy S.p.A.** è tra i principali System Integrator del panorama ICT italiano e affianca oltre 600 clienti di tutti i settori fin dalla fase iniziale di assessment dell'infrastruttura. Con oltre 130 professionisti qualificati, Sinergy offre servizi di advisory "eseguibile", design, implementazione, integrazione, governo e gestione delle soluzioni dal NOC di Torino, proponendo soluzioni all'avanguardia per l'eccellenza del Data Center.

Le 25 risorse dedicate in ambito Information Security e Compliance e l'offerta Cyber Security Suite personalizzata mediante servizi strategici di Security Advisoring, indirizzano tutte le componenti siano esse organizzative, procedurali o tecnologiche.

La Cyber Security Suite ricopre aree multidisciplinari quali: dall'analisi degli attuali livelli di sicurezza all'individuazione delle vulnerabilità con attività di Ethical Hacking; dalla definizione delle soluzioni più idonee per il cliente all'implementazione di sistemi di protezione anche integrati sui nuovi paradigmi Cloud; dal governo della sicurezza al monitoraggio e gestione operativa dei servizi (Flexible Managed Services). L'offerta è in linea con gli standard e best practice internazionali quali ISO 27001, ISO22310, COBIT 5.0 e ITILv3.

**Horizon Security**
www.horizonsecurity.it
www.cybersoc.eu

**Horizon Security** Società italiana specializzata nella Cyber & ICT Security, opera da svariati anni sui più importanti mercati nazionali ed internazionali, affiancando i maggiori Gruppi Industriali, Finanziari, Assicurativi e dei Servizi nell' affrontare le sempre nuove sfide in ambito Cyber & ICT Security.

Attraverso una costante attività di formazione e di investimenti nella Ricerca, Horizon Security è in grado di proporre servizi e soluzioni all'avanguardia al passo con i continui mutamenti degli scenari tecnologici e normativi.

Può contare su numerosi professionisti appassionati e specializzati esclusivamente nell'ambito Cyber & ICT Security in grado di supportare qualunque soluzione organizzativa e tecnologica necessaria a proteggere il vostro business da rischi e minacce.

Grazie alle competenze maturate in ambito *Protezione infrastrutture critiche (SCADA – ICS), Governance Risk e Compliance*, lo sviluppo e l'implementazione di soluzioni per la *Data Protection*, alla disponibilità di un *SOC* proprio, siamo il partner ideale per la gestione di tutte le problematiche inerenti la Cyber Security.

Grafica: Osservatori Digital Innovation
Realizzazione: Danilo Galasso, Emanuela Micello e Stefano Erba
Stampa: Tipografia Litografia A. Scotti | www.ascotti.it

www.osservatori.net

Seguici anche su:

PARTNER

SPONSOR

SUPPORTER

IN COLLABORAZIONE CON

CON IL PATROCINIO DI